Canada Health Infoway
Inforoute Santé du Canada

Electronic Health Record (EHR) Privacy and Security Requirements

Reviewed with Jurisdictions and Providers

V1.1

Montreal

November 30, 2004

Revised February 7, 2005

Preface

This version 1.1 of EHR P&S Requirements is the result of 2 reviews done in January 2005: the first one with a pan-Canadian panel of 7 experts in EHR privacy and security, and the second with a group of 25 EHR privacy and security representatives from Canadian jurisdictions and health care provider associations.

This document does not constitute legal advice in one form or another. Organisations and individuals should seek legal counsel before determining how or whether a given law or regulation affects the implementation or operation of their electronic health record systems.

Please address your comments or questions regarding this document or the Privacy & Security Conceptual Architecture project to:

- Stanley Ratajczak, Director of IT Privacy and Security, 514.397.7334, sratajczak@infoway-inforoute.ca

Executive Summary

This document identifies the privacy and security (P&S) requirements that an interoperable electronic health record (EHR) must meet in order to fully protect the privacy of patient/persons and maintain the confidentiality, integrity and availability of their data. It is the third in a series of documents contributing to the development of a P&S conceptual architecture for the interoperable EHR that Infoway will publish in 2005. An understanding of these P&S requirements will facilitate the future identification of the P&S services needed to support the *EHRS Blueprint.* The final phase of Infoway's Privacy and Security project will develop and validate this conceptual P&S architecture, as well as identify other P&S initiatives to be taken by Infoway.

The P&S requirements discussed in this document are summarized in section 3. They reflect:

- legislative obligations as expressed in applicable data protection laws and regulations;
- established privacy and security best practices; and
- the P&S needs identified in common healthcare situations.

Section 4 of this document describes 28 privacy requirements for an interoperable EHR. These requirements are organised according to the ten privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96). The Code was published in March 1996 as a national standard for Canada. These core principles constitute a widely recognised and principled approach to data protection in an EHR environment.

Section 5 of this document identifies 86 security requirements for an interoperable EHR using ISO/IEC 17799-1:2000 *Code of Practice for Information Security Management* as its organisational framework. The current document follows the format of the proposed revised standard, 17799-1:2004, which ISO/IEC expects to publish prior to the conclusion of this project.; it includes an eleventh key control area: security incident management.

The ISO/IEC 17799 Code of Practice is a widely adopted international standard for information security management. The Code opens with an introduction describing information security and detailing why it is needed, how to assess security requirements and how to assess risks and assign controls. The remainder of the standard is organised into ten sections, each covering a key control area for information security. Together these describe the working objectives of the Code of Practice.

An appendix revisits the P&S issues raised in *Electronic Health Record Privacy and Security Use Cases,*[1] while a second appendix provides a brief description of health data protection legislation in Canada along with a comparison chart contrasting key features of these laws. Finally, the document concludes with a list of references.

[1] See the References section at the end of this document.

Table of Contents

Revised February 7, 2005 ..... **1**
Executive Summary ..... **iii**
Table of Contents ..... **i**
1 Introduction **1**
1.1 Purpose 1
1.2 Objective 1
1.3 Scope 1
1.4 Assumptions 2
1.5 Methodology 3
1.6 Terminology 3
1.6.1 EHR data and personal health information 6
1.7 Abbreviations used 7
1.8 Interpretation of requirements 8
1.9 Applicability 8
2 Privacy and security architecture project background **10**
2.1 Project description 10
2.2 Context for privacy and security requirements analysis 10
2.3 Governance and Consensus 11
3 Summary of requirements **13**
4 Privacy requirements **20**
4.1 Accountability for personal health information 20
4.2 Identifying purposes for collection, use and disclosure personal health information 22
4.3 Consent 24
4.4 Limiting collection of personal health information 31
4.5 Limiting use, disclosure and retention of personal health information 31
4.6 Accuracy of Personal Health Information 35
4.7 Safeguards for the protection of personal health information 35
4.8 Openness about practices concerning the management of personal health information 37
4.9 Individual access to personal health information 37
4.10 Challenging compliance 40
5 Security requirements **42**
5.1 Introduction 42
5.2 Risk Management 43
5.3 Security policy 44
5.4 Organising information security 44
5.4.1 Internal organisation 45
5.4.2 External Parties 46
5.5 Asset management 47
5.5.1 Responsibility for Assets 48
5.5.2 Information Classification 48
5.6 Human Resources Security 50
5.6.1 Prior to Employment 50
5.6.2 During Employment 52
5.6.3 Employment Termination 53
5.7 Physical and Environmental Security 53
5.7.1 Secure Areas 53
5.7.2 Equipment Security 54
5.8 Communications and Operational Management 55
5.8.1 Operational Procedures and Responsibilities 56
5.8.2 Third Party Service Delivery Management 57
5.8.3 System Planning and Acceptance 57

5.8.4 Protection Against Malicious And Mobile Code 58
5.8.5 Backup 58
5.8.6 Network Security Management 58
5.8.7 Media Handling 59
5.8.8 Exchanges Of Information 61
5.8.9 Electronic Commerce Services 61
5.8.10 Monitoring 61
5.9 Access Control 67
5.9.1 Requirements For Access Control 67
5.9.2 User Access Management 68
5.9.3 User Responsibilities 73
5.9.4 Network Access Control 74
5.9.5 Operating System Access Control 75
5.9.6 Application And Information Access Control 75
5.9.7 Workstation Access Control 75
5.9.8 Mobile Computing And Teleworking 76
5.10 Information Systems Acquisition, Development and Maintenance 77
5.10.1 Security Requirements Of Information Systems 77
5.10.2 Correct Processing Of Information 77
5.10.3 Cryptographic Controls 78
5.10.4 Security Of System Files 79
5.10.5 Security In Development And Support Processes 80
5.10.6 Vulnerability Management 80
5.11 Security Incident Management 80
5.11.1 Reporting Incidents And Weaknesses 80
5.11.2 Management Of Incidents And Improvements 81
5.12 Business Continuity Management 81
5.13 Compliance 82
5.13.1 Compliance With Legal Requirements 82
5.13.2 Compliance With Security Policies And Standards 82
5.13.3 Information Systems Audit Considerations 82
APPENDIX A Privacy And Security Implications Arising From Use Case Analysis 83
A.1 Privacy and Security Implications Connected With Actors 83
A.2 Privacy and Security Implications Connected With Use Cases 87
A.3 Consent 92
A.4 Other Issues 94
APPENDIX B Canadian Data Protection Related Legislation – Catalogue And Comparison 96
APPENDIX C Confidentiality, Integrity, Availability and Accountability 117
References 121

1 Introduction

The introduction defines the purpose, objective and scope of the document. It also provides assumptions behind the work done, the methodology followed, definitions of key terms used and other information relevant to the understanding of contents.

Section 2 describes briefly the privacy and security architecture project and the context for the requirements analysis. Section 3 summarises the privacy requirements and the security requirements detailed in sections 4 and 5 respectively.

Appendix A discusses privacy and security implications and issues arising from the use case analysis in the context of requirements identified in this document.

Appendix B presents two tables of information on Canadian data protection related legislation. The first table briefly describes legislation in Canada that is relevant to the privacy and security of the EHR. The second table provides a high-level comparison of the four provincial health data protection statutes and the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*. These tables are for discussion purposes only and should not be construed as legal advice.

Lastly, a last section identifies key references relevant to the contents of this document.

1.1 Purpose

This document describes the overall privacy and security (P&S) requirements for an interoperable electronic health record (EHR). The document has four purposes:

1. **Contribute to the identification of the required services for an interoperable EHR.** An understanding of privacy and security requirements for an interoperable EHR will facilitate the identification of the necessary privacy and security services within the *EHRS Blueprint.*
2. **Communicate with stakeholders.** Infoway will communicate these privacy and security requirements for an interoperable EHR with internal and external stakeholders and the current document will communicate these requirements to the jurisdictions and an external expert advisory panel.
3. **Serve as a foundational document** for the development of the privacy and security architecture for an interoperable EHR.
4. **Describe privacy and security requirements of the Electronic Health Record Infostructure (EHRi),** including privacy and security requirements for organisations connecting to the EHRi and organisations hosting components of the EHRi.

1.2 Objective

This document identifies and describes the privacy and security requirements for an interoperable EHR. In doing so, this document serves as a reference document for the Canadian healthcare IT community. The privacy and security requirements analyzed in this document reflect:

- legislative obligations as expressed in applicable data protection laws and regulations;
- established privacy and security best practices; and
- privacy and security issues identified in common healthcare situations.

1.3 Scope

The scope of this analysis covers the following:

1. all privacy and security requirements within the Electronic Health Record Infostructure (EHRi) as well as the connection points to the EHRi (e.g. the analysis covers organisations contributing to the EHRi as well as organisations that host components of the EHRi);
2. policy and other business related privacy and security requirements that may have an impact on the privacy and security conceptual architecture for an interoperable EHR;
3. legislative requirements identified in the project's legislation scan;
4. privacy and security issues identified in the project’s use cases; and
5. established privacy and security best practices, including international best practices and best practices from other industries (where applicable).

Privacy and security services required for an interoperable EHR are out of scope of this analysis. They are to be covered in a subsequent document.

Although reference is made herein to federal, provincial and territorial laws and regulations of Canada governing the privacy and security of personal health information, this document does not constitute legal advice. Organisations and individuals should seek legal counsel before determining how or whether a given law or regulation affects the implementation or operation of their electronic health record systems.

1.4 Assumptions

Infoway has made the following assumptions in the course of this requirements analysis:

- Infoway has identified privacy and security requirements for this analysis on the basis of current laws and regulations.
- Infoway recognizes that health data protection legislation is currently “in a state of flux”[2] in Canada. For example, Manitoba and Alberta are in the process of a comprehensive review of their respective health data protection statutes (i.e. Manitoba *Personal Health Information Act* and the Alberta *Health Information Act*). While substantial changes to both pieces of legislation are expected in the future, Infoway has predicated this analysis on current versions of the Acts.
- The analysis is predicated on existing standards and codes of practice[3] that are well established in the privacy and security fields. These are noted in the Methodology (section 1.5). Infoway recognizes, however, that an initiative in the privacy field to harmonize Canadian data protection statutes (e.g. the health information privacy and confidentiality framework developed by the Advisory Committee on Information and Emerging Technologies), or efforts to translate the ISO standard Code of Practice for Information Security (ISO/IEC 17799) to healthcare, have a potentially significant impact on this analysis. However, because these documents are still in draft form and are not publicly available, they are excluded from this analysis. If these documents are finalised and released to the public by January 2005, Infoway will re-visit this analysis to consider the impact of these documents on the development of privacy and security requirements for an interoperable EHR.

[2] Infoway notes that health data protection legislation in Canada is also in a state of flux because few jurisdictional legislation has been found to be substantially similar to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) to date.

[3] Section 4 identifies security requirements for an interoperable EHR using ISO/IEC 17799-1:2000 *Code of Practice for Information Security Management* as its organisational framework. ISO will shortly publish a revised version (ISO/IEC 17799-1:2004) that includes an eleventh key control area: security incident management. This document follows the format of the revised standard, 17799-1:2004, which ISO expects to publish prior to the conclusion of this project.

- Finally, this analysis assumes that no transfers of personal health information to the EHRi will be permissible, within or among jurisdictions, except in compliance with the detailed laws and regulations that already exist and that are not, at present, harmonized. As a general rule, Infoway therefore assumes that the jurisdiction of the sender will set the prevailing legal standard for any particular data transfer or exchange.

1.5 Methodology

The analysis separates the privacy and security requirements for the handling of personal health information (PHI) into two categories: (1) privacy requirements and (2) security requirements. Infoway has used the 10 principles of the CSA Model Code[4] as an organisational framework for the privacy requirements. The ISO standard Code of Practice for Information Security (ISO/IEC 17799) has been used as an organisational framework for the security requirements.

The analysis describes each requirement, explains why Infoway selected each requirement, and outlines how each requirement relates to an interoperable EHR. All privacy and security requirements outlined in legislation that are relevant to an interoperable EHR are contained in this analysis. Infoway has selected other requirements, which are *not* necessarily contained in legislation, according to the following criteria:

- Does the requirement address the privacy or security issues illustrated in the project's use cases, including the various classes of user who will interact with the EHRi and its related systems, the various scenarios within which they will use an EHRi, and the individual uses that they will make of different EHRi components?
- Does the requirement reflect an established privacy and security standard that is applicable to the handling of PHI within an interoperable EHR?
- Does the requirement reflect an established best practice that is applicable to the handling of PHI within an interoperable EHR?

1.6 Terminology

Best Practice – *A practice that has been shown in actual application to be of value*.[5] Note that best practices may or may not be required under legislation. For example, although privacy impact assessments are required under the Alberta Health Information Act, they are generally not required under the Ontario *Personal Health Information Protection Act*,[6] although some Ontario health information custodians routinely conduct them on new information systems or projects as part of their privacy best practices.

Custodian – an individual or organization that collects, uses, or discloses personal health information for the purposes of care and treatment, planning and management of the health system or health research.

The individual jurisdiction's legislation typically includes the following entities:

[4] The CSA Model Code also forms the basis of Schedule 1 of PIPEDA (the *Personal Information Protection and Electronic Documents Act*, 2001).

[5] Canada Health Infoway EHR Glossary available at www.infoway-inforoute.ca.

[6] The draft regulations for the Ontario *Personal Health Information Protection Act* require that "health information network providers" conduct privacy impact assessments under specific conditions outlined in regulations. However, health information custodians who are not functioning as a health information network provider are not required to conduct privacy impact assessments. The Act and the draft regulations are available at: http://www.health.gov.on.ca/english/public/updates/archives/hu_03/priv_legislation.html.

- Health service providers, i.e., persons who are licensed or registered to provide health services.
- The Federal/Provincial/Territorial Minister and Department of Health
- Regional Health Authorities (where they exist)
- Hospitals and nursing homes and other identified health care facilities
- Pharmacists and pharmacies
- Boards, agencies, committees and other organizations identified in regulations
- Affiliates/agents e.g. employees, volunteers
- Cancer Board
- Mental Health Board
- Ambulance Operators
- Persons who maintain and administer an EHR system[7]

Data Protection Legislation – This term includes health data protection legislation, as well as private and public sector data protection legislation (e.g. privacy legislation). To date, three provinces have private sector privacy legislation (British Columbia, Alberta, and Quebec.)

Electronic Health Record – *an electronic record that provides each individual in Canada with a secure and private lifetime record of his or her key health history and care within the health system. The record is available electronically to authorized healthcare providers and the individual anywhere, anytime in support of high quality care.*[8] In an Electronic Health Record Infostructure (EHRi), the EHR is the central component that stores, maintains and manages clinical information about patients/persons. The extent of the clinical information sustained by the EHR component may vary based namely on the presence or absence of Domain Repositories in any given jurisdiction.

Electronic Health Record Data (EHR Data) – *the collection of clinical data related to a particular patient/person.*[9] Note the distinction between EHR data and personal health information (PHI) discussed below in subsection 1.6.1.

Electronic Health Record Infostructure (EHRi) – *a collection of common and reusable components in support of a diverse set of health information management applications.*[10] It consists of software solutions for the EHR, data definitions for the EHR and messaging standards for the EHR.

EHRi User – Any individual or organisation authorized to access the EHRi.

[7] Advisory Committee on Information and Emerging Technologies (ACIET), The Pan-Canadian Health Information Privacy and Confidentiality Framework , January 6, 2005.
[8] EHRS Blueprint: An Interoperable EHR Framework, Canada Health Infoway, July 2003, p. 164.
[9] EHRS Blueprint: An Interoperable EHR Framework, Canada Health Infoway, July 2003, p. 163.
[10] EHRS Blueprint: An Interoperable EHR Framework, Canada Health Infoway, July 2003, p. 163.

Electronic Health Record Solution (EHRS) – *a combination of people, organisational entities, business processes, systems, technology and standards that interact and exchange clinical data to provide high quality and effective healthcare*.[11]

Health Data Protection Legislation – Four provinces have enacted comprehensive health data protection legislation to govern the collection, use, and disclosure of individually identifiable health information in the hands of trustees or custodians (Alberta, Saskatchewan, Manitoba, and Ontario.) This legislation also governs an individual's access to his or her own health information.

Information asset – information, stored in any manner, recognised by the organisation that posseses it as being valuable.

Legislative Requirement – *a requirement that is formally outlined in current legislation and/or regulations***.** For example, privacy impact assessments are formally required under the Alberta *Health Information Act*.

Personal Health Information (PHI) –.information about an identifiable individual that relates to the physical or mental health of the individual, or provision of health services to the individual, and may include:

- information about the registration of the individual for the provision of health services,
- information about payments or eligibility for heath care in respect to the individual,
- a number, symbol or particular assigned to an individual to uniquely identify the individual for health care purposes,
- any information about the individual that is collected in the course of the provision of health services to the individual,
- information derived from the testing or examination of a body part or bodily substance, and
- the identification of a person as provider of healthcare to the individual.

Personal health information does not include information that, either by itself or when combined with other information available to the holder, is anonymised, i.e. the identity of the individual who is the subject of the information cannot be readily ascertained from the information.[12] Note the distinction between EHR data and PHI discussed below in subsection 1.6.1.

Personal Information Protection and Electronic Documents Act (PIPEDA) – a federal statute that sets out ground rules for how organisations may collect, use or disclose personal information in the course of commercial activities. The law gives individuals the right to see and ask for corrections to personal information an organisation may have collected about them, subject to specific and limited exceptions. The Act applies to personal information about customers or employees that is collected used or disclosed by the federally regulated sector in the course of commercial activities, or to personal information about customers at provincial organisations performing commercial activities, unless such organisations are already covered by privacy legislation that is "substantially similar" to PIPEDA. In addition, the Act covers all businesses and organisations engaged in commercial activity in Yukon, the Northwest Territories and Nunavut as well as personal information in all inter-provincial and international

[11] EHRS Blueprint: An Interoperable EHR Framework, Canada Health Infoway, July 2003, p. 164.

[12] Advisory Committee on Information and Emerging Technologies (ACIET), The Pan-Canadian Health Information Privacy and Confidentiality Framework , January 6, 2005. The phrase "including the identification of a person as provider of healthcare to the individual" has been added to the ACIET definition.

transactions by organisations subject to the Act. The federal government may exempt organisations or activities in provinces that have their own privacy laws if they are deemed to be substantially similar to the federal law. To assist in making that determination, the Privacy Commissioner is mandated, under the Act, to report to Parliament on the extent to which provinces have passed legislation that is in fact substantially similar.[13]

Point of Service (POS) System — The clinical application systems (e.g. ADT, CIS, LIS, etc.) that operate at the many locations where the healthcare services are delivered to patients/persons. These systems may have human computer interfaces or be medical equipment generating data on a user that is then fed into the EHR. These systems are the sources for all clinical information that make up the EHR Data. They may also access data from the EHRi when it is operational, as well as from their own data stores to provide a more complete view of a patient/person's health history and current information.[14]

Security Critical Data – In addition to protecting the confidentiality, integrity and availability of PHI, components of the EHRS must also protect many other types of data that are critical to the overall security of the system. These data include:

- identifiers and other registration details of system users that could assist an attacker in impersonating a legitimate user;
- data used during user authentication;
- data used in authorization and privilege management to determine what actions an individual user can perform and which data the user can access;
- configuration data for firewalls, intrusion detection systems and other software and hardware resources used to secure components of the EHRS; and
- private or secret cryptographic keys used for encrypting or decrypting data or for generating digital signatures.

Standard – a document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.[15] Examples of standards in the Canadian healthcare sector are ICD-10-CA and HL7.

1.6.1 EHR data and personal health information

As defined in Infoway's EHRS Blueprint, EHR data consists of the collection of clinical data related to a particular patient/person. PHI includes EHR data and much more. The following are the principal types of PHI discussed in this document:

a) EHR data (i.e., clinical data related to a particular patient/person, including medical history, allergies and chronic conditions, lab test orders and results, prescription drug profiles, diagnostic images, healthcare encounter data, and other forms of clinical data);

[13] Excerpted from the Office of the Privacy Commissioner of Canada's Frequently Asked Questions, available at: www.privcom.gc.ca

[14] EHRS Blueprint, p. 37.

[15] ISO/IEC Guide 2:1996, definition 3.2

b) demographic data related to a particular patient/person, including, names, addresses, and other personal contact information;

c) identifiers assigned to a patient/person to uniquely identify the individual for healthcare purposes;

d) emergency contacts for a patient/person, including name, address and other contact information for each emergency contact;

e) substitute decision makers for a patient/person, including name, address and other contact information for each substitute decision maker;

f) consent directives of a particular patient/person, including directives for locking or masking selected data;

g) comments, corrections or other annotations made by patients/persons on data contained in their EHR;

h) public health surveillance data related to a particular patient/person; and

i) audit logs of who has accessed or updated any of the data listed in items a to g above, including identifiers assigned to accessing users, the logged actions they have performed (adding data, updating data, overriding consent directives if applicable during medical emergencies, etc.), and the logged values of fields that have been added, updated, or annotated.

In addition to paper-based repositories of health records, PHI may be received, stored, transmitted or processed in POS systems (e.g.: in a Hospital Information System) and it may also be received, stored, transmitted or processed in the EHRi (e.g.: in a jurisdictional domain repository of drug prescriptions). Whenever PHI is discussed in the current document, it will be made clear whether the discussion is relevant to POS systems or to the EHRi, or both.

1.7 Abbreviations used

CPO	Chief Privacy Officer
EHR	Electronic Health Record
EHRi	Electronic Health Record Infostructure
EHRS	Electronic Health Record Solution
P&S	Privacy and Security
PHI	Personal Health Information
PIPEDA	Personal Information Protection and Electronic Documents Act
POS	Point of Service[16]

[16] Note: the EHRS Blueprint defines (but does not use) the acronym POS to mean "Physician Office System".

1.8 Interpretation of requirements

In the requirements that follow, the words ***must, must not, should,*** and ***should not*** are intended to have the same interpretations as those used by the Internet Engineering Task Force when these words are used in Internet standards[17]:

1. **Must**: this word means that the definition is an absolute requirement of the specification.

2. **Must not**: this phrase mean that the definition is an absolute prohibition of the specification.

3. **Should**: this word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. **Should not**: this phrase means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

1.9 Applicability

Each requirement that follows in Section 4 (Privacy requirements) and Section 5 (Security requirements) applies to one or more of the following:

1. the EHRi,
2. Point of Service (POS) systems connected to the EHRi,
3. organisations hosting components of the EHRi, and
4. organisations connecting to the EHRi.

Note that (1) and (2) refer to systems (i.e., servers, software, etc.) and (3) and (4) refer to organisations (physician practices, clinics, hospitals, provincial ministries of health, etc.)

As noted above in section 1.6 (Terminology), the EHRi (item 1 above) consists of software solutions for the EHR, data definitions for the EHR and messaging standards for the EHR. An example therefore of (1) in the list above would be a provincial infostructure that implements the EHRi in that province.

A POS systems connected to the EHRi (item 2 above) would be one of the following types:

- **a clinical information system (CIS) –** a system installed in physician offices, hospitals or clinics that is dedicated to collecting, storing, manipulating and making available clinical information important to the delivery of healthcare.
- **a hospital information system (HIS) –** an application system that manage all facets of a hospital operation, including patient administration, billing, and clinical records.
- **a pharmacy information system (PIS) –** a system installed in a hospital, pharmacy or drug store chain that is dedicated to collecting, storing, manipulating and making available medication information on patient/persons who are customers of the pharmacy. A PIS is not to be confused with a jurisdictional domain repository of patient/person medication data. BC Pharmanet is an example of the latter. Examples of PIS can be found within several well known drug store chains in Canada.

[17] The definitions are taken from IETF RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", March, 1997.

- **a laboratory information system (LIS)** – a system that manages one or more facets of a clinical laboratory operation, including acquiring and distributing results of laboratory exams as part of clinical records. An LIS is not to be confused with a jurisdictional domain repository of patient/person laboratory test results. The proposed OLIS system in Ontario is an example of the latter. Examples of LIS can be found within virtually all well known companies that provide laboratory diagnostics services in Canada, as well as in most public health labs and hospital labs.
- **a digital imaging and PACS system(DI/PACS) –** a system that permits the use of digital images and textual reports prepared as a result of performing diagnostic studies such as x-rays, cat scans, MRI, etc. A Picture Archiving and Communications System (PACS) is an application that uses an image server to exchange X-rays, CT scans and other medical images over a network. Mini-PACS specialize in one type of image such as an ultra- sound, it can be used to store, retrieve and manage digital images.

An organisation hosting components of the EHRi (item 3 in the list above) would typically be a large publicly funded institution, agency or government ministry. The organisation would be mandated to collect, transmit and/or store PHI electronically, and make various application services available to POS systems that could then connect to the EHRi and make use of the EHRi components that the organisation hosts. An example of such a hosted component would be a provincial domain repository for prescription drug profiles.

Examples of (4) above would include a hospital, a clinic, or a physician office that connects to the EHRi. The connection could be made via a POS system or directly through a web portal.

Some of the requirements that follow are administrative requirements (i.e., they refer to policy and practices), and hence apply to organisations (i.e., to items 3 or 4 in the list above). Other requirements are technical and refer to EHRi or POS systems and software (i.e., to items 1 or 2 above).

The wording of each requirement will unambiguously indicate which of the entities above is the intended target of the demands made by the requirement.

2 Privacy and security architecture project background

2.1 Project description

The *Infoway EHRS Blueprint* (the *Blueprint*) presents the business and technical architecture for an interoperable EHR framework. Essential to the Blueprint are the services required to ensure the privacy and security of PHI accessible from the EHR. Specifically, the privacy and security architecture project is intended to:

- define the privacy and security services to be included in the Blueprint as required to support common solution architecture and common standards needed to ensure interoperability and re-use;
- design a flexible privacy and security conceptual architecture in support of current and future jurisdictional legislative, regulatory and policy requirements; and
- identify specific privacy and security initiatives that Infoway should pursue.

2.2 Context for privacy and security requirements analysis

The current phase of the project includes defining and validating privacy and security requirements that an interoperable EHR must provide. A later phase will develop and validate the privacy and security conceptual architecture, as well as identify privacy and security initiatives, using the project's deliverables as a guide.

An understanding of the privacy and security requirements of an interoperable EHR will facilitate the identification of the necessary privacy and security services within the *Blueprint.* The current document provides this analysis of privacy and security requirements. Most importantly, this documents builds on the legislative scan and use cases conducted earlier in the project to construct a more detailed framework that will facilitate the identification of privacy and security services within the Blueprint (see Figure 1 below).

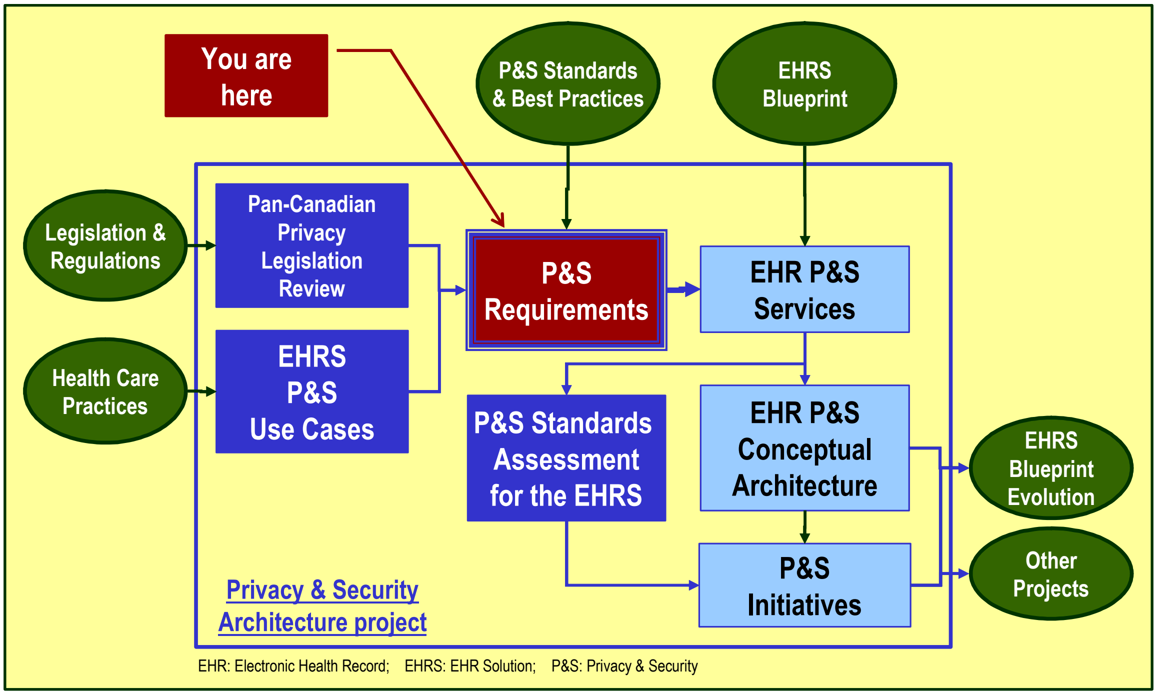
You are here
P&S Standards & Best Practices
EHRS Blueprint
Legislation & Regulations
Pan-Canadian Privacy Legislation Review
P&S Requirements
EHR P&S Services
Health Care Practices
EHRS P&S Use Cases
P&S Standards Assessment for the EHRS
EHR P&S Conceptual Architecture
EHRS Blueprint Evolution
Other Projects
P&S Initiatives
Privacy & Security Architecture project
EHR: Electronic Health Record; EHRS: EHR Solution; P&S: Privacy & Security

Figure 1 Context for this document

2.3 Governance and Consensus

All members of the Canadian healthcare community share in the responsibility to maintain patient privacy and data protection of PHI. No matter how much care and attention is devoted to the technology behind the EHRi, it will never be enough if the policies, procedures, practices, and training needed for its proper and secure operation are neglected. The technical security measured implemented in the EHRi can work flawlessly and yet If the system is administered by those who lack the training to ensure its proper and secure operation, if its users do not understand the confidential nature of the information that they access and do not treat it accordingly, if user registration procedures are sufficiently lacking in rigour that unauthorized third parties can become authorized users, or if the infostructure is used to collect and retain personal information of a kind that patients would not have countenanced had they known, then patient/person privacy will have been breached. It is essential therefore to state the administrative requirements for the secure use and operation of EHRi, as well as the technical requirements for its design and implementation.

In stating these administrative requirements, Infoway is keenly aware that it has no mandate to develop policy or to assess compliance with policy, nor will it ever have such a mandate. The administrative requirements have been developed in close consultation with Canadian health informatics experts and with healthcare representatives of Canada's federal, provincial and territorial jurisdictions and professions. This document continues to evolve within this collaborative framework and it is expected that broad consensus will indeed be achieved. Indeed, it is hoped that the overwhelming majority of healthcare professionals involved with privacy and security issues will come to agree with the requirements as stated either in this document or in a future revision. Nevertheless, the question of exactly what the requirements are for the secure and privacy protective design, implementation and ongoing operation of the EHRi is ultimately a question to be resolved by whatever information governance structure is put in place to guide the deployment of the EHRi across Canada and the future inter-jurisdictional flow of information that the EHRi will facilitate. Many EHRi governance issues are unresolved at the time of this writing. In stating that governance is outside the scope of this document, the authors in no way wish to diminish the important task of resolving these important governance issues.

3 Summary of requirements

The following two tables summarise the privacy requirements and security requirements detailed in sections 4 and 5 below.

Each table indicates whether the requirement is administrative or technical. Administrative requirements are those that involve policy, practices, contractual and other agreements, and staff procedures. Technical requirements are those that place demands upon system architecture and deployment.

An indication is made for each requirement as to whether it applies to the EHRi, POS systems connected to the EHRi, organisations hosting components of the EHRi, or organisations connecting to the EHRi.

Table 1: Summary of privacy requirements

	Requirement Applies to:					
Privacy Requirements	**EHRi**	**POS Systems Connected to EHRi**	**Organisations Hosting Components of EHRi**	**Organisations Connecting to EHRi**	**Administrative Requirement**	**Technical Requirement**
Requirement 1 Accountable Person			√	√	√	
Requirement 2 Third Party Agreements			√	√	√	
Requirement 3 Privacy Policy			√	√	√	
Requirement 4 Privacy Impact Assessments			√		√	√
Requirement 5 Identifying Purposes for Collection, Use and Disclosure			√	√	√	
Requirement 7 Limitation of Collection, Use or Disclosure to Identified Purposes			√	√	√	
Requirement 8 Obtaining Knowledgeable Consent			√	√	√	
Requirement 9 Recording Consent in POS Systems		√			√	√
Requirement 10 Associating Consent with PHI in POS Systems		√			√	√
Requirement 11 Recording Consent in the EHRi	√				√	√
Requirement 12 Associating Consent Directives with PHI in the EHRi	√				√	√
Requirement 13 Logging the Application of Consent Directives	√					√
Requirement 14 Implications of Consent Directives			√	√	√	

Privacy Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	POS Systems Connected to EHRi	Organisations Hosting Components of EHRi	Organisations Connecting to EHRi		
Requirement 15 Recording Identity of Substitute Decision Makers	√				√	√
Requirement 16 No Coerced Consent			√	√	√	
Requirement 17 Collecting Information by Fair and Lawful Means			√	√	√	
Requirement 18 Limiting Use and Disclosure of Personal Health Information to Identified Purposes			√	√	√	
Requirement 19 Logging Access, Modification and Disclosure	√	√				√
Requirement 20 Notifying Patients/Persons of Inappropriate Access, Use or Disclosure			√	√	√	
Requirement 21 Retaining Records	√	√	√	√	√	√
Requirement 22 Accuracy			√	√	√	√
Requirement 22a Denoting Patients/Persons At Elevated Risk	√	√				
Requirement 22b Training Users and Raising Privacy Awareness			√	√	√	
Requirement 23 Openness			√	√	√	
Requirement 24 Patient/Person Access			√	√	√	
Requirement 25 Amending Inaccurate or Incomplete Information			√	√	√	√
Requirement 26 Challenging Compliance			√	√	√	
Requirement 27 Complaint Procedures	√	√			√	
Requirement 28 Investigation	√	√			√	

Table 2: Summary of security requirements

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	POS Systems Connected to EHRi	Organisations Hosting Components of EHRi	Organisations Connecting to EHRi		
Requirement 1 Threat and Risk Assessment			√		√	
Requirement 2 Security Policy			√	√	√	
Requirement 3 Information Security Management, Co-ordination, and Allocation of Responsibilities			√		√	
Requirement 4 Independent Review of Security Policy Implementation			√	√	√	
Requirement 5 Assessing Threats and Risks from Third Parties			√		√	
Requirement 6 Addressing Security in Third Party Agreements			√		√	
Requirement 7 Transmitting PHI			√	√	√	
Requirement 9 Responsibility for Information Assets			√		√	
Requirement 10 Classifying PHI			√	√	√	
Requirement 11 Labelling Personal Health Information As Confidential		√				√
Requirement 12 Addressing User Responsibilities In Job Definitions			√	√	√	
Requirement 13 Addressing User Responsibilities In Terms of Employment			√	√	√	
Requirement 14 Verifying the Identity of Users			√	√	√	
Requirement 15 Confidentiality Agreements			√	√	√	
Requirement 16 Training Users and Raising Security Awareness			√	√	√	
Requirement 17 Terminating User Access When Terminating Employment			√	√	√	√
Requirement 18 Physically Securing EHRi Systems			√		√	√
Requirement 19 Protecting EHRi Systems from Hazards			√		√	√

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	POS Systems Connected to EHRi	Organisations Hosting Components of EHRi	Organisations Connecting to EHRi		
Requirement 20 Protecting EHRi Systems from Disruptions			√		√	√
Requirement 21 Protecting EHRi Equipment Off-Premises			√		√	
Requirement 22 Disposing of or Reusing EHRi Equipment			√	√	√	√
Requirement 23 Removing EHRi Equipment, Data or Software			√		√	
Requirement 24 Controlling Changes to the EHRi			√		√	
Requirement 25 Segregating Duties			√		√	
Requirement 26 Separating Development and Testing from Operations			√		√	√
Requirement 27 Maintaining Capacity			√		√	√
Requirement 28 Upgrading the EHRi			√		√	√
Requirement 29 Protecting Against Malware			√	√	√	√
Requirement 30 Securely Backing Up Data			√		√	√
Requirement 31 Encrypting PHI During Transmission	√					√
Requirement 32 Protecting Source and Destination Integrity During Transmission of PHI	√					√
Requirement 33 Acknowledging Receipt of Transmitted PHI	√					√
Requirement 34 Protecting PHI on Portable Media			√		√	√
Requirement 35 Disposing of Media Containing PHI			√	√	√	√
Requirement 36 Protecting Data Storage			√		√	√
Requirement 37 Protecting Storage of Unencrypted PHI in the EHRi			√		√	
Requirement 38 Logging Transactions in the EHRi	√					√
Requirement 39 Preserving the History of PHI in the EHRi	√					√

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	POS Systems Connected to EHRi	Organisations Hosting Components of EHRi	Organisations Connecting to EHRi		
Requirement 40 Preserving the History of PHI in POS Systems		√				√
Requirement 41 Logging EHRi Transmissions of PHI	√					√
Requirement 42 Logging Access to PHI in POS Systems		√				√
Requirement 43 Minimum Content of Audit Logs	√	√				√
Requirement 44 Retaining Audit Logs			√	√	√	√
Requirement 45 Continuously Logging the EHRi	√					√
Requirement 46 Detecting Patterns of Misuse	√					√
Requirement 47 Reporting Every Access To A Patient/Person's EHR	√					√
Requirement 48 Reporting Every Access By A User	√					√
Requirement 49 Analyzing EHRi Audit Logs for Patients/Persons At Elevated Risk	√					√
Requirement 50 Securing Access to EHRi Audit Logs	√		√		√	√
Requirement 51 Making EHRi Audit Logs Tamper-Proof	√					√
Requirement 52 Regularly Reviewing EHRi Audit Logs	√				√	
Requirement 53 Policy for Access Control	√				√	
Requirement 54 Registering Users				√	√	
Requirement 55 Assigning Identifiers to Users				√		√
Requirement 56 Time Limited User Registration				√	√	
Requirement 57 Reviewing User Registration Details				√	√	
Requirement 58 Granting Access to Users by Role	√	√				√
Requirement 59 Selecting A Single Role Per Session		√				√
Requirement 60 Granting Access to Users in Work Groups	√	√				√

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	POS Systems Connected to EHRi	Organisations Hosting Components of EHRi	Organisations Connecting to EHRi		
Requirement 62 Timely Revocation of Access	√	√				√
Requirement 63 Granting Access By Association	√	√				√
Requirement 64 Acceptable use agreements				√	√	
Requirement 65 Authenticating EHRi Network Access			√			√
Requirement 66 Controlling Access to EHRi Network Diagnostics and Network Management Services			√			√
Requirement 67 Segregating EHRi Network Users, Services and Systems			√			√
Requirement 68 Controlling Routing on EHRi Networks			√			√
Requirement 69 Controlling Access to EHRi System Utilities			√			√
Requirement 70 Restricting Connection Times to EHRi Applications	√					√
Requirement 71 Robustly Authenticating Users	√	√				√
Requirement 72 Restricting Access to Unattended Workstations		√				√
Requirement 73 Acceptable Use of Mobile Devices				√	√	
Requirement 74 Acceptable Use of Teleworking				√	√	
Requirement 75 Protecting Wireless Networks			√	√		√
Requirement 76 Assigning Identifiers to Patients/Persons	√	√				√
Requirement 77 Validating Input Data	√	√				√
Requirement 78 Validating Printed Data		√				√
Requirement 79 Providing Digital Signatures for Users		√				√
Requirement 80 Validating and Preserving Digital Signatures On PHI	√					√

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	POS Systems Connected to EHRi	Organisations Hosting Components of EHRi	Organisations Connecting to EHRi		
Requirement 81 Implementing Software and Upgrades in the EHRi			√		√	
Requirement 82 Protecting EHRi Software			√			√
Requirement 83 Managing Known Vulnerabilities			√			√
Requirement 84 Reporting Security Incidents Involving the EHRi	√	√				√
Requirement 85 Responding to Security Incidents Involving the EHRi			√		√	
Requirement 86 Managing Business Continuity			√		√	
Requirement 87 Testing Business Continuity Plans□			√		√	

4 Privacy requirements

The privacy requirements for an interoperable EHR are organised according to the ten privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96). It was published in March 1996 as a national standard for Canada. Schedule 1 of the federal *Personal Information Protection and Electronic Documents Act* incorporates the CSA Model Code. These core principles facilitate an easily recognisable, principled approach to data protection in an EHR environment.

4.1 Accountability for personal health information

Organisations that collect, use or disclose PHI are responsible for PHI in their care or custody, including information transferred to third parties, and must name someone who will be responsible for facilitating compliance with applicable data protection legislation and the privacy requirements described herein. Although all staff in each organisation connecting to the EHRi or hosting components of the EHRi may be responsible for the collection, use, and disclosure of PHI on a day-to-day basis, it is critical that the organisation designates an individual or individuals accountable for the organisation's overall privacy compliance.

Privacy Requirement 1 Accountable Person

Organisations connecting to the EHRi and organisations hosting components of the EHRi **must** designate and publicly name an individual who is accountable for facilitating compliance with applicable data protection legislation and the following privacy requirements.

Policy & Procedures

Admin Requirement

Rationale: Appointing an individual to be accountable for privacy is both an industry best practice and also a legal requirement under several Canadian Privacy laws.[18], Many healthcare organisations have already designated an individual in this regard, often called the "Chief Privacy Officer". Working with a privacy team representing various relevant components of the organisation, the Chief Privacy Officer is usually the focal point for data protection issues, both internally and externally.

See also Privacy Requirement 27 (Complaint Procedures).

[18] Section 15 of Ontario's *Personal Health Information Protection Act* and section 57 of the Manitoba *Personal Health Information Act* require that health information custodians appoint an individual accountable for the organisation's compliance with these privacy laws*,*

Privacy Requirement 2 Third Party Agreements

Organisations connecting to the EHRi and organisations hosting components of the EHRi **must** use contractual means[19] to provide a comparable level of privacy protection while a third party, such as a service provider, is processing PHI. Such agreements should include the following information:

1. The purpose(s) for which PHI being shared with the third party;

2. a listing of the PHI that will be shared with the third party;

3. the purposes for which the PHI may be used or disclosed by the third party; and

4. obligations on the third party upon termination of the agreement.

Policy & Procedures

Admin Requirement

Rationale: Organisations connecting to or hosting components of the EHRi need to ensure that they only transfer PHI to third parties that use “comparable levels of protection”. However, there are differing legal requirements in different provinces across Canada for the transfer of personal information to third parties. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), for example, requires all organisations to be responsible for personal information in their possession or custody, including information that has been transferred to a third party for processing. Such an organisation must use contractual or other means to provide a comparable level of protection while any third party is processing the information.[20]

See also **Security Requirement 6.**

Privacy Requirement 3 Privacy Policy

Organisations connecting to the EHRi and organisations hosting components of the EHRi **must** implement policies and practices, including:

a) Implementing procedures to protect PHI (see **Security Requirement 2**)
b) Establishing procedures to receive and respond to privacy related complaints and inquiries (see **Privacy Requirement 27**);
c) Training users and communicating to users information about the organisation’s privacy policies and practices (see **Privacy Requirement 22b** and **Security Requirement 15**); and
d) Developing communications materials to explain to the general public the organisation’s privacy policies and practices (see **Privacy Requirement 23**).

Policy & Procedures

Admin Requirement

[19] "Contractual means" includes letters of agreement, data sharing agreements, memoranda of understanding, etc.

[20] Most health data protection legislation includes similar provisions, including Alberta *Health Information Act*, BC *Freedom of Information and Protection of Privacy Act*, Manitoba *Personal Health Information Act*, Ontario *Personal Health Information Protection Act*, Saskatchewan *Health Information Protection Act* and Quebec *Act Respecting Protection of Personal Information in the Private Sector*. See the discussion of this provision in Stephanie Perrin, Heather H. Black, David H. Flaherty, and T. Murray Rankin, The Personal Information Protection and Electronic Documents Act: An Annotated Guide (Irwin Law, Toronto, 2001), p. 16. The consultants acknowledge their indebtedness to the authors of this informed commentary on Schedule 1 of PIPEDA (pp. 13-46).

Rationale: It is necessary for the mutual benefit of all EHRi users, including POS system users connected to the EHRi, that policies and procedures be in place to ensure compliance with legal obligations for data protection. A detailed privacy policy will operationalize fair information practices and lead to the development of sound information management procedures, clearer security procedures and practices, reduce the collection and management of unnecessary PHI, and facilitate compliance with relevant data protection legislation.

Privacy Requirement 4 Privacy Impact Assessments

Organisations hosting components of the EHRi, **should** assess, by means of a Privacy Impact Assessment, the risks to personal privacy associated with implementation of the hosted components and **should** implement appropriate privacy controls to mitigate identified risks. Privacy Impact Assessments **should** be made available to the public upon request.

Policy & Procedures
Admin Requirement **Tech Requirement**

Rationale: Privacy Impact Assessments are essential for outlining privacy risks and risk mitigation strategies associated with access to PHI by third parties. Comprehensive Privacy Impact Assessments need to address such issues as privacy risk management, record linkages, and security safeguards. The confidentiality of data related to healthcare providers also needs to be considered. In some F/P/T jurisdictions, Privacy Impact Assessments are also required by law.[21]

See also **Security Requirement 5**.

4.2 Identifying purposes for collection, use and disclosure personal health information

In order to allow patients/persons to make appropriate decisions about their PHI, it is important that they are made aware of and understand the purposes for which it is being collected, used, and disclosed. The emphasis on openness about the purposes for collection of PHI is meant to ensure that patients/persons will have ample opportunity to find out what will be done with their PHI, especially in addition to the delivery of healthcare (e.g. research or health surveillance activities).

Furthermore, a number of provincial jurisdictions have a legal requirement to identify purposes for which PHI is collected, [22] as well as identify any new purposes prior to using information for these new purposes. To satisfy this legal requirement, healthcare organisations must identify the purposes for which they collect, use and disclose a patient/person's PHI.

[21] Alberta *Health Information Act*, section 64.

[22] The general public only needs a brief list of the main categories, not a complete list of relevant disclosures, for example, such as exists in a statute. See, for example the Ontario *Personal Health Information Protection Act,* sections 38-50.

Privacy Requirement 5 Identifying Purposes for Collection, Use and Disclosure

Organisations connected to the EHRi and organisations hosting components of the EHRi **must**:

a) identify all the purposes for which PHI will be collected, used, and disclosed at or before the time it is collected[23]; and

b) make a reasonable effort to inform patient/persons of these purposes, in a readily understandable manner, prior to collecting their PHI.

Policy & Procedures

Admin Requirement

Rationale: This requirement ties together the concepts of obtaining "knowledgeable" consent and stating purposes for information use (see section 4.8 below). The goal is to make a reasonable effort to ensure that patients/persons understand the purposes for which organisations connected to the EHRi and organisations hosting components of the EHRi collect, use and disclose their PHI.[24]

Depending upon the way in which PHI is collected, organisations can fulfill this requirement orally, in writing, or by posting a notice. An admission or appointment form, for example, may give notice of the purposes. However, the novelty of the EHR and the anxiety it can arouse about the protection of privacy interests make it imperative that patients/persons be informed, in an appropriate way, of the prospective uses and disclosures of their personal information. Patients/persons should be given as much information as they wish to have.

NOTE: Privacy Requirement 6 Associating Identified Purposes With Collected PHI has been delete. The requirements will be renumbered in the next version of this document.

Privacy Requirement 7 Limitation of Collection to Identified Purposes

Organisations connecting to the EHRi or organisations hosting components of the EHRi **should** only collect PHI necessary to fulfill the purposes that they have identified (see **Privacy Requirement 5**).

Policy & Procedures

Admin Requirement

Rationale: The ultimate goal is to have no secret, or unspecified, collections, uses or disclosures of personal information held in an EHRi or in POS systems connected to the EHRi. This is an especially delicate issue in healthcare, because a patient/person may not have much of a choice with respect to collection, use, or disclosure, if he or she wishes to receive healthcare. Such patients/persons have a right to know what uses and disclosures, in particular, are mandated by law, such as for mandatory reporting of infectious diseases or suspected child abuse or for law enforcement.

[23] In some situations, such as healthcare emergencies, it may not be reasonably possible to identify the purposes for which PHI is collected, used, and disclosed *at or before* the time it is collect. In these situations the purposes for which PHI is collected, used, and disclosed *must* be identified at the first reasonable opportunity.

[24] Ontario, *Personal Health Information Protection Act*, section 16(1) requires a health information custodian to make available to the public a written statement that provides a general description of the custodian's information practices in a manner that is practicable in the circumstances. This would apply as well in an EHRi regime.

4.3 Consent

Laws may require express, implied or deemed consent for specific collections, uses and disclosures of PHI. Express consent includes any action by a patient/person or their authorized representative (e.g. parent, guardian or substitute decision maker) specifically to authorize the collection, use or disclosure of personal information (e.g. a signature, a check-off box, a verbal approval). Implied consent is consent that can be reasonably determined through the actions or inactions of the patient/person, for example, a patient/person presenting himself to a pharmacist, a laboratory, an emergency department, or a physician in private practice.[25] With "deemed" consent it does not matter whether the patient/person has actually consented; the law permits organisations to act as if the patient/person has consented; there is no right to withdraw or withhold consent. In contrast, all of those rights are present with implied consent. The assumption of reasonableness usually rests on how well the patient/person was informed about the intended collection, use, or disclosure of his or her personal information. An organisation should be able to demonstrate that it complied with applicable legislative requirements and that the patient/person had a reasonable opportunity to know that information was going to be collected and used for specific purposes and persisted with the action that resulted in the information flow.[26, 27]

It is assumed that based on jurisdictional requirements for consent that at least some POS systems connected to the EHRi may eventually have specific "consent fields" that will allow POS users to enter or "check-off" how consent was obtained, withdrawn or revoked in those cases where consent was required for specific activities. An interoperable EHR may therefore require the capturing of consent for the collection, use and disclosure of PHI in many ways. For example:

- An admission or appointment form may be used to seek consent, collect PHI, and inform patients/persons of the uses that will be made of their PHI;
- A check-off box may be used to allow patients/persons to request that their PHI not be shared with other organisations, the so-called "lock box" concept.[28] Patients/persons who do not check off the box are assumed to consent to the transfer of this information to third parties;
- Consent may be given orally; or
- Consent may also be given at the time that patients/persons use a health service.

A number of data protection laws have introduced a concept of a PHI "lock box", most recently, Ontario's *Personal Health Information Protection Act*. The EHRi must reflect legal obligations in its privacy requirements in all of their relative sophistication in this novel area. The ultimate obligation is to

[25] Canadian Standards Association, Making the CSA Privacy Code Work for You. A Workbook on applying the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830) to your organisation (Etobicoke, Ontario, December, 1996, ISBN 0-921347-57-X), p. 11. Ontario, *Personal Health Information Protection Act*, section 18(2) does not define express or implied consent.

[26] Perrin, Black, Flaherty, and Rankin, The Personal Information Protection and Electronic Documents Act: An Annotated Guide, pp. 28-29.

[27] Ontario, Personal Health Information Protection Act, section 18.

[28] See Ontario, *Personal Health Information Protection Act*, sections 37(1)(a), 38(1)(a), and 50(1)(e), as qualified by section 19(2): "cannot prohibit or restrict any recording of personal health information by a health information custodian that is required by law or by established standards of professional practice or institutional practice;" 20(3): "if the disclosing custodian does not have the consent of the individual to disclose all the personal health information about the individual that it considers reasonably necessary for that purpose;" and 38(2): "if an instruction of the individual made under that clause [38(1)(a)] prevents the custodian from disclosing all the PHI that the custodian considers reasonably necessary to disclose for the provision of health case or assisting in the provision of healthcare to the individual, the custodian shall notify the person to whom it makes the disclosure of that fact."

meet the wishes of the patient/person, in those circumstances where he or she is able to place express instructions on the allowable uses and disclosures of his or her PHI.[29]

Privacy Requirement 8 Obtaining Knowledgeable[30] Consent

Except where inappropriate (e.g. specifically exempted by law or professional code of practice), organisations connecting to the EHRi, and organisations hosting components of the EHRi **should** obtain the knowledge[31] and consent of each patient/person for the collection, use or disclosure of his or her PHI —and where required by law, **must**— obtain the knowledge and consent of each patient/person for the collection, use or disclosure of his or her PHI.[32]

Policy & Procedures

Admin Requirement

Rationale: There are legal requirements in all existing health data protection statutes as well as the Federal *Personal Information Protection and Electronic Documents Act* regarding consent. In addition to meeting these legal requirements, healthcare organisations should also seek to meet high ethical and moral standards for information consent, which is vital to the protection of privacy as an aspect of human dignity and the protection of human rights. Several regulatory colleges have advised their members to seek consent for the collection, use or disclosure

[29] Patients/persons are able to make express instructions concerning the allowable uses and disclosures of their PHI under sections 37(1)(a), 38(1)(a), and 50(1) of Ontario's *Personal Health Information Protection Act* (see also footnote 28). Section 22(2)(a) of the Manitoba *Personal Health Information Act* states that health information custodians may disclose PHI to a person providing healthcare to the patient/person, unless the patient/person states otherwise. Section 58(2) of the Alberta *Health Information Act* requires healthcare providers, in deciding how much health information to disclose, to consider as an important factor any expressed wishes of the patient/person who is the subject of the information relating to disclosure of the information, together with any other factors the custodian considers relevant.

[30] The use of the term "knowledgeable" in this requirement does not constitute endorsement of the knowledgeable consent required for the collection, use and disclosure of personal health information under the Ontario *Personal Health Information Protection Act. Infoway* recognizes that the rules for consent for the collection, use and disclosure of personal health information vary among jurisdictions; *Infoway* does not advocate one jurisdiction's consent rules over another.

[31] A consent is considered knowledgeable under section 18(5) of Ontario *Personal Health Information Protection Act* if it is reasonable in the circumstances that the patient/person knows: (a) the purposes of the collection, use and disclosure, as the case may be, and (b) that the individual may give or withhold consent. "Knowledgeable consent" is a different standard from "informed consent". The latter requires that the patient/person: (a) receives information about the purposes of the collection use and disclosure, the expected benefits of the collection, use and disclosure, the material risks of the collection, use and disclosure, alternative to the collection, use and disclosure, and the likely consequences of not permitting the collection, use and disclosure that a reasonable person in the same circumstances would encounter in order to make a decision about the treatment; and (b) receives responses to his or her requests for additional information about those matters.

[32] One of the fundamental requirements of consent is that the person providing consent must be competent to do so. As such, a substitute decision-maker is needed if the person who is the subject of the information is not able to provide consent when required under the legislation. The list of persons who are authorized to act as substitute decision-makers varies depending on the jurisdiction. Ontario has the most well developed scheme for substitute decision-making. Ontario's *Personal Health Information Protection Act* (sections 21-28) incorporates the hierarchy of substitute decision-makers found in the Health Care Consent Act. A patient has the right to apply to the Consent and Capacity Board for a review of a determination that he or she is incapable of providing consent.

of PHI.[33] The requirement to acquire patients/persons' knowledge and consent gives them an element of control over their PHI, but allows for this control to be overridden in specific circumstances for reasons of public or individual safety or ensuring the efficient operation of the healthcare system.

It is important to note that a patient/person may withdraw consent at any time, subject to legal or contractual restrictions.[34] In the healthcare setting, the withdrawal of consent may in fact make it impossible for a patient/person to receive, or continue to receive, healthcare.[35]

The requirement to obtain knowledgeable consent is an administrative requirements but there are associated technical requirements as well and these follow below (Privacy Requirement 9 to Privacy Requirement 13).

Privacy Requirement 9 Recording Consent in POS Systems

POS systems connected to the EHRi where required by law, **must** be able to record a patient/person's consent directives, including the withholding,[36] withdrawal or revocation of consent.[37]

Policy & Procedures

Admin Requirement

Tech Requirement

Rationale:

Healthcare organisations must know that they have obtained the consents required in their particular jurisdiction for the purposes for which they will collect, use or disclose PHI (see **Privacy Requirement 5**).

The form of the consent sought by organisations connecting to the EHRi may vary, depending upon the jurisdiction, circumstances under which the information was collected (e.g. medical emergencies) and the type of information (e.g. mandatory reporting of communicable diseases). In the Canadian EHR environment, the required forms of consent are largely established by various laws, most notably health data protection legislation and public sector privacy

[33] The Canadian Nurses Association's "Code of Ethics for Registered Nurses" (p.8) requires that, "Nurses safeguard information learned in the context of a professional relationship, and ensure it is shared outside the health care team only with the person's informed consent, or as may be legally required, or where the failure to disclose would cause significant harm."

[34] Note that consent cannot be withdrawn or revoked for a purpose permitted by legislation or in jurisdictions with a "deemed consent" model. Also, the revocation of consent does not commonly have a retroactive effect.

[35] Ontario, *Personal Health Information Protection Act*, section 19(1), for example, provides that a withdrawal of express or implied consent "shall not have retroactive effect."

[36] For the purposes of this document, withholding, withdrawing and revoking of consent include the patient/person placing restrictions on the uses and/or disclosures of his or her PHI – commonly referred to as a "lock box". Lock box provisions are included in the Manitoba *Personal Health Information Act* and the Ontario *Personal Health Information Protection Act* (see footnotes 28 and 29). However, these statutes also include provisions allowing for a patient/person's "lock box" instructions to be overridden. For example, a "lock box" could be overridden for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons (section 40(1), Ontario *Personal Health Information Protection Act*). The ability for a patient/person to restrict uses and disclosures of his or her PHI, while allowing these instruction to be overridden in certain circumstances, is commonly technically implemented through what is called a "masking" and "unmasking" mechanism.

[37] As an interim solution, jurisdictions may choose to deploy standalone consent processes, such as a separate "consent application" or a "consent call-centre." Although these processes may provide individuals with the opportunity to express their consent directives with no impact on legacy POS systems, Infoway believes that, in order to ensure system efficiency and effectiveness, future POS systems should include the ability to record an individuals' consent directive.

legislation. Those entering PHI into a POS system within a particular jurisdiction have the primary obligation of obtaining and recording the consent directives of patients/persons. The POS system has to ensure that those accessing this PHI only obtain access to information that is legitimately available on the basis of consent or legal authorization to use or disclose (e.g., auditing or law enforcement).

See also **Privacy Requirement 10** for the technical implications of handling consent and **Privacy Requirement 11** for an analogous requirement for recording consent in the EHRi.

Privacy Requirement 10 Associating Consent with PHI in POS Systems

Where POS systems connected to the EHRi record a patient/person's consent directives, including the withholding, withdrawal or revocation of consent, such POS systems **must** transmit these consent directives to the EHRi, in a consistent form, whenever they transmit the associated PHI to the EHRi.

Policy & Procedures

Admin Requirement **Tech Requirement**

Rationale: Not all jurisdictions will require POS system to collect consent directives. Where these directives are collected, it is essential that they be transmitted to the EHRi whenever the associated PHI is to be transmitted. This will ensure proper EHRi processing of these consent directives prior to transmission of PHI to another jurisdiction. Note that this shifts the burden of ensuring compliance with the regulations of other jurisdictions from the POS system to the EHRi – a reasonable approach given the large number of jurisdictions and the varied complexities vis-à-vis consent among them.

The standards and formats of such consent data is beyond the scope of this document, but will be discussed further in the future "Privacy and Security Standards Assessment" and the "Privacy and Security Services" deliverables (see Section 2.2 "Context for privacy and security requirements analysis**").**

Privacy Requirement 11 Recording Consent in the EHRi

The EHRi where required by law, **must** be able to record a patient/person's consent directives, including the withholding, withdrawal or revocation of consent[36] and **must** be able to do so in a way that allows each jurisdiction to comply with its own legal requirements on consent.

Policy & Procedures

Admin Requirement **Tech Requirement**

Rationale: Healthcare organisations must be able to determine if a patient/person has provided or withheld consent as required in their particular jurisdiction. Consequently, those organisations wishing to disclose PHI to another jurisdiction must do so in a manner that respects the legal requirements for consent in their own jurisdiction (i.e. the jurisdiction of the disclosing organisation). As a practical matter, a healthcare organisation wishing to access PHI from *another* jurisdiction must do so in a manner that respects the legal requirements for consent to disclose PHI in the jurisdiction of the organisation that holds the data as well as satisfy all the legal requirements for consent to access PHI in its own jurisdiction. (Otherwise the sender cannot honour the access request). This has profound implications for the interoperability of the EHRi. Information contained within a patient/person's EHR may carry with it the legal requirements for consent from multiple jurisdictions (see **Privacy Requirement 12**). Before permitting accesses to PHI, the EHRi must ensure that all necessary legal requirements are upheld before transmitting data to a requestor.

As noted above, the format of such consent data is beyond the scope of this document, but will be discussed fully in the future "Privacy and Security Standards Assessment" and the "Privacy and Security Services and Components" deliverables (see Section 2.2 "Context for privacy and security requirements analysis**").**

See also **Privacy Requirement 12** for the technical implications of handling consent.

Privacy Requirement 12 Associating Consent Directives with PHI in the EHRi

When consent is required by law, whenever receiving, storing, processing, or transmitting PHI, the EHRi **must** be able to:

a) maintain the association between this data and the consent directives under which it may be used or disclosed;

b) process these consent directives before transmitting the associated data and block the transmission where it would violate the directives and where no exception for such a disclosure is outlined in law; and

c) notify the requestor whenever data is blocked as in b) above.

Admin Requirement

Tech Requirement

Rationale: This will allow organisations connecting to the EHRi, or hosting components of the EHRi, to *apply* a patient/person's consent directives in their jurisdiction as well as across jurisdictions. EHRi and systems connecting to the EHRi will also need a consistent representation of consent and masking/lockbox directives in support of interoperability requirements within and ultimately between jurisdictions.

See also the rationale for **Privacy Requirement 9**.

Privacy Requirement 13 Logging the Application of Consent Directives

The EHRi **must** be able to:

a) log when the processing of consent directives (cf. **Privacy Requirement 12**, item b) prohibits the transmission of data;

b) log the identity of any user who overrides a patient/person's consent directives, the reason for the consent override, and the date and time when the consent override occurred. and

c) alert the individual accountable for facilitating privacy compliance in the organisation where the accessing user works as well as in the organisation where the information was collected that such a consent override has occurred.

Tech Requirement

Rationale: Since some health data protection laws, like Ontario's *Personal Health Information Protection Act*, allow both masking, unmasking, and notice of existing masking to third parties, the EHRi and POS systems connected to the EHRi will need to track by means of an audit log the identify of anyone who unmasks or unlocks a record (see **Security Requirement 38** and **Security Requirement 43**).

Furthermore, some health data protection legislation requires that health information custodians notify a patient/person if his or her information is stolen, lost, or accessed by unauthorized persons.[38] The individual(s) responsible for facilitating an organisation's privacy compliance will be greatly assisted in determining when a potential "unauthorized" access or disclosure of PHI has taken place if they are notified when an individual's consent directives are overridden. Overriding of a patient/person's consent directives must be monitored in both the organisation where the PHI has been collected and the organisation from which the information is being accessed.[39]

As logs will themselves contain confidential information, they must be made both secure and tamper-proof. Their security requirements are discussed in **Security Requirement 50** (**Securing Access to EHRi Audit Logs**) and **Security Requirement 51** (**Making EHRi Audit Logs Tamper-Proof**).

In addition to logging overrides of a patient/person's consent directives (Item b in the list above) and alerting accountable individuals that a consent override has occurred (item c in the list above), there is also a related requirement to notify patients/persons when access has been deemed inappropriate (see **Privacy Requirement 20**).

See also **Privacy Requirement 11** and **Privacy Requirement 12**.

Privacy Requirement 14 Implications of Consent Directives

Organisations connecting to the EHRi or hosting components of the EHRi **should** ensure patients/persons are informed about the potential implications of their consent directives, including directives for locking or masking PHI.

Policy & Procedures

Admin Requirement

[38] Ontario, Personal Health Information Protection Act, section 12(2)

[39] This complex situation is further exacerbated in the context of primary care physicians who, in jurisdictions where health data protection legislation exists, may be responsible for facilitating his or her own privacy compliance.

Rationale:

When a patient/person elects to place restrictions on the use or disclosure of his/her PHI, there is a potential that they are putting their own safety or the safety of others at risk. Healthcare providers require all relevant PHI from a patient/person's medical history in order to definitively diagnose and safely treat a patient/person. Therefore, when patients/persons request that their healthcare provider mask or lock components of their PHI, it may not be possible for their healthcare team to provide appropriate care. The potential negative outcomes associated with locking or masking PHI relevant to a patient/person's care include misdiagnosis, adverse drug events or even healthcare providers refusing to provide care.[40] These implications should be explained by qualified healthcare professionals to patients/persons in order to ensure that their full knowledge and consent is obtained (see Privacy Requirement 8).

The fulfillment of this requirement will also work to protect healthcare providers from litigation associated with any negative outcomes related to the withholding or masking of PHI.

See also **Privacy Requirement 8.**

Privacy Requirement 15 Recording Identity of Substitute Decision Makers

Where required to do so by law ,the EHRi and POS systems connected to the EHRi **must** have the ability to indicate when consent is given on behalf of a patient/person by a substitute decision maker (e.g. consent given by an authorized representative), as well as identify this substitute decision maker and the substitute decision maker's relation to the patient/person.

Admin Requirement **Tech Requirement**

Rationale:

Consent can be given not only by a patient/person but also be given by an authorized representative (such as a legal guardian, a substitute decision maker, or a person having power of attorney). Establishing capacity to consent and providing for substitute decision-making are two of the most complex aspects of data protection. Provincial and territorial laws govern these activities.[41]

The determination of an individual's substitute decision maker is typically a ranking process whereby if no individual fitting the first role/relationship in the list (e.g. spouse or guardian) can be found, then the custodian must attempt to locate the next potential substitute decision maker in the ranking process (e.g. sibling). When a suitable substitute decision make has been found, the custodian must document the relation of that substitute decision maker to the patient/person to ensure that the custodian's selection can later be audited, justified, or reappraised.

[40] The College of Physicians and Surgeons of Ontario states the following with regards to patients/persons who lock components of their medical history, "The College believes that patient safety should always remain paramount. As such, in non-emergency situations, physicians are not obliged to accept or treat a patient about whom they have insufficient information. Physicians are advised to speak directly to their patients about the consequences of their decision to withhold health information. It is very possible that a patient, who has chosen to withhold personal health information may agree to disclose the information in the context of a specific health encounter and a specific, identified physician. When patients decide to maintain their decision, and not divulge their personal health information, physicians may wish to attempt to obtain the necessary information by taking a thorough medical history." Full details available at: http://www.cpso.on.ca/Publications/Dialogue/1104/privacy.htm

[41] See, for example, Ontario, Personal Health Information Protection Act, section 21-28.

See also **Privacy Requirement 8**.

Privacy Requirement 16 No Coerced Consent

Organisations connecting to the EHRi and organisations hosting components of the EHRi **must not**, as a condition of the supply of a service, require a patient/person to consent to the collection, use or disclosure of PHI beyond that required to fulfill the explicitly specified and legitimate purposes.

Policy & Procedures

Admin Requirement

Rationale: In the healthcare context, there is a great deal of case law on the "imbalance of power" between the healthcare provider and patient. As such, rules for collection, use and disclosure should be strictly delineated and observed because patients will often not object to certain PHI collections, uses and disclosures in light of "vulnerable" health circumstances. In the rare circumstances where a patient withdraws or withholds consent and the healthcare provider believes that care cannot be provided safely, the healthcare provider may determine that it is appropriate to refuse to provide treatment.[42]

4.4 Limiting collection of personal health information

As outlined in **Privacy Requirement 5**, organisations connecting to the EHRi and organisations hosting components of the EHRi should limit collection of PHI to that which is necessary for the identified purposes. PHI should not be collected indiscriminately. In an EHR environment, the use of electronic forms to gather personal information should facilitate a process of only collecting necessary information and, for example, clearly indicating when the provision of personal information is optional. A caveat is that healthcare providers may collect any information deemed relevant to the purposes stated to patients/persons and then ensure that it is only used and disclosed on a "need to know" basis.

Privacy Requirement 17 Collecting Information by Fair and Lawful Means

Organisations connecting to the EHRi, and organisations hosting components of the EHRi **must not** collect PHI by misleading or deceiving patients/persons or healthcare providers about the purposes for which information is being collected.

Policy & Procedures

Admin Requirement

Rationale: Personal information must not be collected by unfair or illegal means. The antidote is fully informing patients/persons and providing appropriate notices of intended purposes for data collection, use, and disclosure. If, for example, contact tracing is a potential consequence of a lab test and a mandatory one, then patients/persons should receive this information.

4.5 Limiting use, disclosure and retention of personal health information

When organisations identify the purposes for which they collect PHI (**Privacy Requirement 5**) and seek the appropriate consent for these purposes (**Privacy Requirement 8**), it is imperative that they then only use, disclose and retain information for these purposes. In many cases in health care, the content of records of PHI, as well as record retention periods, are mandated by statute, regulations and various bylaws for healthcare professionals.[43]

[42] See Industry Canada's PIPEDA Awareness Raising Tools (PARTs) Initiative For The Health Sector, available at: http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00235e.html

[43] For example, PHI collected through the course of a clinical trial must be retained for a period of 25 years (Food and Drug Regulations - Sections C.05.010, C.05.011 and C.05.012)

In addition, the distinction between use and disclosure is also highly relevant.[44] Use refers to any processing and treatment of data within the organisation, whereas disclosure refers to the release of the information to third parties (outside of the originating organisation, even in an EHR environment).[45]

[44] See Perrin, Black, Flaherty, and Rankin, The Personal Information Protection and Electronic Documents Act: An Annotated Guide, p. 33.

[45] Note to reader: this may be modified by statute. For example, the Ontario *Personal Health Information Protection Act* contains numerous provisions about a "health information custodian" sharing information with "agents" of the custodian.

Privacy Requirement 18 Limiting Use and Disclosure of Personal Health Information to Identified Purposes

Organisations connecting to the EHRi and organisations hosting components of the EHRi **must only** use or disclose PHI for purposes consistent with those for which it was collected, except with the consent of the patient/person or as permitted or required by law.[46]

Policy & Procedures

Admin Requirement **Tech Requirement**

Rationale: The Alberta *Health Information Protection Act,* Manitoba *Personal Health Information Protection Act* and Ontario *Personal Health Information Act* all require that custodians of PHI only collect, use or disclose as much PHI as is reasonably necessary to carry out the identified purposes. For more information, see "duty to collect, use or disclose in a limited manner" in Appendix B below.

Also, this requirement is a standard and traditional fair information practice and, in places where health data protection legislation has been introduced, does not impede upon custodians' ability to provide care. Theses statutes typically permit or require a number of uses and disclosures of PHI related to provision of healthcare, supporting the operation of the healthcare system, or ensuring public health;[47] such legislative provisions vary by jurisdiction.

In section 45.9 (Access Control), a variety of security requirements are stated that provide roust access control to the EHRi and the PHI it contains. These requirements will greatly assist in operationalizing the limitation of use and disclosure of this PH to authorized users with appropriate roles and privileges.

Privacy Requirement 19 Logging Access, Modification, and Disclosure

The EHRi and POS systems connected to the EHRi **must:**

a) have a mechanism to record every access, modification or disclosure of PHI, together with the time and identity of the accessing user;

b) have a mechanism to record every access, modification or disclosure of provider and user registration data[48], together with the time and identity of the accessing user; and

Tech Requirement

[46] It was determined through the document consultation process that no effective technical means currently exists to limit the uses and disclosures of PHI to identified purposes. The development of such a solution would need to take into account a number of issues, including the following: the identification of purposes will need to be harmonized or standardized; a means of associating the identified purposes with the PHI will need to be established; a means to check the purposes that PHI will be used or disclosed for against those identified at the time of collection will need to be established; and, a means by which PHI would be blocked where the purpose for which the PHI will be used or disclosed are not consistent with those purposes identified will need to be established.

[47] See, for example, Ontario, *Personal Health Information Protection Act*, sections 31-33, 37-50 dealing with at least fifteen types of uses and disclosures.

[48] Provider and user registration information includes data about identifiable healthcare providers and other EHRi users, such as their names, addresses, practice license information, and other user registration information. Provider registration information would not constitute personal health

c) where required by law, have mechanisms to alert the organisation’s individual accountable for privacy (see **Privacy Requirement 1**) when it is suspected that PHI has been accessed, used or disclosed inappropriately.

Rationale: Specific legislation requires organisations to record access, modifications, and disclosures of PHI.[49] Where such accesses, uses and disclosures fall outside of what is permitted by the EHRi, individuals accountable for privacy compliance need to be alerted.

Logs of access, modification and disclosure will themselves contain confidential information and must therefore be made both secure and tamper-proof. Their security requirements are discussed in **Security Requirement 38** through **Security Requirement 52**. Also see **Privacy Requirement 13** for the logging of consent directives.

Privacy Requirement 20 Notifying Patients/Persons of Inappropriate Access, Use or Disclosure

Organisations hosting components of the EHRi and organisations connecting to the EHRi **should** notify patients/persons when it is determined that his or her PHI has been inappropriately accessed, used or disclosed in accordance with applicable laws, regulations and organisational policies and procedures.

Policy & Procedures
Admin Requirement

Rationale: The latest health privacy law, Ontario’s *Personal Health Information Protection Act*, perhaps in anticipation of an enhanced electronic health record environment, makes provision for notification.[50]

Privacy Requirement 21 Retaining Records

The EHRi, POS systems connected to the EHRi, organisations connecting to the EHRi, and organisations hosting components of the EHRi:

a) **must** retain PHI in accordance with record-keeping requirements outlined in legislation; and

b) **should** develop guidelines and implement procedures with respect to the retention of PHI, including minimum and maximum retention periods.

Policy & Procedures
Admin Requirement

Tech Requirement

Rationale: This is perceived to be a heavy burden in legacy or paper based systems; the electronic health record environment should be designed to implement such rules systematically. At the same time, patients/persons need to recognize the need of the healthcare system to hold certain core information about them on a more permanent basis.

See also **Security Requirement 22** and **Security Requirement 35.**

information, unless the information relates directly to the provision of healthcare to an identifiable patient/person.

[49] Manitoba, Personal Health Information Regulations, section 4(1), and Ontario, Medicine Act Regulations, section 20(5).

[50] Ontario, Personal Health Information Protection Act, section 12(2)

4.6 Accuracy of Personal Health Information

The requirement for accuracy as a fair information practice has particular relevance for the delivery of healthcare to patients/persons, who share with organisations a commitment to accuracy in order to ensure efficient and effective delivery of healthcare. The goal for healthcare organisations is to have PHI that is sufficiently accurate, complete and up-to-date to minimize the possibility that inappropriate PHI may be used to make a decision about a patient/person.

Privacy Requirement 22 Accuracy

The EHRi, POS systems connected to the EHRi, organisations connecting to the EHRi and organisations hosting components of the EHRi **must** take reasonable steps or make a reasonable effort to:

a) ensure that PHI is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used, including disclosures of PHI to third parties; and

b) accurately identify a patient/person when accessing or modifying his or her PHI

Admin Requirement

Tech Requirement

Rationale: An electronic health record environment should facilitate the achievement of better quality records by building in automatic checks on data entry and making it easier to update even the most basic demographic and location information on any patient/person.

In addition, it is of critical importance for patient safety and a number of other reasons, including the overall success of the EHRS, that EHRi users accurately identify patients/persons prior to accessing or modifying their PHI.

See also **Security Requirement 77**.

4.7 Safeguards for the protection of personal health information

The EHRi, organisations connecting to the EHRi, and organisations hosting components of the EHRi **must** protect PHI, through the application of appropriate security safeguards, against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Most of these requirements are dealt with in detail in Section 5 of this document**.**

Concern for physical and system security has always been at the core of data protection and it will be of special importance in a developed electronic health record system, since the risks of a breach of security can be so devastating for the patient/person. One particular reason to take all aspects of security seriously for an EHRi is that once sensitive personal information has been disclosed, it is almost always impossible to “put the genie back into the bottle”. The damage to the patient/person has happened and is likely irreparable. The organisation may then be subject to complaints to an oversight body, adverse publicity, fines and/or prosecution.[51]

[51] See Ontario, *Personal Health Information Protection Act*, sections 65 (damages for breach of privacy), 72 (offences).

Privacy Requirement 22a Denoting Patients/Persons At Elevated Risk

The EHRi **must** provide functions for marking records of selected patients/persons[52] and subsequently making accesses to such data subject to mandatory auditing by the individual accountable for privacy compliance in the organisation.

Tech Requirement

Rationale:

This requirement greatly facilitates the determination of suspicious or wrongful use of access privileges with regard to patients who are high profile or whose confidentiality is otherwise especially at risk.

The records of certain patients/persons (e.g. celebrities, politicians, and newsmakers) may be at elevated risk of access by those who do not have a need-to-know. It may therefore be prudent to place additional audit controls on these records to protect patient privacy. The EHRi should recognize this practical reality and facilitate the rapid and regular audit of access to these records (perhaps involving notification to a privacy officer on each access).

This requirement should *not* be construed as meaning that the information in the records of such patient/persons are somehow more confidential than those of ordinary citizens or that these records, as information assets, are more valuable than those that are not at elevated risk of inappropriate access. Rather, the requirement ensures that the capability exists to rapidly identify prurient interest by users who lack a legitimate need-to-know.

See **Security Requirement 49** for audit logging requirements related to this privacy requirement.

Privacy Requirement 22b Training Users and Raising Privacy Awareness

All organisations hosting components of the EHRi or connecting to the EHRi **must** ensure that privacy education and training and regular updates in organisational privacy policies and procedures are provided to each permanent or temporary employee or third-party contractor who is a registered user of a POS connected to the EHRi or who has access to hosted components of the EHRi.

Policy & Procedures

Admin Requirement

Rationale:

Organisations connecting to the EHRi and organisations hosting components of the EHRi need to make their employees aware of the importance of maintaining the privacy of PHI. Training on an ongoing basis is absolutely essential for achieving all aspects of privacy. Also, as a best practice, such training should be complemented by a readily available list of frequently asked privacy questions and answers. While large organisations like hospitals may find it relatively easy to design such training, the problems are even more difficult when it comes to small operations like individual pharmacies, nursing stations in remote communities, and the offices of private physicians, where the physician is often the only healthcare professional on staff. Organisations should undertake departmental site visits on a continuing basis to test the awareness of their staff of privacy, data protection, and security obligations. Failure to do so could hinder the future success of electronic health records development.

See also security section 5.6.2.1 (Information Security Awareness, Education and Training).

[52] Examples of such patients might include cabinet ministers, celebrities and public figures, patients/persons receiving police protection, and others whose personal data could be especially at risk (either from users who are merely curious or from those who have malicious intent.

4.8 Openness about practices concerning the management of personal health information

This section is closely related to the ‘accountability’ privacy requirements discussed in Section 4.1 above. The intent of this section is to make it possible for concerned members of the public to know the purposes for collecting, using, and disclosing PHI about them. Privacy oversight bodies (e.g. Information and Privacy Commissioners) may also want assurance that healthcare organisations have privacy management plans in place.

Privacy Requirement 23 Openness

Organisations connecting to the EHRi, and organisations hosting components of the EHRi **must** make readily available to the public specific information about their policies and practices relating to the management of PHI.

At a minimum, these organisations **should** make available, by appropriate means, the following information, in accordance with applicable legislation:

a) the name or title, and the address, of the person who is accountable for the organisation’s policies and practices and to whom complaints or inquiries can be forwarded (see **Privacy Requirement 1**);

b) the means by which patients/persons can gain access to PHI held by the organisation to which they are authorized to access (see **Privacy Requirement 24**);

c) a description of the personal information held by the organisation, including a general account of the manner in which the organisation obtains consent; the purposes for collecting, using, and disclosing PHI; the limitations on PHI collection, use, disclosure, and retention; and how the organisation maintains the accuracy of this information;

d) a general description of the administrative, technical and physical safeguards and practices the organisation maintains with respect to PHI; and

e) what PHI is made available to related organisations.

Policy & Procedures

Admin Requirement

Rationale: In the spirit of openness that this privacy requirement embodies, members of the public must be able to acquire information about the management of PHI within the EHRi, at organisations connecting to the EHRi, or at organisations hosting components of the EHRi without unreasonable effort and in a form that is generally understandable to them.

While the list above is not exhaustive, it is a helpful indication of the ways in which organisations involved in the EHRi can promote accountability and an informed clientele over time. While they cannot force patients/persons to read the material made available to them, the participating organisations are reminded by this checklist of the various ways it can reduce anxieties about privacy and security.

4.9 Individual access to personal health information

Historically, there was doubt as to whether patients should be entitled to have access to their own PHI. It was argued that allowing patients access to their own records would lead to unfounded lawsuits, that patients would not understand their records, that physicians would be deterred from keeping complete and frank records, and that records could be harmful to patients. It is now well established that patients have a legal right of access to their own health information, subject to limited exceptions in specified circumstances.[53]

[53] *McInerney v. MacDonald*, [1992] 2 S.C.R. 138 at 155-57.

In certain situations, the EHRi, organisations connecting to the EHRi, or organisations hosting components of the EHRi may not be able to provide access to all the PHI it holds about a patient/person. Exceptions to the access requirements should be limited and specific.[54] The reason for denying access should be provided to the patient/person. Exceptions may include information that is prohibitively costly to provide,[55] information that contains references to other individuals (third parties),[56] information that cannot be disclosed for legal, security, or commercial proprietary reasons,[57] information that is subject to solicitor-client litigation privilege[58], and cases where healthcare organisations have the legal right to transfer access requests to other parties.

Complying with access requests is not intended to pose an unreasonable burden on healthcare organisations,[59] but there are important differences in legal requirements between jurisdictions. For example, note that under the Alberta *Health Information Act*, a health information custodian that discloses PHI must make a note of the name of the person to whom the custodian disclosed the information; the date and purpose of the disclosure; and a description of the information disclosed. The information must typically be retained for a period of 10 years following the date of disclosure. The patient has a right of access to this information.

Privacy Requirement 24 Patient/Person Access

Organisations connecting to the EHRi and organisations hosting components of the EHRi **must**, upon request**:**

a) inform a patient/person of the existence, use and disclosure[60] of his or her PHI and shall give the patient/person direct access to that PHI where such access is not prohibited by legislation;[61]

b) respond to requests for access to a patient/person's PHI within a reasonable time and make it available in a form that is generally understandable; and

c) allow a patient/person to challenge the accuracy and completeness of his or her PHI and have it amended as appropriate.

Policy & Procedures

Admin Requirement

Rationale: This fair information practice provides each patient/person with an almost unlimited right of access to his or her personal information as a matter of respect for human dignity and the protection of human rights. This is especially important

[54] The Supreme Court of Canada determined in *McInerney* v. *MacDonald* that individuals have a right of access to their own PHI held by a physician.

[55] The Industry Committee of the House of Commons removed such an exemption from PIPEDA (Perrin, Black, Flaherty, and Rankin, The Personal Information Protection and Electronic Documents Act: An Annotated Guide, p. 40).

[56] PIPEDA, section 9(1).

[57] PIPEDA, sections 9(3)(b), (c). and (c.1); Ontario, *Personal Health Information Protection Act*, sections 52(1)(b) and (c).

[58] PIPEDA, section 9(3)(a); Ontario, *Personal Health Information Protection Act*, section 52(1)(a).

[59] Ontario, *Personal Health Information Protection Act*, section 54(6), for example, allows a health information custodian to refuse a request if it has "reasonable grounds" to believe is "frivolous or vexatious or is made in bad faith…."

[60] The record of uses and disclosures of a patient/person's PHI is made up of information logged in compliance with **Security Requirement 38**.

[61] For acceptable reasons to reject access request under law, see Alberta *Health Information Act* section 11, British Columbia *Freedom of Information and Protection of Privacy Act,* sections 12-22, Manitoba *Personal Health Information Act*, section 11(1), Ontario *Personal Health Information Protection Act,* section 52, Saskatchewan *Health Information Protection Act* section 38.

in the healthcare context where patients/persons are expected to divulge such sensitive personal information to their healthcare providers. Patients/persons thus have a right to check that the information being used to treat them is accurate. This right will be even more important in an electronic healthcare environment, where so much information about any patient can be readily assembled. This access right is one check against mistakes that could harm a patient. As discussed further below, the patient/person also has a right to challenge factual errors in particular (see **Privacy Requirement 25**).

This right of access includes as well the right of the patient/person to be told what information the organisation holds about him or her and how it has been used. These rights were discussed above in connection with the privacy requirements under “Identifying Purposes” and “Limiting Use, Disclosure, and Retention.”

Privacy Requirement 25 Amending Inaccurate or Incomplete Information

Organisations connecting to the EHRi and organisations hosting components of the EHRi **should**:

a) amend PHI when a patient/person successfully demonstrates the inaccuracy or incompleteness of this information;

b) notify EHRi users that have accessed the information in question that the information has been amended when the amended information can reasonably be expected to have effect on the ongoing treatment of the patient/person;

c) record the substance of the unresolved challenge when the organisation disagrees with the patient/person's assessment of incompleteness or inaccuracy; and

d) transmit the existence of the unresolved challenge to EHRi users accessing the information in question.

Policy & Procedures

Admin Requirement

Tech Requirement

Rationale:

Decisions made by Information and Privacy Commissioners (or their equivalents across Canada) have resulted in jurisprudence that emphasizes that only factual errors can be literally corrected, such as a birth date. Matters of opinion are exactly that, including a diagnosis by a healthcare professional that a patient/person wishes to contest. The issue of correction, deletion, or addition is especially relevant if the information can make a possible difference in the treatment of a person or in decisions made about him or her.[62] Depending upon the nature of the information challenged, amendment may involve the correction, deletion, or addition of information.

Some corrections, deletions, or amendments will have a particular relevance to the ongoing healthcare of a patient/person, and they should be made known

[62] Ontario, *Personal Health Information Protection Act*, section 58(8) establishes a limited duty to correct “if the individual demonstrates, to the satisfaction of the custodian, that the record is incomplete or inaccurate for the purposes for which the custodian uses the information and gives the custodian the information necessary to enable the custodian to correct the record.” But there is no obligation to correct a record that “consists of a professional opinion or observation that a custodian has made in good faith about the individual (section 58(b).

appropriately.[63] Fortunately, a developed electronic health record system will automatically distribute the most up to date information when it is required for authorized purposes.

4.10 Challenging compliance

The right of any patient/person to lodge a privacy complaint has been a core fair information practice for thirty years.

Privacy Requirement 26 Challenging Compliance

Organisations connecting to the EHRi, and organisations hosting components of the EHRi **must** give patients/persons the right to address a challenge concerning compliance with these requirements to the designated individual or individuals specified in **Privacy Requirement 1**.

Policy & Procedures

Admin Requirement

Rationale: To give effect to privacy requirements like **Privacy Requirement 3** and **Privacy Requirement 7** patients must be able to challenge an organisation's compliance with those requirements.

Privacy Requirement 27 Complaint Procedures

Organisations connecting to the EHRi and organisations hosting components of the EHRi **must**

a) put easily accessible and simple-to-use procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of PHI;

b) inform complainants and inquirers of the existence of these procedures

c) treat all received complaints as confidential.

Policy & Procedures

Admin Requirement

Rationale: Healthcare organisations should respond positively and informatively to complaints and questions, and may consider using their designated contact person or persons for this function. The preparation of Frequently Asked Questions and making them readily available is an important first step in avoiding complaints and questions in the first instance.

Even if healthcare organisations seek to manage complaints locally and internally by sophisticated mechanisms for their resolution, they should still inform complainants if they have a right to make a privacy complaint to the provincial or territorial Information and Privacy Commissioner (or equivalent).[64]

[63] See the approach adopted in Ontario, *Personal Health Information Protection Act*, section 55(1).

[64] This is a requirement under the "written public statement" provisions in the Ontario *Personal Health Information Protection Act* (section 16).

Privacy Requirement 28 Investigation

Organisations connecting to the EHRi and organisations hosting components of the EHRi **must** investigate all privacy related complaints. If a complaint is found to be justified, the EHRi, organisations connecting to the EHRi and organisations hosting components of the EHRi **should** take appropriate measures, including, if necessary, amending their policies and practices and notifying the complainant of actions taken.

Policy & Procedures

Admin Requirement

See also section 5.8.10.1 Audit Logging for a discussion of the requirements pertaining to audit logging and section 5.11.1 (Reporting Incidents And Weaknesses) for a discussion of security incident reporting and handling. These latter requirements greatly facilitate timely and thorough investigation of privacy related complaints.

Rationale: Privacy complaints must be taken seriously. Since so many aspects of data protection are now regulated by detailed laws and regulations, a number of complaints will be answered by informing the complainant of what the law requires an organisation to do in specific circumstances. If a complainant wants to change the law, other available avenues exist.

5 Security requirements

5.1 Introduction

ISO/IEC 17799-1:2000 *Code of Practice for Information Security Management* is a widely adopted international standard for information security management. In December 2000, it was adopted by the International Standards Organisation (ISO) from an existing British standard (BS 7799) published by the British Standards Institute. The ISO/IEC 17799 Code of Practice opens with an Introduction describing Information Security, why it is needed, how to assess security requirements and how to assess risks and assign controls. The remainder of the standard is organised into ten sections, each covering a key control area for information security. Together these provide the working objectives of the Code of Practice. ISO will shortly publish a revised version (ISO/IEC 17799-1:2004) that includes among its revisions, an eleventh key control area: security incident management.

In this section on security requirements, the current document follows the format of the revised standard, 17799-1:2004. This revised standard is expected to be published by ISO prior to the conclusion of this project. All eleven security control objectives are therefore covered in the sections that follow:

1. security policy,
2. organising information security,
3. asset management,
4. human resources security,
5. physical and environmental security,
6. communications and operational management,
7. access control,
8. information systems acquisition, development and maintenance,
9. security incident management,
10. business continuity management, and
11. compliance.

At a minimum, five activities need to be carried out by an organisation hosting components of the EHRi in order to satisfy the requirements of 17799:

- an appropriate management structure within the organisation (e.g.: a committee, a management forum, or a management hierarchy) must assume responsibility for setting and enforcing organisational security policy and for managing privacy, security and business continuity risks (see section 5.4);
- a security policy must be created, promulgated and enforced by administrative and technical means (see section 5.3);
- privacy, security and business continuity risks must be analysed by means of a Threat and Risk Assessment (see section 5.2) and those risks must be managed against the objectives set by the security policy;
- compliance with the security policy must be assessed on an ongoing basis (see section 5.13);
- privacy, security and business continuity risks must be re-analysed when significant changes are made to the components of the EHRi that the organisation is hosting (see section 5.2).

All of the security requirements below are predicated on the assumption that organisations will take seriously their obligation to perform these five activities and that they will be diligent in carrying them out.

5.2 Risk Management

Risk assessment is an essential feature of ISO/IEC 17799. The interested reader can find examples of risk assessment methodologies in ISO/IEC TR 13335-1 (*Guidelines for the Management of IT Security: Techniques for the Management of IT Security*).

An organisation needs to implement a risk management process within the organisation. This process needs to have the support and commitment of the highest levels of management within the organisation; otherwise it will be difficult to implement and to enforce. Responsibilities for information risk management throughout the organisation will need to be assigned. Key organisational objectives in matters related to information risk management will need to be defined. Risk management processes will then need to be put in place to assess, manage and mitigate risk on an ongoing basis.

An essential step in mitigating risks associated with information systems such as the EHRi is to perform a threat and risk assessment.

Security Requirement 1 Threat and Risk Assessment

Organisations hosting components of the EHRi **must** – and origanisations connecting to the EHRi **should** – assess threats and risks to these components by careful review of a Threat and Risk Assessment (TRA). At a minimum such a TRA **must** include:

a) an inventory of all information assets supporting the EHRi components – including data, services, and technology – that must be protected and a determination of which assets include PHI;

b) an assessment, for each information asset, of how critical it will be to maintain the confidentiality, integrity, and availability of the asset, and accountability for the asset;

c) a vulnerability analysis, including a comprehensive listing of the privacy and security vulnerabilities of the hosted EHRi components a listing of the actual or planned safeguards that can protect against those vulnerabilities;

d) a risk analysis that determines the residual risk after actual or planned safeguards are put in place;

e) a recommendation of whether residual risk is to be:

   i) further reduced (by adding specific safeguards to the system or scaling back system functionality),

   ii) transferred to a third party, or

   iii) accepted by the organisation.

Policy & Procedures

Admin Requirement

Rationale: A Threat and Risk Assessment (TRA) is needed identify, quantify, and prioritize risks against criteria for risk acceptance. The results will determine priorities for managing information security risks and for implementing controls selected to protect against these risks. A TRA includes a systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against various criteria to determine the significance of the risks (risk evaluation). A TRA allows these risk assessments to be undertaken in a methodical manner capable of producing comparable and reproducible results.

A TRA should also be updated periodically to address changes in security requirements, changes in the risk situation, and when significant changes occur.

5.3 Security policy

The objective of a security policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. ISO/IEC 17799 considers security policy to be an essential tool in providing a clear, written framework from which to effectively implement and administer IT security.

Security Requirement 2 Security Policy

Organisations connecting to the EHRi or hosting components of the EHRi **must** have a written IT security policy that is approved by management, published, and communicated to all employees and relevant external parties.

Admin Requirement

Rationale: This requirement addresses the need to accept responsibility for security within organisations that are health information custodians, trustees and/or suppliers of health infostructure services . It also follows directly from **Privacy Requirement 3**.

5.4 Organising information security

The objectives of organising information security are to:

1. manage information security within an enterprise;
2. maintain the security of organisational information processing facilities and information assets accessed by third parties; and
3. maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

Management responsibility for security is essential for organisations storing, transmitting or processing PHI. This is especially true for organisations that will rely upon managed services provided by third parties. Effective coordination is also an essential ingredient in maintaining information security. Both require an explicit security management infrastructure.

5.4.1 Internal organisation

5.4.1.1 Management commitment to information security, co-ordination, and allocation of responsibilities

Security Requirement 3 Information Security Management, Co-ordination, and Allocation of Responsibilites

Organisations connecting to the EHRi and hosting components of the EHRi **must:**

a) clearly define and assign information security responsibilities; and

b) ensure that Information security activities relating to the EHRi are co-ordinated by representatives from different parts of the organisation who have relevant roles and job functions.

Policy & Procedures

Admin Requirement

Privacy Requirement 1 on page 20 effectively addresses the need to assign responsibility for privacy within organisations who are health information custodians and/or suppliers of health infostructure. It also addresses the need to assign responsibility for security within organisations whose employees are accessing PHI. The requirement above does the same for security[65].

Rationale: In addition to complementing **Privacy Requirement 1**, this security requirement is necessary to meet the legal requirements of several jurisdictions for accountability (see the discussion above in section 4.1 "Accountability for personal health information").

Information security responsibilities may include one or more of the following:

- performing security assessments and evaluating the organisation's information security risks (see **Security Requirement 1**);
- developing appropriate security policies (see **Security Requirement 2**);
- architecting, implementing and monitoring an enterprise wide information security program ensuring the confidentiality, integrity, and availability of information and the integrity and availability of systems;
- developing and implementing security awareness training programs (see **Security Requirement 16**);
- assessing, building and managing an effective information security department ;
- managing expense budgets for IT security services and capital expenditures;
- establishing protocols to proactively test and protect the integrity, confidentiality, and availability of information enterprise wide within the context of the organisation's privacy and security policies;
- reviewing audit logs (see **Security Requirement 52**);
- maintaining effective business continuity and disaster recovery plans (see **Security Requirement 86**); and
- serving as an information security expert for the executive staff of the organisation;

[65] Note that responsibility for patient/person privacy is separate from responsibility for information security and often these tasks rest with distinct individuals within the organisation who have differing backgrounds and skill sets; although both must work together co-operatively toward the common goal of protecting the confidentiality of PHI.

Rarely do these responsibilities all rest with a single individual. Rather, they are typically apportioned to several individuals within the organisation and this makes the clear and unambiguous assignment of these responsibilities all the more critical.

Note: Security Requirement 4 from the previous version of this document has been combined with **Security Requirement 3** above. All requirements will be renumbered in the next version of this document.

5.4.1.2 Independent Review of Information Security

Security Requirement 4 Independent Review of Security Policy Implementation

Organisations connecting to the EHRi or hosting components of the EHRi **must** have the implementation of their information security policy either:

a) reviewed independently; or

b) attested to in a written declaration by the organisation's chief executive officer or board of directors.

Policy & Procedures

Admin Requirement

Rationale: This requirement is intended to ensure the quality of security policies and to ensure that they are enforced. This will be especially important when the EHRi facilitates a high level of interoperability among and within jurisdictions. PHI flowing from one jurisdiction to another must do so in an environment where a minimum level of protection is afforded regardless of which jurisdiction the information finds itself. This requirement also follows from the accountability requirements in section 4.1.

Third party review can and should occur at many levels: policy reviews, organisational IT security reviews, EHRi-wide Threat and Risk Assessments, TRAs for specific systems, security architecture reviews, technical system testing such as vulnerability testing, and compliance audits against policies and procedures.

5.4.2 External Parties

5.4.2.1 Identification of Risks Related to External Parties

Security Requirement 5 Assessing Threats and Risks from Third Parties

Organisations hosting components of the EHRi **must** assess, by means of threat and risk analysis, the risks associated with access by external parties to hosted components or to facilities management by external parties and **must** implement appropriate security controls where necessary to mitigate identified risks.

Policy & Procedures

Admin Requirement

Rationale: Risk assessment is essential for effective management of third party access and the requirement above is a direct consequence of **Privacy Requirement 2**.

See also section 4.1 (Accountability for personal health information) for a discussion of the legal requirements concerning third-party service delivery management (e.g. PIPEDA and Ontario *Personal Health Information Protection Act*).

5.4.2.2 Addressing Security in Third-Party Agreements

Security Requirement 6 Addressing Security in Third Party Agreements

Organisations hosting components of the EHRi **must** base the following third party arrangements on formal contracts containing all necessary security requirements:

a) outsourcing management or control of all or some part of EHRi hosted components;

b) third-party facilities management for EHRi hosted components; or.

c) access to the EHRi by third parties.

Policy & Procedures

Admin Requirement

Rationale: This requirement is intended to impress upon third parties their legal responsibility for protecting the confidentiality and integrity of PHI and other security critical system data. It is also intended to enforce security responsibilities on service providers.

Security Requirement 7 Transmitting PHI

Organisations hosting components of the EHRi **must** inform organisations connecting to the EHRi that data they receive from the EHRi are confidential and the duty of such connecting organisations to protect the confidentiality of PHI received from the EHRi **must** be formally addressed.

Policy & Procedures

Admin Requirement

Rationale: This administrative requirement is intended to ensure that confidentiality remains enforced as data flows beyond the direct control of a healthcare organisation.

There are several technical requirements related to the transmission of PHI: see **Security Requirement 31** (**Encrypting PHI During Transmission**), **Security Requirement 32** (**Protecting Source and Destination Integrity During Transmission of PHI**), **Security Requirement 33** (**Acknowledging Receipt of Transmitted PHI**). **Security Requirement 34** (**Protecting PHI on Portable Media**), **Security Requirement 41** (**Logging EHRi Transmissions of PHI**), **Security Requirement 70** (**Restricting Connection Times to EHRi Applications**), **Security Requirement 71** (**Robustly Authenticating Users**), and **Security Requirement 75** (**Protecting Wireless Networks**).

See also **Privacy Requirement 1**, **Privacy Requirement 2**, **Privacy Requirement 12**, and **Privacy Requirement 18**.

Note: Security Requirement 8 "Addressing Security in Outsourcing" has been combined with **Security Requirement 6** above**.**

5.5 Asset management

The objectives of information asset management is to achieve and maintain appropriate protection of organisational assets. Information assets pertaining to the EHRi include all of the following:

- EHRi data,
- EHRi software,
- EHRi servers,

- Supporting software (operating systems, anti-virus software, etc.), and
- supporting hardware (firewalls, routers, etc.).

5.5.1 Responsibility for Assets

Security Requirement 9 Responsibility for Information Assets

Organisations hosting components of the EHRi **must**:

a) account for all health information assets available via the hosted component (inventory of assets),

b) have a nominated custodian of these health information assets, and

c) have rules governing the acceptable use of these assets that are identified, documented, and put into practice.

Policy & Procedures

Admin Requirement

Rationale: This requirement is intended to ensure that an inventory of health information assets is maintained, that custodianship of these assets is clearly delineated, and that acceptable use policy is articulated and enforced.

Experience with Y2K clearly showed the importance of maintaining an inventory of information assets, including systems and software. Custodianship follows from **Privacy Requirement 1**. Acceptable use follows directly from **Privacy Requirement 3**.

See also **Privacy Requirement 5**, **Privacy Requirement 7**, **Privacy Requirement 11**, and **Privacy Requirement 15**.

5.5.2 Information Classification

5.5.2.1 Classification Guidelines

Determining levels of protection for information assets in health informatics is a complex subject. Comparisons with government and/or military data classifications can be misleading. The following are important characteristics of information assets within healthcare:

a) The confidentiality of PHI is often largely subjective, rather than objective; which is to say that ultimately only the data subject (i.e., the patient) can make a proper determination of the relative confidentiality of various fields or grouping of data. For example, a patient/person escaping from an abusive relationship may consider her new address and phone number to be much more confidential than clinical data about setting her broken arm.

b) The confidentiality of PHI is context dependent. For example, the name and address of a patient/person in a list of admissions to a hospital's emergency department may not be considered especially confidential by that patient; yet the same name and address in a list of admissions to a clinic treating sexual impotency may be considered highly confidential by that patient.

c) The confidentiality of PHI can shift over the lifetime of a patient's record. For example, changing societal attitudes over the last 20 years have resulted in many patients no longer considering their sexual orientation to be confidential. Conversely, attitudes toward drug and alcohol dependency have caused some patients to consider addiction counselling data to be, if anything, even more confidential today that they would have been considered 20 years ago.

Because one cannot predict the sensitivity of a given element of PHI through all its uses and phases of its life cycle that all PHI should be subject to careful protection at all times. Identifying and (where appropriate) protectively labelling information assets as confidential can be an important tool in staff training and awareness. It may also be an important component of data protection agreements among jurisdictions and with third party organisations and their staff. The identification and labelling of information assets is also an essential component of ISO/IEC 17799[66]. In light of the above, a strong argument can be made to uniformly classify PHI as "confidential". Attempts to introduce gradations of confidentiality not only run counter to the three characteristics discussed above, but also run counter to jurisdictional legislation that defines PHI in broad terms.

Security Requirement 10 Classifying PHI

All organisations connecting to the EHRi or hosting components of the EHRi **must** classify data contained within a patient/person's EHR as confidential PHI.

Policy & Procedures

Admin Requirement

Rationale: This requirement ensures that users are fully aware that all PHI is considered confidential. It also ensures that there is no uncertainty about the extent of the information to which the privacy requirements apply. As discussed above, this requirement also precludes graded shades of confidentiality (e.g.: lab data more confidential than medication profile, or patient address data less confidential than billing data) and concomitant graded shades of security. All data contained within a patient/person's EHR is to be considered confidential and its confidentiality uniformly protected.

Uniformity of confidentiality is also a prerequisite for any realistic sharing of data across jurisdictions.

Note that while all PHI is uniformly classified as confidential, other requirements allow for records of "at risk" patient/persons to be specially tagged so that access to their records can be closely monitored. See **Security Requirement 49** (**Analyzing EHRi Audit Logs for Patients/Persons At Elevated Risk**).

5.5.2.2 Information Labelling and Handling

Security Requirement 11 Labelling Personal Health Information As Confidential

All POS systems connected to the EHRi **must** be capable of informing each POS user the confidential nature of PHI by showing this labelling on any hardcopy printout displaying the data and either:

a) showing this labelling on any screen displaying the data, or else

b) displaying this labelling to the user upon logging into the POS application (perhaps as part of an acceptable use policy).

Tech Requirement

Rationale: This requirement ensures that all healthcare providers and support staff are aware that the specific information they are handling is confidential PHI. This is especially important where the information is contained in email, faxes or other documents which may contain a mixture of confidential and non-confidential information.

[66] See References at the end of this document.

It is understood that an acceptable use statement tends to be ignored after a few uses of the system. The primary advantage of displaying such an acceptable use statement on an ongoing basis is in providing grounds for prosecution should the user not comply (i.e., not treat the information as confidential).

5.6 Human Resources Security

The objectives of human resource security are to:

1. reduce risks of human error, theft, fraud or misuse of facilities;
2. ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;
3. minimize the damage from security incidents and malfunctions; and
4. learn from such incidents.

5.6.1 Prior to Employment

5.6.1.1 Roles and Responsibilities

Security Requirement 12 Addressing User Responsibilities in Job Definitions

All organisations connecting to the EHRi or hosting components of the EHRi **should** document in job definitions the security roles and responsibilities of staff who are registered users of healthcare applications accessible via the EHRi, as laid down in the organisation’s information security policy.

These roles must be defined in a standardised or harmonized manner so as to ensure future interoperability of authentication services between POS systems and the EHRi.

Policy & Procedures

Admin Requirement

Rationale: This ISO/IEC 17799 requirement is intended to reinforce the formalisation of security roles and responsibilities. Where feasible, such user responsibilities can usefully be adopted from the practice guidelines that exist within each jurisdiction for the various regulated health professions.

Note that several other requirements are also related to job definitions; specifically those involving role-based access control. See requirements **Security Requirement 43**, **Security Requirement 58**, **Security Requirement 59**, and **Note that "Security Requirement 61**.

5.6.1.2 Terms and Conditions of Employment

Security Requirement 13 Addressing User Responsibilities in Terms of Employment

All organisations connecting to the EHRi or hosting components of the EHRi **must** include in the terms and conditions of employment of employees (permanent, part-time or contracted) who are, or will be, users of POS systems connected to the EHRi, a statement about the employee’s responsibility for information security and privacy.

Policy & Procedures

Admin Requirement

As a practical matter, it may only be possible to implement this requirement with new hires.

Rationale: This requirement follows from **Privacy Requirement 2** and **Privacy Requirement 3** and in industrial sectors outside of healthcare, this is usually considered a basic requirement. It is important to note that many healthcare workers are not bound by a licensing body or a professional code of ethics. Examples include hospital ward clerks, medical receptionists, billing clerks, clerical staff, administrators, and many others.

User responsibilities include:

- maintaining the confidentiality of PHI;
- not sharing user IDs, passwords, or other means of accessing the EHRi with other users (see **Security Requirement 55**, **Security Requirement 64**, and **Security Requirement 71**); and
- following appropriate procedures when using mobile devices or when working off-site or at home (see **Security Requirement 21**, **Security Requirement 34**, **Security Requirement 73**, and **Security Requirement 74**);

Terms of Employment should also include actions to be taken if the employee, contractor, or third-party user disregards the organisation's security requirements.

Terms of Employment involving maintaining confidentiality should survive employment termination (see provisions for confidentiality agreements in **Security Requirement 15**). Termination of employment is discussed further in section **Security Requirement 17**.

5.6.1.3 Screening

Security Requirement 14 Verifying the Identity of Users

All organisations hosting components of the EHRi or connecting to the EHRi **must** verify the identity and address of each permanent or temporary staff member or contractor who will become a registered user of a POS connected to the EHRi or who will have access to hosted components of the EHRi.

Policy & Procedures

Admin Requirement

Rationale: The majority of breaches of information security continue to be caused by insiders, including those breaches that occur in the healthcare sector. Proper identification of staff and the address at which they can be found (or traced) is an essential component of effective prosecution for violations of confidentiality.

Note that this requirement does not mandate (or even suggest) such measures as background checks on employees, which is the responsibility of jurisdictions. A simple verification of name and address from reliable identification documents (driver's license for example) suffices to meet the requirement. Such verification of identity documents helps to ensure that effective prosecution or litigation can be brought against individuals who can be shown, as a result of analyzing audit logs, to have abused their access privileges.

Although uncontroversial in other industrial sectors (banking and finance for example), verification checks are often not a part of healthcare hires (especially for staff who are not members of a professional society). As a practical matter therefore, this requirement may have to be phased in over time.

See also **Security Requirement 54**, **Security Requirement 55**, and **Security Requirement 57** for a discussion of EHRi user registration. User authentication is dealt with in **Security Requirement 71**.

5.6.1.4 Confidentiality Agreements

Security Requirement 15 Confidentiality Agreements

All organisations hosting components of the EHRi or connecting to the EHRi **must** obtain a signed confidentiality agreement from each permanent or temporary staff member or contractor who is a registered user of a POS connected to the EHRi or who has access to hosted components of the EHRi as part of his or her initial terms and conditions of employment. The confidential agreement must survive the termination of employment.

Policy & Procedures

Admin Requirement

Rationale: The signing of *confidentiality agreements is widely adopted* in other industrial sectors (banking and finance for example) and its adoption in healthcare is rapidly increasing. A recent *Infoway* survey found that about nine out of ten Canadian healthcare organisations have their employees sign confidentiality agreements.[67]The requirement above is intended to provide an legal means of seeking redress against staff who violate the confidentiality of PHI[68].

In general, health information legislation contains an obligation to maintain administrative safeguards and some jurisdictions have more specific provisions, albeit none that provide specific guidance on confidentiality agreements. For example, Saskatchewan's health information legislation provides that a trustee must "ensure compliance with this Act by its employees", although the methods of ensuring compliance are not specified. Manitoba's health information legislation provides that each employee must sign a pledge of confidentiality that includes an acknowledgment that he or she is bound by the trustee's policies and procedures and is aware of the consequences of breaching them. Other jurisdictional legislation frames general workplace agreements (e.g. the Normes du Travail in Québec). Confidentiality agreements need to be carefully worded to comply with jurisdictional requirements.

5.6.2 During Employment

5.6.2.1 Information Security Awareness, Education and Training

Security Requirement 16 Training Users and Raising Security Awareness

All organisations hosting components of the EHRi or connecting to the EHRi **must** ensure that information security education and training and regular updates in organisational security policies and procedures are provided to each permanent or temporary employee or third-party contractor who is a registered user of a POS connected to the EHRi or who has access to hosted components of the EHRi.

Policy & Procedures

Admin Requirement

Rationale: Training in security awareness is essential. All users need to be made aware of the confidentiality of PHI, and the procedures required for maintaining this confidentiality. As well, users should be made aware of the importance of

[67] Canada Health Infoway, Infoway Pan-Canadian EHR Survey: Phase I, Results and Analysis, September 2002.

[68] As noted above, many healthcare workers are not bound by a licensing body or a professional code of ethics. Examples include hospital ward clerks, medical receptionists, billing clerks, clerical staff, administrators, and many others. It is essential therefore to dispel the notion that redress for breach of confidentiality can rest solely with the disciplinary procedures of professional organisations and regulatory bodies.

maintaining the confidentiality of information that refers to identifiable healthcare providers.

Staff who are involved in providing or maintaining security services related to the EHRi should be provided with access to appropriate security alerts and other technical security information to raise and maintain awareness of security threats.

Finally, it should be noted that while the requirement for training users on data protection is stated in Privacy Requirement 22b, there is an obvious expectation that privacy and security training be treated together in a coherently and consistent fashion.

5.6.3 Employment Termination

Security Requirement 17 Terminating User Access When Terminating Employment

All organisations hosting components of the EHRi or connecting to the EHRi **must**, as soon as possible, terminate the user access privileges of each permanent or temporary employee or third-party contractor who is a registered user of a POS connected to the EHRi or who has access to hosted components of the EHRi upon termination of their employment with the organisation.

Policy & Procedures

Admin Requirement

Tech Requirement

Rationale: Effective termination of user access privileges is a minimum requirement but in the absence of single sign-on capabilities and shared authentication services, it is not always effectually handled. Termination of user access privileges will also include termination of digital signatures (see "**Security Requirement 79 Providing Digital Signatures for Users**").

See also the requirement for time limited user registrations (**Security Requirement 56**) and the requirement that confidentiality agreements survive the termination of employment mandated by **Security Requirement 15**.

5.7 Physical and Environmental Security

The objectives of physical and environmental security are to:

1. prevent unauthorized access, damage and interference to business premises and information;
2. prevent loss, damage or compromise of assets and interruption to business activities; and
3. prevent compromise or theft of information and information processing facilities.

5.7.1 Secure Areas

Security Requirement 18 Physically Securing EHRi Systems

All organisations hosting components of the EHRi **must** use security perimeters to protect areas that contain information processing facilities supporting EHRi servers, applications or data. These secure areas **must** be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Policy & Procedures

Admin Requirement

Tech Requirement

Rationale: Perimeter security of servers and other aspects of application hosting is a minimum requirement for ensuring the availability and integrity of these important applications and data and for ensuring the confidentiality of information in storage that is not already secured cryptographically. In turn, controlling access is a minimum requirement of perimeter security.

The provisions for physical safeguards vary among jurisdictions. The most detailed provisions are found in Manitoba's health information legislation, which require the trustee to ensure that PHI is maintained in a designated area or areas that is subject to appropriate security safeguards; and to limit physical access to designated areas to authorized persons.

5.7.2 Equipment Security

5.7.2.1 Equipment Siting and Protection

Security Requirement 19 Protecting EHRi Systems from Hazards

All organisations hosting components of the EHRi **must** protect sites and equipment supporting the EHRi to reduce the risks from environmental threats and hazards.

Admin Requirement Tech Requirement

Rationale: This is a minimum requirement for protecting EHRi system integrity and availability.

5.7.2.2 Supporting Utilities

Security Requirement 20 Protecting EHRi Systems from Disruptions

All organisations hosting components of the EHRi **must** protect equipment supporting the EHRi from power failures and other disruptions caused by failures in supporting utilities.

Admin Requirement Tech Requirement

Rationale: This is a minimum requirement for protecting system availability in the 24/7 operational environment of healthcare. Healthcare demands high system availability, especially in those instances where disruptions of supporting utilities are caused by disasters that themselves result in injuries and therefore place a heavy burden on emergency health services.

5.7.2.3 Equipment Maintenance and Security of Equipment Off-Premises

Security Requirement 21 Protecting EHRi Equipment Off-Premises and During Maintenance

All organisations hosting components of the EHRi **must** ensure that equipment supporting the EHRi:

1) is not used outside their premises without appropriate safeguards and prior authorization by the organisation's management, and

2) is repaired or serviced by authorized personnel only.

Admin Requirement

Examples of off-site use include:

- the temporary siting of servers off-site during renovations to premises,
- the relocation of operations during disaster recovery,
- the testing or reconfiguration of equipment off-site, and
- laptops or home computers used by system administrators to monitor or manage operations.

Use of laptops or home computers by healthcare providers to access the EHRi is discussed in section 5.9.8.

Rationale: This is a minimum requirement. It is important to note that arbitrary transfer of equipment (and the information it may contain) from one location to another may violate one or more of the privacy requirements in section 4.5 ("Limiting use, disclosure and retention of personal health information").

5.7.2.4 Secure Disposal or Reuse of Equipment

Security Requirement 22 Disposing of or Reusing EHRi Equipment

All organisations hosting components of the EHRi or connecting to the EHRi **must** securely overwrite or else destroy all media containing EHRi application software, PHI, or security critical system data when no longer required for use.

Admin Requirement **Tech Requirement**

Rationale: This is a minimum requirement. Legal requirements follow from the Manitoba regulations pursuant to *Personal Health Information Act*: "to ensure the security of PHI in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose".

Note also the discussion in section 4.5 ("Limiting use, disclosure and retention of personal health information") on the legal requirements for safe disposal.

Removal of equipment for repair is covered in the next section. See also **Security Requirement 35**

5.7.2.5 Removal of Property

Security Requirement 23 Removing EHRi Equipment, Data or Software

All organisations hosting components of the EHRi **must not** allow equipment, data or software supporting the EHRi to be removed without authorization by the organisation's management.

Admin Requirement

Rationale: This is a minimum requirement. It is important to note that arbitrary removal of equipment (and the information it may contain) from one location to another may violate one or more of the privacy requirements in section 4.5 ("Limiting use, disclosure and retention of personal health information").

5.8 Communications and Operational Management

The objectives of communications and operational management security are to:

1. ensure the correct and secure operation of information processing facilities;
2. minimize the risk of systems failures;
3. protect the integrity of software and information;
4. maintain the integrity and availability of information processing and communication;

5. ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
6. prevent damage to assets and interruptions to business activities; and
7. prevent loss, modification or misuse of information exchanged between organisations.

5.8.1 Operational Procedures and Responsibilities

5.8.1.1 Change Management

Security Requirement 24 Controlling Changes to the EHRi

All organisations hosting components of the EHRi **must** control changes to information processing facilities and systems that support the EHRi by means of a formal and structured change control process to ensure the appropriate control of host applications and systems.

Policy & Procedures

Admin Requirement

Rationale: Failures in change management are a common source of security problems.

5.8.1.2 Segregation of Duties

Security Requirement 25 Segregating Duties

All organisations hosting components of the EHRi **should**, where feasible, segregate duties and areas of responsibility of permanent or temporary employees or third-party contractors who have access to hosted components of the EHRi in order to reduce opportunities for unauthorized modification or misuse of PHI and security critical system data.

Policy & Procedures

Admin Requirement

Rationale: Separation of duties is a cornerstone of operational security, albeit one which can be difficult to implement in a healthcare environment, especially in smaller organisations.

It is established best practice in many industrial sectors (e.g., financial services) to put "checks and balances" in place that ensure tasks assigned to employees are coordinated such that one person cannot flout organisational policies while avoiding detection.

5.8.1.3 Separation of Development, Test and Operational Facilities

Security Requirement 26 Separating Development and Testing from Operations

All organisations hosting components of the EHRi **must** separate the development and testing environments for those EHRi components from the operational environments for those components.

Rules for the migration of software from development to operational status **must** be defined and documented by the organisation hosting the affected application(s).

Policy & Procedures

Admin Requirement

Tech Requirement

This requirement may not affect organisations that do not develop applications in-house, although a testing upgrades, software patches, etc. may necessitate a separate test environment, even in the absence of in-house development.

Rationale: Separation of testing and production is a minimum requirement.

5.8.2 Third Party Service Delivery Management

Third party service delivery is dealt with in **Security Requirement 5** and in **Security Requirement 6**.

5.8.3 System Planning and Acceptance

Security Requirement 27 Maintaining Capacity

All organisations hosting components of the EHRi **must** monitor capacity demands and project future capacity requirements to ensure adequate processing power and storage will be made available to host those EHRi components.

Policy & Procedures

Admin Requirement

Tech Requirement

As stated in ISO/IEC 17799:2000, “managers should use this (capacity) information to identify and avoid potential bottlenecks that might present a threat to system security or user services, and plan appropriate remedial action”.

Rationale: This is a basic requirement for maintaining system availability.

Security Requirement 28 Upgrading the EHRi

All organisations hosting components of the EHRi **must:**

a) establish acceptance criteria for planned new information systems, upgrades and new versions;

b) carry out functional and security tests of the system prior to acceptance; and

c) ensure that all existing PHI and security critical data are continually safeguarded during the upgrade.

Policy & Procedures

Admin Requirement

Tech Requirement

Rationale: This is a basic requirement for maintaining system integrity.

5.8.4 Protection Against Malicious And Mobile Code

Security Requirement 29 Protecting Against Malware

All organisations hosting components of the EHRi or connecting to the EHRi **must** implement appropriate detection and prevention controls and appropriate user awareness procedures to protect against malicious software (viruses, worms, etc.)

Admin Requirement **Tech Requirement**

Rationale: This is a minimum requirement for the prevention of security breaches facilitated by malware.

5.8.5 Backup

Security Requirement 30 Securely Backing Up Data

All organisations hosting components of the EHRi **must**

a) back up[69] PHI and security critical system data in a manner that ensures the confidentiality, integrity, and availability of the data ; and

b) store the backed-up data in a physically secure environment off-site (see section 5.7).

Admin Requirement **Tech Requirement**

Rationale: Several technologies are available to ensure the confidentiality of data during storage, such as encryption or the use of de-identified data. Jurisdictions must determine the level of protection required based on risk, technical and operational aspects.

5.8.6 Network Security Management

Security Requirement 31 Encrypting PHI During Transmission

The EHRi and POS systems connected to the EHRi **must** apply industry standard cryptographic algorithms and protocols during transmission of PHI to maintain the confidentiality and integrity of this data whenever it is transmitted outside the physical security perimeter[70] that protects information processing facilities supporting EHRi servers, applications or data.

Tech Requirement

Rationale: Interception of confidential information is a serious risk and its alteration in transit has severe consequences. Providing for the confidentiality and integrity of PHI transmitted by the EHRi is a minimum requirement.

Health information legislation does not contain specific directions regarding protection of information during transmission, but there are some general requirements. For example, Ontario's health information legislation requires

[69] In this statement, backup refers to copies of data made for short-term disaster recovery purposes, as distinguished from copies made for long-term archiving purposes.

[70] Requirements for maintaining a physical security perimeter are found in **Security Requirement 18**.

custodians to “transfer” PHI in a secure manner. Manitoba’s health information legislation requires a trustee who uses electronic means to request disclosure and to respond to requests for disclosure to implement procedures to prevent the interception of information by unauthorized persons.

Security Requirement 32 Protecting Source and Destination Integrity During Transmission of PHI

The EHRi **must** protect the source and destination of the message against masquerade during data transmission of PHI to maintain its confidentiality and integrity.

Tech Requirement

Rationale: This is a minimum requirement to protect against the threat of masquerade. This requirement facilitates trusted end-to-end information flow and would require that a technology such as digital signatures, dedicated lines, or virtual private networks be implemented to protect source and destination.

Security Requirement 33 Acknowledging Receipt of Transmitted PHI

Where appropriate, the EHRi **must** obtain acknowledgement of receipt during data transmission of PHI to ensure that the transmitted data was received.

Tech Requirement

Rationale: Message acknowledgement via handshaking or other methods is a minimum requirement to ensure complete receipt of information at its destination.

5.8.7 Media Handling

5.8.7.1 Management of Removable Computer Media

Security Requirement 34 Protecting PHI on Portable Media

All organisations hosting components of the EHRi **must** – and organisations connecting to the EHRi **should** – ensure that PHI and other security critical data stored on removable media are:

a) encrypted while the media are in transit to protect the data's confidentiality and integrity; and

b) protected from theft, where appropriate, while the media are in transit to protect the data's availability.

Policy & Procedures

Admin Requirement **Tech Requirement**

Rationale: This requirement protects information stored on removable media. Mobile devices are covered in **Security Requirement 73** (**Acceptable Use of Mobile Devices**).

5.8.7.2 Disposal of Media

Security Requirement 35 Disposing of Media Containing PHI

All organisations connecting to the EHRi or hosting components of the EHRi should destroy, permanently erase or make anonymous PHI contained on media that are no longer required.

Admin Requirement **Tech Requirement**

Rationale: This is a minimum requirement. Legal requirements follow from the Manitoba regulations pursuant to *Personal Health Information Act*: “to ensure the security of PHI in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose”.

Note that this requirement refers to disposal of media, not the deletion of records (i.e., it presumes that relevant data have been copied to other media or exist in other systems prior to media disposal. Note also the discussion in section 4.5 ("Limiting use, disclosure and retention of personal health information") on the legal requirements for safe disposal.

Finally, it is important to note that several high profile lapses in health informatics security have been caused by improper disposal of media.

See also **Security Requirement 22** on the disposal and reuse of EHRi equipment.

5.8.7.3 Information Handling Procedures

Security Requirement 36 Protecting Data Storage

All organisations hosting components of the EHRi **must** protect electronic media containing PHI or security critical system data, including user registration data, by one or more of the following means:

a) physically protecting the media in accordance with **Security Requirement 18**;

b) securely de-identifying the PHI it contains; or

c) encrypting the data it contains.

Admin Requirement **Tech Requirement**

Rationale: Protection of the PHI is essential if use and disclosure of this information is to be controlled. In this sense, this requirement follows from the privacy requirements of section 4.5. Encryption of data stores is still uncommon in healthcare and healthcare organisations have been slow to make use of contemporary technology for encrypting databases. Attempts to de-identify data stored in databases are frequently inadequate and sometimes easy to subvert.

Protection of user registration data is essential to maintaining its integrity (and hence the integrity of the user authentication process). Protecting its confidentiality is essential to maintaining the trust of healthcare providers (who, for example, do not want to be sent marketing materials from spammers gaining access to a poorly secured list of contact details for users).

While physical protection of data storage will always be essential (to protect system availability), de-identification and encryption should be seriously considered in the design of any new system.

Security Requirement 37 Protecting Storage of Unencrypted PHI in the EHRi

All organisations hosting components of the EHRi **must** monitor the status and location of media containing unencrypted EHRi data or security critical data, including user registration data, and ensure this data remains physically protected.

Policy & Procedures

Admin Requirement

Rationale: This requirement follows directly from the Privacy Requirements in section 4.5 and complements **Security Requirement 36** in ensuring the confidentiality and availability of EHRi data.

5.8.8 Exchanges Of Information

5.8.8.1 Information Exchange Policies and Procedures

The policies and procedures required of organisations hosting components of the EHRi are discussed in **Privacy Requirement 2** and in **Security Requirement 7**.

5.8.8.2 Exchange Agreements

Information exchange agreements should be executed between (among) jurisdictions operating EHRi components prior to PHI flowing across provincial/territorial borders. Such agreements would clarify the mutual custodial responsibilities of jurisdictions with relation to PHI. The detailed content of such inter-jurisdictional data exchange agreements is beyond the scope of this document, but it should be noted that there are standards in place for the content of such documents. See for example: ISO standard 22857, "Health Informatics: Guidelines on data protection to facilitate trans-border flows of personal health information".

5.8.9 Electronic Commerce Services

This section of ISO/IEC 17799 is not currently relevant to the *EHRS Blueprint* and its related services.

5.8.10 Monitoring

Of all security requirements protecting PHI, one of the most important is audit and logging. These ensure accountability for patients/persons entrusting their information to electronic health record systems and also ensure that users will conform to policies on acceptable use of the EHRi.

5.8.10.1 Audit Logging

Security Requirement 38 Logging Transactions in the EHRi

The EHRi **must** create a secure audit record each time a user:

a) accesses, creates or updates[71] PHI of a patient/person via the EHRi;

b) overrides the consent directives of a patient/person via the EHRi;

c) accesses, via the EHRi, data that is locked or masked by instruction of a patient/person; or

d) .accesses, creates or updates registration data on an EHRi user.

Tech Requirement

Rationale: Audit records should contain the necessary information to answer the following questions:

1. For a given user, what PHI did they access, create or update and when?
2. For a given element of PHI, what users have accessed, created or updated it and when?

This requirement follows from **Privacy Requirement 13** and **Privacy Requirement 19** and is also required for effective compliance with legislation in some jurisdictions.[72] It also follows secondarily from **NOTE: Privacy Requirement 6**, **Privacy Requirement 13** and **Privacy Requirement 24**. Legal requirements also arise from the Manitoba *Personal Health Information Act* Regulations, which state:

Additional safeguards for electronic health information systems

4(1) *A trustee shall ensure every electronic information system that the trustee designs or acquires after December 11, 2000:*

(a) produces an electronic record of every successful or unsuccessful attempt to

(i) gain access to the personal health information maintained on the system,

(ii) add to, delete or modify the personal health information maintained on the system; and

(b) records every transmission of personal health information maintained on the system.

Audit information may be stored in POS systems, as well as in the EHRi. To construct an authoritative transcript of which users have accessed a patient/person's PHI or what PHI a user has accessed, all audit records will need to be accessible and hence audit requirements meeting the strictest existing

[71] Note that PHI cannot be deleted, only updated and archived.

[72] Ontario, *Personal Health Information Protection Act,* sections 12(2) and 17(3). These sections require a health information custodian to notify a patient/person when his or her information is stolen, lost or accessed by an unauthorized individual.

jurisdictional legal requirements are essential to support full interoperability across jurisdictions.

Interoperability also contributes to the rationale for consistent and uniform logging. While there is no widely adopted standard in Canada for healthcare audit logging, the IHE standard “Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications” describes an XML schema for reporting information necessary for privacy and security auditing of healthcare applications and is endorsed by the IHE IT Infrastructure Technical Framework Supplement 2004-2005 Audit Trail and Node Authentication Profile Public Comment Version, published in June 2004.[73]

Security Requirement 39 Preserving the History of PHI in the EHRi

The EHRi **must** be capable of displaying the former content of a record at any point in the past, as well the associated details of who entered, accessed or modified the data and at what time.

Tech Requirement

Rationale: Such a capacity allows reconstruction of the state of an EHR at any point in time. This requirement is necessary for a number of purposes, including negligence actions, and professional disciplinary matters. Maintenance of data integrity necessitate this type of logging.

Some jurisdictions within Canada also allow patients/persons to attach a statement of disagreement to an element of information that a patient believes to be incorrect (and where the healthcare provider who authored it does not). The EHRi must be able to facilitate the existence of such statements of disagreement concerning the accuracy or inaccuracy of a data element.

Security Requirement 40 Preserving the History of PHI in POS Systems

All POS systems connected to the EHRi **should** be capable of displaying the former content of a record at any point in the past, as well and the associated details of who entered, accessed or modified the data and at what time).

Tech Requirement

Rationale: Such an audit log allows reconstruction of the state of any EHR stored within the POS system at any point in time. Maintenance of data integrity and effective logging of changes to PHI necessitate this type of audit logging.

Security Requirement 41 Logging EHRi Transmissions of PHI

The EHRi **must** be capable of determining all past recipients of data from an EHR and must be capable of notifying them if data in the EHR is subsequently amended.

Tech Requirement

Rationale: This requirement facilitates system-wide audit of message transmission and delivery. It is also follows as a consequence of **Privacy Requirement 25**.

[73] The “Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications” is available at: http://www.ietf.org/internet-drafts/draft-marshall-security-audit-12.txt

Though logging of all past recipients can quickly grow huge, the cost of online storage continues to fall by half each year and even terabyte storage capacity is no longer prohibitively expensive for many healthcare organisations.

The EHRi may be required to keep a record of all cross-jurisdictional transfers of PHI. This requirement follows from jurisdictional legislation. For example, Alberta's health information legislation requires a custodian that discloses PHI to make a note of the name of the person to whom the custodian disclosed the information; the date and purpose of the disclosure; and a description of the information disclosed. The latter requirement (a description of the information disclosed) is not directly met by the requirement above, but is when the requirement above is taken together with the other audit logging requirements in this section.

Security Requirement 42 Logging Access to PHI in POS Systems

All POS systems connected to the EHRi **must** record in an audit log every instance of a user accessing, updating, or archiving PHI.

Tech Requirement

Rationale: This requirement follows from **Privacy Requirement 19**.

Security Requirement 43 Minimum Content of Audit Logs

The EHRi audit log and the audit logs of POS systems connecting to the EHRi **must** contain:

a) the user ID of the accessing user;

b) the role the user is exercising[74];

c) the organisation of the accessing user (at least in those cases where an individual accesses information on behalf of more than one organisation);

d) the patient ID of the data subject (patient/person);

e) the function performed by the accessing user;

f) a time stamp;

g) in the case of access override to blocked or masked records or portions of records, a reason for the override, as chosen by the user making the access; and

h) in the case of changes to consent directives made by a substitute decision-maker, the identity of the decision-maker.

Tech Requirement

Rationale: This requirement follows from **Privacy Requirement 10**, **Privacy Requirement 15** and **Privacy Requirement 19**, as well as from common practice in information security.

[74] A user may be assigned more than one role but **Security Requirement 59** mandates that the user can only exercise one role at a time.

Security Requirement 44 Retaining Audit Logs

All organisations hosting components of the EHRi or connecting to the EHRi **must** retain[75] the audit log for the entire retention period of the records audited, to enable investigations to be carried out when necessary and to provide evidence where necessary.

Admin Requirement

Tech Requirement

Rationale: This requirement follows from **Privacy Requirement 19**, **Privacy Requirement 20** and **Privacy Requirement 21**.

Note that Alberta's health information legislation requires a custodian that discloses PHI to make a note of the name of the person to whom the custodian disclosed the information; the date and purpose of the disclosure; and a description of the information disclosed. The information must be retained for a period of 10 years following the date of disclosure.

Audit logs must be retained in a form that allows analysis of log contents. See **Security Requirement 46**, **Security Requirement 47**, **Security Requirement 48**, and **Security Requirement 49**.

5.8.10.2 Monitoring System Use

Security Requirement 45 Continuously Logging the EHRi

EHRi audit logging **must** be operational at all times.

Tech Requirement

Rationale: This is a minimum requirement and ensures logging cannot be turned off while the system is in operation.

Security Requirement 46 Detecting Patterns of Misuse

The EHRi **must** provide automated analysis tools to assist system auditors in the detection and prevention of system misuse (e.g. data harvesting).

Tech Requirement

Rationale: This requirement mandates that automated tools actively look for anomalous patterns of access. Such active intrusion detection is an essential feature of robust security systems.

Unlike audit logging itself, the analysis tools need not be continuously available. It suffices that such tools be available when needed. Need will be determined by system design and by appropriate Threat and Risk Analysis.

Security Requirement 47 Reporting Every Access To A Patient/Person's EHR

The EHRi **must** be capable of identifying of all users who have accessed or modified a given patient's/person's record(s) over a given period of time.

Tech Requirement

[75] Retention need not be in an online format. It suffices that audit log data be backed up or archived in a manner that allows for its subsequent access provided this can still be done in a reasonably timely and cost effective manner.

Rationale: This requirement is intended to facilitate the discovery of inappropriate access and assist in subsequent disciplinary or legal action. Note that unique identifiers for users are specified in **Security Requirement 55**.

Security Requirement 48 Reporting Every Access By A User

The EHRi **must** be capable of identifying all patients/persons whose records have been accessed or modified by a given user over a given period of time.

Tech Requirement

Rationale: This requirement greatly facilitates the determination of suspicious or wrongful use of access privileges.

Unique identifiers for users are specified in **Security Requirement 55**.

Security Requirement 49 Analyzing EHRi Audit Logs for Patients/Persons At Elevated Risk

The EHRi **must** provide functions for analyzing logs and audit trails to allow the identification of all users who have accessed or modified such record(s) over a given period of time.

Tech Requirement

Rationale: This requirement greatly facilitates the determination of suspicious or wrongful use of access privileges with regard to patients who are high profile or whose confidentiality is otherwise especially at risk.

As noted in the discussion of Privacy Requirement 22a, the records of certain patients/persons (e.g. celebrities, politicians, and newsmakers) may be at elevated risk of access by those who do not have a need-to-know. It may therefore be prudent to place additional audit controls on these records to protect patient privacy. The EHRi should recognize this practical reality and facilitate the rapid and regular audit of access to these records (perhaps involving notification to a privacy officer on each access).

This requirement should *not* be construed as meaning that the information in the records of such patient/persons are somehow more confidential than those of ordinary citizens or that these records, as information assets, are more valuable than those that are not at elevated risk of inappropriate access. Rather, the requirement ensures that the capability exists to rapidly identify prurient interest by users who lack a legitimate need-to-know.

See Privacy Requirement 22a for the requirement to provide a facility to denote which patients/persons are at elevated risk.

5.8.10.3 Protection of Log Information

Security Requirement 50 Securing Access to EHRi Audit Logs

The EHRi **must** secure access to audit records and **must** safeguard access to system audit tools and audit trails to prevent misuse or compromise.

Admin Requirement **Tech Requirement**

Rationale: This is a minimum requirement for maintaining system integrity and the confidentiality of information contained in the audit log. Confidentiality is critical since a third party obtaining access to such a log might infer PHI from audit log entries (e.g., from a log entry indicating update of a patient record by a user at a cancer care centre, it could be inferred that the patient has cancer).

Security Requirement 51 Making EHRi Audit Logs Tamper-Proof

The EHRi **must** provide appropriate security measures to protect audit logs from tampering.

Tech Requirement

Rationale: This is a minimum requirement for maintaining system integrity.

5.8.10.4 Review of System Logs and Audit Trails

Security Requirement 52 Regularly Reviewing EHRi Audit Logs

All organisations hosting components of the EHRi **must** subject system logs and audit logs to detailed review; on a regular and ongoing basis.

Admin Requirement

Rationale: Audit trails are of questionable utility if not reviewed and so periodic review ought to be a minimum requirement. Note that analysis tools that facilitate audit trail review are mandated in Security Requirement 46, Security Requirement 47, Security Requirement 48 and Security Requirement 49. Review of audit logs should be done by one or more responsible individuals assigned the task as in **Security Requirement 3**. Audit log review can be greatly aided by software such as intrusion detection systems that look for unusual patterns of use and facilitate exception reporting.

Note that Manitoba's health information legislation requires a trustee to regularly review audit trails "to detect any security breaches."

5.9 Access Control

The objectives of this section of ISO/IEC 17799 are to:

1. control access to information;
2. prevent unauthorized access to information systems;
3. ensure the protection of networked services;
4. prevent unauthorized computer access;
5. detect unauthorized activities; and
6. ensure information security when using mobile computing and tele-networking facilities.

5.9.1 Requirements For Access Control

Security Requirement 53 Policy for Access Control

All organisations hosting components of the EHRi **must** develop an Access Control Policy for the EHRi.

Admin Requirement

Rationale: This is a minimum requirement for the rational and effective deployment of access control mechanisms.

The task is considerably simplified to the extent that jurisdictions can cooperate in defining a common or harmonized access control policy.

5.9.2 User Access Management

5.9.2.1 User Registration

In what follows, the identification and registration of users includes:

a) the accurate capture of a user's identity (e.g.: Joan Smith, born March 26 1982, currently resident on Bloor Street, Toronto);

b) the accurate capture of a user's enduring professional credentials (e.g.: Dr. Joan Smith, Cardiologist) and/or job title (e.g.: Susan Jones, Medical Receptionist); and

c) the proper assignment of a user id.

This is in contradistinction to privilege management (see section 5.9.2.2) which relies upon the accuracy of the information above to assign and manage privileges. The distinction can best be illustrated operationally: ideally, users should be identified once (at initial registration), their registration optionally subject to periodic renewal as appropriate, and their privileges managed on an ongoing basis (with changes being made as required by their work).

Note that patients/persons are not typically system users, although patients/persons who are able to access all or part of their personal data online (e.g., via an online portal) would indeed be system users (albeit ones who are granted limited functionality). Note also that there are healthcare applications where a user may seek general health advice and information. While this request for information may be recorded, the accessing user remains anonymous (many Web sites offering information on pregnancy, AIDS or other public health topics operate in this fashion). Users of such general information sites do not require registration and are excluded from consideration in the discussion below.

Security Requirement 54 Registering Users

All organisations connecting to the EHRi **must** subject potential users of POS systems that connect to the EHRi to a formal user registration process. These user registration procedures **must** ensure:

a) that the level of user identification that is provided is consistent with the assurance required, given the value of the information assets and the functions that will become available to the user;

b) that each potential user has a legitimate relationship with the organisation;

c) that each potential user has a legitimate need to access PHI via the EHRi.

Policy & Procedures

Admin Requirement

Rationale: This requirement follows directly from **Privacy Requirement 13** and from the legal requirements of several jurisdictions that those accessing and updating PHI be identified. For example, in Manitoba, the identity of the person seeking to use PHI must be verified as a person the trustee of the information has authorized to use the information.

This requirement also implies that, for example, users who are assigned roles that can access PHI must be identified more rigorously than users who can only access, for example, anonymised data.

Registration need not be a purely manual process. Effective use of technical means (e.g., online registration via the Internet, backed by pre-established databases of shared secrets and roles drawn from provider registries) may greatly enhance the registration process.

There is no current agreement among jurisdictions about how best to register users, nor are there shared registration procedures or accepted best practices for registering the users of healthcare applications.

Security Requirement 55 Assigning Identifiers to Users

All organisations connecting to the EHRi **must** ensure that users of POS systems that connect to the EHRi are assigned an identifier (user ID) that, in combination with other identifiers (e.g., facility identifiers, jurisdictional identifiers, etc.) can uniquely identify the user within the EHRi.

POS systems **must** support the unique identification of users.

Tech Requirement

Rationale: This requirement facilitates system-wide audit and trusted end-to-end security.

Security Requirement 56 Time Limited User Registration

All organisations connecting to the EHRi **must** ensure that the registration of users of POS systems that connect to the EHRi is time limited (after which, the user's registration will need to be renewed).

Policy & Procedures

Admin Requirement

Note that renewal of registration is not synonymous with re-identification (i.e. in a well-designed registration process, users who have been effectively identified once do not necessarily need to be re-identified from scratch when their registration is renewed). Some POS systems will automatically support this requirement, while others will need to be supplemented by manual processes (e.g.: an annual review of users and whether their access is still merited). However it is achieved, time limited user registration can be an effective strategy to prevent continued access by users whose employment is terminated or whose contracts have ended.

The timely revocation of access privileges is covered in **Security Requirement 62**. Note that revocation of specific access privileges is a separate issue from time limited user registration (which ensures that all access is terminated after a period of time, unless registration is explicitly renewed).

Note also that time limited registration does not imply that archiving and audit log requirements for registration data can be foreshortened.

Rationale: This requirement and the previous one are a hedge against the misadministration of users who are initially granted high levels of access and then transferred to positions where such levels of access are no longer needed.

Security Requirement 57 Reviewing User Registration Details

All organisations connecting to the EHRi **should** periodically review user registration details to ensure that they are complete, accurate and that access to the EHRi is still required.

Policy & Procedures

Admin Requirement

This requirement, together with requirement Security Requirement 56 ensures that user registration details (for example, a contact phone number or email address) remain current.

Rationale: This requirement facilitates accountability.

5.9.2.2 Privilege Management

For the EHRi, the overarching objective is to provide security controls to ensure that access to specific records, and, where appropriate, to specific elements of PHI within those records, is granted only to those EHRi users with a legitimate need-to-know. A user's need-to-know can be determined in one of more of the following ways:

- through explicit pre-defined care relationships (e.g.: a patient/person's family physician),
- through general work assignments (e.g.: when a physician fills in for another physician who is sick),
- through associative relationships (e.g.: a physician in a primary care group should be able to access the records of patient/persons seen by physicians in that primary care group),
- through explicit delegation (e.g.: a nurse hired by a primary care practice should be able to access the records of patients/persons whose family physicians make up the clinic),
- through referral (e.g.: a physician refers a patient/person to a specialist), and
- through explicit ad-hoc assertions by an individual care provider (e.g.: in the provision of emergency medicine).

In the subsections that follow, several access control methodologies are discussed that, when taken together, ensure the confidentiality and integrity of PHI by restricting user access to those with a legitimate need-to-know. These access control methodologies are:

a) **role-based access control**, which relies upon the professional credentials and job titles of users established during registration to restrict users to just those access privileges that are required to fulfil one or more well-defined roles;

b) **workgroup based access control**, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access; and

c) **discretionary access control**, which relies upon users with a legitimate relationship to a patient/person's EHR (a family physician, say) to confer access to other users who have no previously established relationship to that patient/person's EHR (a specialist, say).

Role-Based Access Control

Role-based access control limits the access of a user to specific portions of records (e.g.: demographic data)and to specific functions that can be performed on those portions of records (e.g.: update contact details in the demographic data). It is *not* typically used to limit access to the records of specific patients/persons, as this is the task of workgroup based access control and/or discretionary access control.

Note that patients/persons are not typically system users, although patients/persons who are able to access all or part of their data online (e.g., via a portal) would indeed be system users who are exercising the role of “Patient”.

Security Requirement 58 Granting Access to Users by Role

The EHRi and all POS systems connected to the EHRi **must** support role-based access control (RBAC) capable of mapping each user to one or more roles, and each role to one or more system functions.

Tech Requirement

Rationale: As a practical matter, users of POS systems connected to the EHRi (and there will be many thousands of them) cannot individually be mapped to system functions upon user registration in order to control the extent of their user access privileges. Such a mapping is too complex and too error prone to be done on a user-by-user basis. Rather, users must be mapped to roles, and then the roles mapped to system functions.

There are significant issues related to using RBAC to support an interoperable EHR that must be resolved before the EHRi can make full and effective use of RBAC. These issues are summarised in Appendix A-1 **Privacy and Security Implications Connected With Actors**.

Security Requirement 59 Selecting A Single Role Per Session

All POS systems connected to the EHRi **must** ensure that each user will access applications and services of the EHRi in a single role (i.e., users who have been registered with more than one non-overlapping role **must** designate a single role during each EHRi session).

Tech Requirement

Rationale: Users who wear many disparate hats need to wear them one at a time. For example, a general practitioner who works in the Emergency Department of a rural hospital one day a week (and who has emergency override privileges while on duty) must clearly indicate to the POS system when she is acting in this capacity and must do so prior to accessing a patient/person's EHR via the EHRi. Another example would be an EHRi user accessing EHRi records as a clinician and also sometimes as a researcher.

A hierarchical organisation of roles, accommodating users who frequently switch between dual roles that are both related to clinical care, would greatly reduce user frustration from needlessly having to switch between one role and the other. Properly designed roles will ensure that users rarely, if ever, have switch roles by initiating a new session.

Workgroup-Based Access Control

Workgroup-based access control allows users to be assigned to working groups such as:

a) organisations (e.g.: a primary care clinic or a primary health care team in a rural community),

b) organisational units (e.g.: the emergency department of a hospital), or

c) health and social care teams.

Users can then rapidly be given access to all the records of patients in the care of that team. This facilitates the rapid deployment of users who may move frequently from one team to another (for example, based on hospital shifts).

Note that the use here of the phrase "working groups" does *not* refer to membership in a professional association (nurses, say) as this is already covered by role-based access control, as described above. Rather, workgroup-based access control allows a user with a given role (say, family physician) to exercise the access privileges of that role upon all the records accessible by members of the working group (say, patients/persons in a primary care clinic).

Security Requirement 60 Granting Access to Users in Work Groups

The EHRi and all POS systems connected to the EHRi **must** be capable of assigning users to working groups and of granting access to records based on working groups.

Tech Requirement

Rationale: It is unreasonable to assume that all physicians will be able, via the EHRi, to view the EHR of all Canadian patients/persons. At a minimum, VIPs and other selected patients will require restriction of their EHRs to just those individuals who are known members of their healthcare team. This is a privacy protective feature that all Canadians might reasonably expect to protect their PHI from potential access by any arbitrary healthcare provider registered to use the EHRi. This in turn requires some mechanism for obtaining information on a patient/person's relationships with his or her healthcare providers. Such information could be extracted from the patient/person's EHR. In addition, there may be a need to maintain a list of one or more workgroups to which the user is a member. Examples might include surgical teams at a specific hospital or physicians with admitting privileges at a specific hospital. Such workgroups would enable a user's relationship with a patient/person to be inferred from existing relationships between the patient/person and other members of the workgroup.

It is important to note that the EHRi cannot reasonably be the authoritative source of information for all workgroup assignments, as they are too fluid and change too quickly to manage centrally. It is expected that POS systems will track such assignments where necessary (e.g., in a hospital information system) and that the EHRi will rely on this data where available. It *is* expected that the EHRi will be capable of deducing whether a bona fide relationship exists between a patient/person and a healthcare provider where such a relationship can be inferred from the existing PHI (e.g.: where a healthcare provider has already provided care to the patient/person, contributed data to the patient/person's EHR, ordered tests, prescribed medications, etc.).

Note that "Security Requirement 61 Work Groups Do Not Override Roles" has been removed, as it is superfluous; i.e., it logically follows from the definitions above of role based access control and workgroup-based access control.

Security Requirement 62 Timely Revocation of Access Privileges

The EHRi and all POS systems connected to the EHRi **must** support the revocation of user access privileges in a timely manner; i.e. to immediately prevent the user from logging on, after access privileges have been revoked.

Tech Requirement

Revocation of user access privileges does not in itself alter the status of data that the user has already entered. For example, a repeat prescription entered as an e-prescription would remain in force. Punitive revocation of a user's access privileges may need to be accompanied by a review of data entered by the user; such determination must be made on a case-by-case basis.

Rationale: This requirement ensures that user access privileges to the EHRi can be immediately and systematically suspended if there are grounds to do so.

Discretionary Access Control

Discretionary access control is familiar to anyone who has ever used a Windows PC connected to a LAN. The owner of a file is free to grant access rights to the file to others (hence "discretionary" access control). In healthcare, a user who has full access to a record (a responsible physician, say) may need to rapidly grant access to a user who has never had a previous legitimate relationship with the patient (a specialist, say). The patient may not be present or even conscious when this access control decision is made. Discretionary access control occupies a middle ground between the two extremes of, on the one hand, allowing all users in a given role access to a huge pool of electronic health records; and on the other hand, requiring explicit consent for each user to access each record.

Security Requirement 63 Granting Access By Association

The EHRi and all POS systems connected to the EHRi:

a) **must** be capable of associating users (healthcare providers) with the records of patients/persons and allowing future access based on this association; i.e., they must be capable of granting discretionary access to records based on a registered user with legitimate and pre-existing access to a patient's record(s) granting access rights for that (those) record(s) to another registered user;

b) **must not** allow users to grant other users access to a record if the granting users themselves do not possess such access with respect to the record; and

Note that granting other users access to a record does not over-ride the role based access control restrictions of those other users.

Tech Requirement

Rationale: This requirement is essential if Security Requirement 60 is to be made effectively operational. As noted above, discretionary access control does not "trump" role based access control. For example, a family physician can grant another physician (a specialist, say) full access to one of her patient's records. The specialist might later use that access to write an e-prescription for the patient. However, if the physician grants access to a nurse, the nurse cannot later write an e-prescription for the patient, as role based access control would typically prevent nurses from exercising such a function.

Security Requirement 63a Reporting the Access Privileges of a User

The EHRi must – and POS systems connected to the EHRi should – provide functionality that can report, for a given user:

a) which records the user can access;

b) which portions of the record the user can access;

c) which privileges (viewing, modification, etc.) the user has in respect to each of these records.

Rationale: Past experience with popular operating system software has shown how difficult it can be to determine whether a given user can access a given record or exercise a given privilege unless there is an explicit facility within the system to answer such questions. The lack of such a facility can make it extremely difficult to detect and correct errors in the assignment of user access privileges.

5.9.3 User Responsibilities

Security Requirement 64 Acceptable Use Agreements

Organisations connecting to the EHRi must define user responsibilities, make users aware of them and have users agree to them as part of an acceptable use agreement.

Admin Requirement

Rationale: Acceptable use agreements are an important part of ensuring that users are aware of their responsibilities (and hence help to support **Security Requirement 16**) as well as provide the basis for legal redress if users abuse their access rights.

Administrative overhead can be substantially reduced when electronic agreements are used instead of paper.

5.9.4 Network Access Control

Security Requirement 65 Authenticating EHRi Network Access

Organisations hosting components of the EHRi **must** ensure that all EHRi connections to remote servers and applications are authenticated. This includes connections via the Internet.

Tech Requirement

Rationale: This helps to ensure that applications containing PHI are not compromised by masquerading remote servers and/or applications.

Security Requirement 66 Controlling Access to EHRi Network Diagnostics and Network Management Services

Organisations hosting components of the EHRi **must** securely control access to diagnostic ports and services on networks hosting those components.

Tech Requirement

Rationale: This is a minimum requirement for maintaining overall network security.

Security Requirement 67 Segregating EHRi Network Users, Services and Systems

Organisations hosting components of the EHRi **must** introduce network controls to segregate information services, users and information systems that are not involved in access to or hosting of the EHRi.

Tech Requirement

Rationale: Network security plays a fundamental role in preventing unauthorized access to servers, data, and other information assets. An appropriate level of network security needs to be applied to protect EHRi resources. The intent of this requirement is to separate, for example, the hosting of healthcare applications containing PHI from servers hosting applications unrelated to PHI. Network firewalls are a typical example of how network segregation is achieved.

Security Requirement 68 Controlling Routing on EHRi Networks

Organisations hosting components of the EHRi **must** have routing controls[76] on networks hosting those components to ensure that data flows across the network perimeter do not breach the organisation's access control policy.

Tech Requirement

Rationale: This requirement is intended to protect against a variety of denial of service attacks. Most networks today have at least rudimentary routing control implemented in firewalls.

[76] Firewalls are a popular example of routing controls.

5.9.5 Operating System Access Control

Security Requirement 69 Controlling Access to EHRi System Utilities

Organisations hosting components of the EHRi, **must** restrict and control the use of system utility programs.

Tech Requirement

Rationale: This requirement is a hedge against facilitated hacking.

Security Requirement 70 Restricting Connection Times to EHRi Applications

Where appropriate, the EHRi **should** restrict connection duration to EHRi application services to provide additional security for access to those applications.

Tech Requirement

Rationale: This requirement is sometimes used in high security applications to force a reconnect (and hence re-authentication) when a connection has been held open for an excessively long time. The length of time to maintain a connect varies with the nature of the application and the types of connections (e.g.: server to server or client to server). Given the messaging framework defined in the EHRS Blueprint, connections to an EHRi would typically not last more then a few minutes.

5.9.6 Application And Information Access Control

Security Requirement 71 Robustly Authenticating Users

The EHRi and all POS systems connected to the EHRi **must** robustly authenticate users.

Tech Requirement

Rationale: Uncontrolled user access is a frequent enabler of security breaches. Moreover, some level of uniformity in the strength of authentication will likely be needed to support cross-jurisdictional interoperability.

It is important to note that this requirement would likely necessitate the implementation of robust authentication technologies:

1. digital certificates;
2. biometrics;
3. smart cards or other hardware tokens; or
4. standards-based secure and robust password schemes.

It is expected that the EHRi and POS systems connected to the EHRi will work together to accomplish the task of authenticating users who access the EHRi; i.e., users do not need to be authenticated twice.

5.9.7 Workstation Access Control

Mobile devices and wireless connections are changing the very notion of workstations. Nevertheless, some basic security requirements remain for the protection of workstations in healthcare, as these can often be found in areas that can be accessed by patients and other unauthorized personnel. Mobile devices and wireless devices are dealt with in section 5.9.8.

Security Requirement 72 Restricting Access to Unattended Workstations

All POS systems connected to the EHRi **must** protect unattended workstations against an unauthorized person taking the opportunity to use the workstation while the POS is active, either with automatic timeout after a period of inactivity or by placing the workstations in a physically secure area.

Tech Requirement

Rationale: Most systems already implementing this requirement, at least at a rudimentary level (e.g.: automatic timeout after a period of inactivity). Some workstations are positioned in physically secure areas (e.g.: behind the prescriptions dispensing counter in a pharmacy). Proper positioning of workstations also plays a role in ensuring that the patients/persons cannot see the details of other people's records.

5.9.8 Mobile Computing And Teleworking

As noted in ISO/IEC 17799, mobile network wireless connections, while similar to those of wired networks, have some important differences from an information security point of view. Some wireless encryption protocols such as WEP (Wired Equivalent Privacy) are immature and have known weaknesses that render them largely ineffective. Moreover, information stored on mobile devices may not be backed up because of limited network bandwidth or because the devices are not connected at the times when back-ups are scheduled.

Security Requirement 73 Acceptable Use of Mobile Devices

Organisations connecting to the EHRi **should**:

a) prepare policy on the precautions to be taken when using mobile computing devices, including wireless devices; and

b) require their mobile users to follow this policy.

Policy & Procedures

Admin Requirement

Rationale: The use of mobile devices in healthcare is increasing rapidly. Canadian healthcare jurisdictions largely lack effective guidelines on the secure use of mobile devices in healthcare.

Security Requirement 74 Acceptable Use of Teleworking

Organisations connecting to the EHRi **should**:

a) prepare policy on the precautions to be taken when teleworking; and

b) prohibit teleworking by a POS user unless the user agrees to abide by this policy.

Policy & Procedures

Admin Requirement

Rationale: The use of teleworking in healthcare is widespread. Canadian healthcare jurisdictions largely lack effective guidelines on the secure use of teleworking in healthcare.

Security Requirement 75 Protecting Wireless Networks

Organisations hosting components of the EHRi or connecting to the EHRi **must** protect wireless connections from unauthorized access or misuse.

Tech Requirement

Rationale: Application of wireless networking to healthcare needs to be done securely to prevent interception and decryption of wireless network traffic and to protect against end-user masquerade, man-in-the-middle attacks, access point spoofing, session hijacking, and potentially denial of service. All of these can be addressed through the use of encryption. It should also be noted that wireless connections make physical security boundaries ineffective. This, combined with **Security Requirement 31** (**Encrypting PHI During Transmission**) implies that all wireless communication of PHI be encrypted. The requirement above makes this implicit requirement explicit.

5.10 Information Systems Acquisition, Development and Maintenance

The objectives of information systems acquisition, development and maintenance security are to:

1. ensure security is built into operational systems;
2. prevent loss, modification or misuse of user data in application systems;
3. protect the confidentiality, authenticity, availability and integrity of information;
4. ensure IT projects and support activities are conducted in a secure manner; and
5. maintain the security of application system software and data.

5.10.1 Security Requirements Of Information Systems

The requirements of the EHRi are summarised in the table in section 2.2.3.

5.10.2 Correct Processing Of Information

Security Requirement 76 Uniquely Identifying Patients/Persons

The EHRi and POS systems connected to the EHRi **must:**

a) ensure that patients/persons are assigned an identifier (patient ID) that can uniquely identify the patient/person within the EHRi or within the POS system, and

b) must be capable of merging two or more EHR records if it is determined that multiple records for the same patient/person have been unintentionally created.

Tech Requirement

Rationale: Although painfully obvious, the need to uniquely identify patients/persons has significant consequences for the operation of the EHRi, including the need to manage multiple identifiers, possibly map those identifiers to a unique internal identifier, and merge records where it is determined that they both belong to the same individual and that separate records have been unintentionally created.

In addition to the unique patient identifiers referred to above, the EHRi might also support additional so-called "meaningless but unique identifiers" and to manage these internal identifiers separately from publicly available identifiers in order to provide for default depersonalization. Discussion of internal identifiers and other technical means of achieving anonymisation and pseudonymisation is outside the scope of this document.

5.10.2.1 Input Data Validation

Security Requirement 77 Validating Input Data

The EHRi and all POS systems connected to the EHRi **must** include, wherever feasible, measures to safeguard against user error by validating data input to ensure that it is correct and appropriate. The following controls **should** be considered:

a) input checks to detect the following errors:
   1) out-of-range values;
   2) invalid characters in data fields;
   3) missing or incomplete data;
   4) exceeding upper and lower data volume limits;
   5) unauthorized or inconsistent control data;
b) procedures for responding to validation errors.

Tech Requirement

Rationale: This is a minimum requirement to promote data integrity.

5.10.2.2 Output Data Validation

Security Requirement 78 Validating Printed Data

All POS systems connected to the EHRi **should** ensure it is possible to check that hardcopy print-outs are complete (e.g.: "page 3 of 5").

Tech Requirement

Rationale: This is a minimum requirement to promote data integrity. It prevents covert selective presentation of data.

5.10.3 Cryptographic Controls

To the extent that the EHRi supports the replacement of paper-based prescriptions, a facility for the application, recognition and verification of digital signatures will be among the services provided by the EHRi, as Canadian law requires that prescriptions be signed.[77] Although the principle use of digital signatures would probably be for e-prescribing, there are many other less common situations where the signature of a physician might be required upon a form (for example, death certificates). Processing of these other paper based forms would also benefit from augmentation with e-forms and the concomitant use of digital signatures by physicians. Finally, digital signatures play an important role in providing so-called "security assertions" – reliable attestations that a given user or system has a given attribute.

In addition to physicians, many other users might benefit from a digital signature capability; for example, registration clerks, administrators, and users renewing their access or requesting changes in registration details. As well, digital signatures can themselves form the basis of an effective two-factor authentication methodology as per **Security Requirement 71** (**Robustly Authenticating Users**), and so can fulfil this function as well as provide for signature capability.

[77] Regulations under the Food and Drug Act require that prescriptions be either in writing or verbal:

> *G.03.002. No pharmacist shall, except as otherwise provided in this Part, dispense a controlled drug to any person unless he has first been furnished with a prescription therefore, and*
>
> *(a) if the prescription is in writing, it has been signed and dated by the practitioner issuing the same and the signature of the practitioner where not known to the pharmacist, has been verified by him; or*
>
> *(b) if the prescription is given verbally, the pharmacist has taken reasonable precaution to satisfy himself that the person giving the prescription is a practitioner.*

Security Requirement 79 Providing Digital Signatures for Users

All POS systems connected to the EHRi providing functions where users are required to apply the electronic equivalent of a handwritten signature **must:**

a) allow such POS users to apply a digital signature that satisfies the requirements under PIPEDA and its regulations[78] for an "electronic signature";

b) store, backup or archive the digital signature whenever the signed data is stored, backed up or archived;

c) transmit the digital signature whenever the signed data is transmitted; and

d) allow all POS users to confirm, whenever they access signed data, that the signature is valid (i.e., that the associated signature certificate has not been revoked).

Tech Requirement

Rationale: This is a minimum requirement for the provision of e-prescribing and other services where an authorized signature is required. Note that PIPEDA is not the only Canadian legislation that gives authority to digital signatures. Several provinces and territories have also enacted legislation allowing for the use of a digital signature where pen-and-ink signatures were previously required. Health Canada is currently investigating the possibility of amending the Food and Drug Act to allow the use of digital signatures on prescriptions.

Security Requirement 80 Validating and Preserving Digital Signatures On PHI

Whenever the EHRi receives data containing a digital signature that satisfies the PIPEDA's electronic signature requirements, the EHRi must:

a) confirm upon receipt that the signature is valid (i.e., that the associated signature certificate has not been revoked);

b) preserve the digital signature whenever the signed data is stored, backed up or archived;

c) transmit the digital signature whenever the signed data is transmitted; and

d) confirm before transmission that the signature was valid at the time it was applied (e.g.., that the associated signature certificate had not been revoked);

Tech Requirement

Rationale: This is a minimum requirement for the provision of e-prescribing and other services where an authorized signature is required.

5.10.4 Security Of System Files

Security Requirement 81 Implementing Software and Upgrades in the EHRi

Organisations hosting components of the EHRi **must** put procedures be in place to control the implementation of software and upgrades on operational systems hosting these components.

Policy & Procedures

Admin Requirement

Rationale: Change control is a minimum requirement for protecting the security of operational systems.

[78] The technical requirements for electronic signatures are defined in "Secure Electronic Signature Regulations", Canada Gazette, vol. 138, no. 19, May 8 , 2004.

See also **Security Requirement 28** for other requirements on upgrading the EHRi.

5.10.5 Security In Development And Support Processes

Security Requirement 82 Protecting EHRi Software

Organisations hosting components of the EHRi **must** maintain control over access to program source libraries for EHRi components where such libraries are within the control of the organisation.

Tech Requirement

Rationale: This requirement is a hedge against facilitated hacking and is a basic requirement.

5.10.6 Vulnerability Management

Security Requirement 83 Managing Known Vulnerabilities

Organisations hosting components of the EHRi **must** take steps to test for and prevent the exploitation of published vulnerabilities in systems and software that host those component.

Tech Requirement

Rationale: This requirement prevents the exploitation of known vulnerabilities in systems that have not been updated with currently available security patches. It also mandates that security patches which fix known security problems either be applied when available or else effective alternative steps be taken to address the security problem. Effective security vulnerability management of new or significantly upgraded systems and software should also include penetration testing.

5.11 Security Incident Management

The objectives of security incident management are to:

1. build a reporting infrastructure for reporting incidents and weakness; and
2. manage incidents and institute improvements to prevent their future occurrence.

5.11.1 Reporting Incidents And Weaknesses

Security Requirement 84 Reporting Security Incidents Involving the EHRi

The EHRi **must –** and all POS systems connected to the EHRi **should** – trigger a notification to the accountable person specified in **Security Requirement 3** of every detected pattern of system misuse (see **Security Requirement 46**)

Tech Requirement

Rationale: Ultimately the decision of who the responsible person would be is a governance issue for the organisation.

Though a technical requirement, legacy POS systems may need to be augmented by administrative procedures to overcome limitations in their capacity to carry out automated notifications.

See also Privacy Requirement 20 (Notifying Patients/Persons of Inappropriate Access, Use or Disclosure).

5.11.2 Management Of Incidents And Improvements

Security Requirement 85 Responding to Security Incidents Involving the EHRi

Organisations hosting components of the EHRi **must** establish incident management responsibilities and procedures to ensure a quick, effective and orderly response to security incidents and to collect and preserve incident-related data such as audit trails, logs and other evidence.

Policy & Procedures

Admin Requirement

Rationale: This is a minimum requirement. Security incident management procedures are intended to restore normal EHRi operations in a timely manner, and to minimise any loss of confidentiality or data and system integrity. Legal requirements also arise from the Ontario Regulations that require notifying a patient/person at the first reasonable opportunity if the patient/person's information is stolen, lost or accessed by unauthorized persons.

5.12 Business Continuity Management

The objective of business continuity management is to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

Security Requirement 86 Managing Business Continuity

Organisations hosting components of the EHRi **must** put in place a managed process for developing and maintaining business continuity throughout the organisation, including:

a) developing a strategic plan, based on appropriate risk assessment, for the overall approach to business continuity;

b) developing written plans to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes relating to the EHRi; and

c) maintaining a unified framework of business continuity plans to ensure that all plans are consistent, and to identify priorities for testing and maintenance.

Policy & Procedures

Admin Requirement

Rationale: A managed process for developing and maintaining business continuity is a minimum requirement. An overarching framework tied to a risk assessment is a requirement of effective business continuity management. Written plans (item b) are a requirement of effective business continuity management. Item c is intended to integrate business continuity planning in IT systems with broader plans to maintain services to patients.

Organisations hosting components of the EHRi will need multiple business continuity functions and they will all need to be addressed in a comprehensive manner to ensure the EHRi access and functionally are continually maintained.

Security Requirement 87 Testing Business Continuity Plans

Organisations hosting components of the EHRi **must** regularly test and maintain business continuity plans by regular reviews to ensure that they are up to date and effective.

Policy & Procedures

Rationale: The actual testing of business continuity plans is both essential and often difficult to carry out, especially in small organisations.

5.13 Compliance

The objectives of compliance in information security management are to:

1) avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements;
2) ensure compliance of systems with organisational security policies and standards; and
3) maximize the effectiveness of and minimize interference with/from the system audit process.

5.13.1 Compliance With Legal Requirements

The legal requirements for the EHRi are discussed throughout this document.

5.13.2 Compliance With Security Policies And Standards

Security standards for the EHRi are discussed in a separate document (see the document map in Figure 1 Context for this document)

Compliance to jurisdictional IT security polices and standards are outside the scope of this document.

5.13.3 Information Systems Audit Considerations

Audit standards for the EHRi will be based on jurisdictional requirements and standards.

APPENDIX A Privacy And Security Implications Arising From Use Case Analysis

In the report *Electronic Health Record Privacy and Security Use Cases,* the privacy and security considerations involved in a wide range of realistic health care scenarios were examined in detail. The document focused on scenarios relevant to the implementation of *Infoway's* EHR architecture. Its analysis showed, in general, how each type of use can be accomplished in a secure and privacy-protective manner. Section 7 of the document summarized aspects requiring further analysis, as well as problematical special cases. Readers of that document may wish to follow the further development of these ideas in the corresponding subsections below, where the privacy and security issues dealt with previously are related to the relevant requirements detailed in the current document.

A.1 Privacy and Security Implications Connected With Actors

Many issues were raised during the use case analysis that related to the designation of roles to individual users for the purposes of grouping them for privacy and security purposes. These issues included the following:

1. **No Agreed Upon Roles for Role Based Access Control**
   There is no agreed upon set of healthcare roles in any Canadian jurisdiction that covers all healthcare providers. Moreover, the definitions and uses of roles can be context based and vary in meaning and application from one jurisdiction to another (indeed, between one hospital and another within the same jurisdiction).
2. **Recognition for Regulated Healthcare Professionals Vary Among Jurisdictions**
   Some groups of healthcare providers may have professional standing in one Canadian jurisdiction but not in another (e.g. midwives).
3. **No Agreed Upon Mapping from Roles to Privileges**
   Even when roles are accepted across Canada as professional designations (e.g.: "physician" and "nurse") there is ongoing debate concerning the specific separation of duties among these roles (e.g.: the role of nurses in the medical decision making process and the concomitant level of access required to a patient/person's EHR in order for a nurse to properly perform his/her duties as they relate to that decision making process).
4. **Emergency Override Privileges Can be Difficult to Determine**
   In some cases, the role of emergency care provider may be situational. In rural areas, for example, a primary healthcare provider may be "on call" at the local hospital's emergency clinic one or two nights a week. Their role may therefore be "emergency care provider" on Monday and Thursday nights, and "primary care provider" at other times. Although the role of emergency care provider could be construed as being tied in part to a location (in this case, the emergency department of a local hospital), this too may be problematic. Paramedics are an example of a role that has emergency access that is not tied to the location of an emergency department.
5. **Provider Registries are Incomplete**
   Currently no operational online federal, provincial, or territorial registry contains an exhaustive listing of all healthcare providers who are regulated professionals within the jurisdiction (although some are close to achieving this goal).

6. **Not All Users Will Be Regulated Health Professionals**
   There are individuals involved in healthcare who are not recognized professionals in any jurisdiction. For example, medical receptionists play an important role in maintaining demographic and emergency contact information, as well as in scheduling appointments for patients/persons. Some of this information may be highly personal and confidential[79], but no Canadian jurisdiction regulates medical receptionists nor is any likely to do so in the near future.
7. **Substitute Decision Makers May Require Identification**
   Substitute decision makers may be required to make decision concerning treatment, as well to make decisions concerning the patient/person's consent directives. For example, substitute decision maker would need to decide which other family members could be notified of a patient's medical condition if the patient was unable to communicate or was incapable of making decisions on their own behalf. In such situations, it may be necessary to verify the identity of the patient as well as the substitute decision maker.
8. **Identification of Systems, Servers, and Applications**
   How uniquely should such systems be identified? For example, a CIS may operate at several different clinic sites. Must each access from the clinic's CIS to the EHRi be uniquely identified as to which site is making the access or does it suffice to simply identify the clinic? In deployments of HIS and CIS that involve both distributed and centralised server configurations, such identification issues are not trivial to resolve.
9. **Keeping PHI from System and Administrative Personnel**
   EHRi system administrators may have access to PHI that they are not authorized to retrieve; either directly via system tools other than the application level user interface or via integration engines that process and exchange information. System level testing, diagnosis and maintenance should be done, to the greatest extent possible, using test data, not actual PHI. An EHRi that effectively encrypts such PHI during storage and when in transit could avoid these unintended disclosures to system personnel and other insiders (albeit with attendant overhead in administration and processing) but there are many other options as well, including decoupling of personal identifiers from healthcare information.[80]
10. **Keeping PHI from Unauthorized Third Parties**
   Unauthorized third parties may retrieve or even alter PHI in transit (e.g., by intercepting unencrypted transmission of data), in repositories (e.g., by "hacking" into database repositories), or in storage on secondary media (e.g., by obtaining unencrypted data backups or data archives). Hackers are not the only unauthorized third parties who have obtained access to PHI. It has also been unintentionally disclosed to improperly supervised contractors and other "legitimate" third parties who have exploited flaws in system design, policy, or procedures to gain access to personal health data.

[79] As discussed in *Electronic Health Record Privacy and Security Use Case, d*emographic information and appointment schedules may contain a wealth of personal information that would be regarded by the data subject as highly confidential. For example:
a) an individual seeking treatment after escaping from an abusive spouse might be gravely concerned about the confidentiality of her new phone number and address;
b) a middle aged male patient whose emergency contact data refers to another male at the same address and home phone number as the patient might be concerned that inferences could be drawn from such data about his sexual orientation; and
c) a patient scheduled for an appointment at a drug rehabilitation clinic might concerned about inferences drawn about the patient being dependant on drugs or alcohol..

[80] Most privacy legislation does not allow for—nor does it address—these types of unintended disclosures. Such disclosures could create significant problems in the context of an interoperable EHRi, given that they normally occur below the level of system access where audits occur and therefore are not documented and subsequently cannot be monitored.

Issues 1 to 3 and 5 to 6 are essentially problems in role based access control and they are not directly addressed by the privacy and security requirements described in sections 4 and 5, although several security requirements mandate the use of role based access control (**Security Requirement 58**, **Security Requirement 59**, and **Note that "Security Requirement 61**). Resolving the problems discussed in issues 1, 2, 3, 5, and 6 will be critically important to the establishment of an interoperable EHRi.

Issue 4 (determining emergency override privileges) is effectively addressed by the combination of several security requirements:

- **Security Requirement 58** requires a user with access to emergency override functions to be assigned at least one user role that has access to these emergency override functions.
- **Security Requirement 59** requires a user with multiple roles to specify at the beginning of the online session which role the user is exercising. This ensures that a user who does not work exclusively in an emergency department will not have access to emergency override functions while working in a non-emergency setting (e.g., when providing family medicine in a physician practice).
- **Security Requirement 43** specifies that the role exercised by the user while performing an action (e.g.: accessing or updating a record) must be logged in an audit trail. Users whose roles include a role with access to emergency override functions and who invokes that role in a non-emergency situation in order to exercise those emergency override functions may therefore be subject to disciplinary procedures based upon the evidence provided by the audit log.

Issue 7 (identifying substitute decision makers) is dealt with in **Privacy Requirement 15** and **Security Requirement 43 Minimum Content of Audit Logs**.

Issue 8 (Identifying systems, servers, and applications) has been studied carefully and a determination has been made that there is no P&S requirement to uniquely identify applications, systems, or servers. All users are registered and uniquely identified (c.f. **Security Requirement 54** and **Security Requirement 55**) and all organisations connecting to EHRi are also identified and their access logged as appropriate (**Security Requirement 43 Minimum Content of Audit Logs**), but there is no essential need – from a privacy or security viewpoint – to identify systems, servers or applications.

Issue 9 is effectively dealt with by a combination of many security requirements, including:

- **Security Requirement 12**,
- **Security Requirement 13**,
- **Security Requirement 15**,
- **Security Requirement 16**,
- **Security Requirement 17**,
- **Security Requirement 25**,
- **Security Requirement 26**,
- **Security Requirement 45**,
- **Security Requirement 51**, and
- **Security Requirement 52**.

Issue 10 (keeping PHI from unauthorized third parties) is dealt with by the combination of the following security requirements:

- **Security Requirement 19**,
- **Security Requirement 20**,
- **Security Requirement 21**,
- **Security Requirement 22**,
- **Security Requirement 23**,
- **Security Requirement 24**,
- **Security Requirement 29**,
- **Security Requirement 30**,
- **Security Requirement 31**,
- **Security Requirement 32**,
- **Security Requirement 34**,
- **Security Requirement 35**,
- **Security Requirement 36**,
- **Security Requirement 51**,
- **Security Requirement 52**,
- **Security Requirement 66**,
- **Security Requirement 67**,
- **Security Requirement 68**,
- **Security Requirement 69**,
- **Security Requirement 70**,
- **Security Requirement 71**,
- **Security Requirement 72**,
- **Security Requirement 75**,
- **Security Requirement 82**,
- **Security Requirement 83** and
- **Security Requirement 85**.

A.2 Privacy and Security Implications Connected With Use Cases

Several issues are raised by the use cases described in *Electronic Health Record Privacy and Security Use Cases*:

1. **Matching The Patient/Person Being Treated to the Record Retrieved**[81]

   Before relying on information provided by an EHR, healthcare providers need access to sufficient information to ensure that the patient/person matches the EHR). Matching a patient/person under treatment to an existing record can be a non-trivial task. Some POS systems enhance security by including photo ID of the patient/person belonging to the record. Such enhancements may themselves create privacy problems, as they potentially permit the implicit capture of facial characteristics such as race that are not included as fields of data. The requirements for patient/person identification and the data used to support it may also vary from jurisdiction to jurisdiction.

   The provision of emergency care and other situations in which adequate patient identification may not have been possible will inevitably create instances of multiple records for the same patient/person. There must therefore be some capacity within the EHRi to merge multiple instances of patient records into a single record. Such merging requires the greatest care and will therefore necessitate not only personnel trained in such merging, but may also require technical tools to better facilitate the integration of information from the original records into a unified whole.

   Security Requirement 76 addresses this need for unique identification of patients/persons and for the ability to merge records that belong to the same patient/person.

2. **Applying Authentication Technologies to Users In A Healthcare Setting**[82]

   Beyond simple password systems, many technologies that are more sophisticated fail in a healthcare environment. For example, latex gloves rule out the use of fingerprint identification systems (unless the user is subjected to the cumbersome and time consuming effort of removing a glove, authenticating, and then putting on a new glove) and surgical masks prevent face recognition software from functioning. Authentication technologies must be carefully chosen from among those that have a proven track record in the healthcare settings for which they are intended.

   Jurisdictional practices may also vary and a common standard of trust in support of interoperability may require minimum standards for EHRi user authentication. As well, the interactions between local authentication performed by POS applications and the EHRi (and its requirements for authenticated user access to support audit logging) have yet to be architected and the wide variety of POS applications currently in use will make this a challenging task.

   Security Requirement 71 addresses the issue of robust authentication.

[81] See Use Case 6.1 "Confirm Patient/Person Identification" in *Electronic Health Record Privacy and Security Use Cases.*

[82] See Use Case 6.2 "Authenticate EHRi user" in Electronic Health Record Privacy and Security Use Cases.

3. **Authorizing EHRi Users**[83]

Authorization of EHRi users is made difficult by the sometimes fluid nature of healthcare provisioning. For example, membership in a patient/person's healthcare team may be highly dynamic and change daily as specialists are called upon to perform specialized tests on the patient and rule out differential diagnoses. A patient/person may be closely involved today with a healthcare provider that they had never before met. This complexity is further exacerbated in a multi-jurisdictional environment. As EHRs become increasingly interoperable and the number of EHR users grows, so to does the risk of inappropriate access. Whenever a request to retrieve a patient/person’s EHR is initiated from a jurisdiction where a patient/person has not received care in the past, some additional authorization mechanisms may need to be invoked.

Finally, the EHRi will rely to a great extent on the functional information provided by the local POS application about the function that the user is attempting to perform (or the system the user is attempting to access). The structure of these transactions and the data model to support them has not been consistently architected.

These issues are addressed by the following requirements:

- **Privacy Requirement 5**,
- **NOTE: Privacy Requirement 6**,
- **Security Requirement 53**,
- **Security Requirement 54**,
- **Security Requirement 55**,
- **Security Requirement 56**,
- **Security Requirement 57**,
- **Security Requirement 58**,
- **Security Requirement 59**,
- **Security Requirement 60**,
- **Note that "Security Requirement 61**,
- **Security Requirement 62**,
- **Security Requirement 63**, and
- **Security Requirement 64**.

4. **Grouping PHI for Privacy Purposes**[84]

The division, for the purposes of privacy protection, of various types of information in a patient/person's EHR into categories such as demographic information, medical history, mental health data, etc. may have practical implications for the administration of features that allow certain types of personal health information to be masked or locked upon receipt of (or by means of) consent directives from the data subject (i.e., the patient/person).

[83] See Use Case 6.3 "Authorize EHRI user" in Electronic Health Record Privacy and Security Use Cases.

[84] See Use Case 6.5 "Retrieve Patient/Person's EHR" and Use Case 6.6 "Update Patient/Person's EHR" in *Electronic Health Record Privacy and Security Use Cases.*

The specifics of this issue is not addressed by any of the requirements, although **Privacy Requirement 8**, **Privacy Requirement 9**, **Privacy Requirement 10**, **Privacy Requirement 11**, and **Privacy Requirement 12** specify that consent data be captured by POS systems and transmitted to the EHRi when transmitting the underlying PHI. The appropriate grouping of data elements for the purposes of applying consent directives will be studied further in a later stage of Infoway's P&S project.

5. **Maintaining Confidentiality And Integrity Of PHI In Storage And Transit[85]**

Maintaining the confidentiality and integrity of data in transit is essential for maintaining privacy and security. Encryption technology is now routinely applied to network traffic to protect its passage across networks such as the Internet[86], The enduring confidentiality of PHI and the low cost of storing huge volumes of intercepted network traffic combine to place stringent demands on the cryptographic protection of PHI during transmission.

This issue is reflected in **Security Requirement 31**, **Security Requirement 32**, and **Security Requirement 33**.

Maintaining the confidentiality and integrity of data in storage, backup and archive is made more difficult by the still infrequent use of encryption to protect PHI in storage, and by the difficulty of providing effective physical security for the servers in smaller clinics and physician offices that host POS applications.

Security Requirement 18, **Security Requirement 21**, **Security Requirement 34**, **Security Requirement 36**, and **Security Requirement 37** address this issue.

6. Conferring Access[87]

An interoperable EHRi requires mechanisms for conferring access to a patient/person's EHR from one healthcare provider to another (e.g.: from a primary care provider to a specialist to whom the patient/person is being referred). The proper architecting of such mechanisms, the policies for their use, and the auditing of their use are all essential for the maintenance of privacy and security.

The issue of conferring access is addressed in **Security Requirement 63**. Auditing is dealt with in the following requirements:

- **Security Requirement 38**,
- **Security Requirement 39**,
- **Security Requirement 40**,
- **Security Requirement 41**,
- **Security Requirement 42**,
- **Security Requirement 43**, and

[85] See Use Case 6.5 "Retrieve Patient/Person's EHR" and Use Case 6.6 "Update Patient/Person's EHR" in *Electronic Health Record Privacy and Security Use Cases.*

[86] The application of encryption to protect network traffic can create so-called Virtual Private Networks (VPNs) out of the public Internet.

[87] See Use Case 6.7 in Electronic Health Record Privacy and Security Use Cases.

- **Security Requirement 52**.

7. **Support for Digital Signatures**[88]

To the extent that the EHRi allows the delivery of e-prescriptions from prescribing healthcare providers (e.g.: physicians) to dispensing healthcare provider (e.g.: pharmacists) there will be a need for the EHRi to support digital signatures. This in turn will require, on a technical level, the recognition of valid Certification Authorities and the capacity to check for certificate revocation. It will also require consistent policies and procedures for issuing digital certificates that meet the high standards of digital certificate issuance demanded of e-prescribing. Issuing digital certificates to e-prescribers will be a non-trivial undertaking.

Digital signatures are addressed in **Security Requirement 79** and **Security Requirement 80**.

8. **Alerting Healthcare Providers of Critical Results**[89]

The EHRi will include an alerting/notification function, which, when a certain specified condition is met, sends an alert/notification to an EHRi user. In addition to the liability implications if an alert is not properly delivered, there may be privacy and security implications if alerts are misrouted or are forwarded to other healthcare providers against the patient/person's consent directives. It is important to note that laws provide for custodians to override consent directives.

The architecting of the alerts function must be carefully constructed to preserve the privacy of patient/persons. The issue of alerts is discussed in **Security Requirement 84** and the responsibilities of organisations to provide responsible individuals to respond to alerts is addressed in **Privacy Requirement 1** and **Error! Reference source not found.**.

The right of patients/persons to be notified of inappropriate access, use or disclosure— should it occur— is addressed in **Privacy Requirement 20**.

9. **Allowing Patient/Person Access to Portions of their EHR**[90]

It is unclear to what extent patients'/persons' access can ever be provided via direct online access to clinical information, i.e., without the mediating influence of a primary care provider to interpret the record's content, provide counselling, and help the patient/person understand the healthcare implications of the record's contents. There may however be portions of the record that might be amenable to direct (i.e., unmediated) access; demographic data is a prime example. What remains outstanding is the issue of which PHI is amenable to unmediated access.

The requirements do not address the issue of facilitating unmediated access to EHR data but the right to (mediated) access is confirmed by **Privacy Requirement 24**.

Some jurisdictions also allow patients/persons to challenge the accuracy and/or completeness of their personal health information. If patients/persons are provided with access to their EHR, even in a limited or mediated fashion, the EHRi may need to include a mechanism to facilitate conformance with this legal requirement, as well as ensure organisations respond to such requests within the legally permitted amount of time. Failure to facilitate such challenges to

[88] See Use Case 6.23 in Electronic Health Record Privacy and Security Use Cases.
[89] See Use Case 6.19 et al. in Electronic Health Record Privacy and Security Use Cases.
[90] See Use Case 6.26 in Electronic Health Record Privacy and Security Use Cases.

accuracy and/or completeness in a secure electronic fashion may lead patients/persons to attempt to communicate sensitive personal health information they believe to be inaccurate or incomplete to their healthcare provider using potentially less secure means, such as email or fax.

The issue of challenging accuracy is effectively addressed by the combination of **Privacy Requirement 24**, **Privacy Requirement 25**, and **Privacy Requirement 26**.

10. **Establishing User Roles**[91]

Although many healthcare providers are regulated healthcare professionals whose credentials can be obtained from regulatory colleges, other actors such as medical receptionists draw their authority to retrieve or update portions of the EHR (demographic information for example) from a healthcare custodian (for example, a physician in a solo practice who has employed the receptionist). Maintaining this "chain of authority" back to a regulated healthcare professional or officially recognized custodian 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 user registration process and hence may add considerable complexity to the simpler model of relying on provider registries drawn from the licensed credentials of the jurisdictional regulatory colleges.

This issue is addressed by **Security Requirement 54** which specifies that user registration practices effectively maintain the chain of authority discussed above. The specific details of these registration practices is beyond the scope of this document.

11. **Reviewing Logs**[92]

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/intra-jurisdictional systems and inter-jurisdictional systems such as HIAL[93] are not addressed in the EHRS Blueprint. Responsibilities must be carefully delineated so that the entire EHRi remains continuously defended against intrusion. Even routine (i.e., non-real-time critical) logging of events merits routine, scheduled review and analysis and this too raises issues around responsibility for episodic audit of inter-jurisdictional information flows on a regular and timely basis.

The general issue of audit log review is addressed in **Security Requirement 52** and the need for continuous audit logging in **Security Requirement 45**. Notification of critical events is addressed in **Security Requirement 84** and the issue of dealing with security incidents is addressed in **Security Requirement 85**. The detailed delineation of responsibilities between local/intra-jurisdictional systems and inter-jurisdictional systems such as HIAL are beyond the scope of this document, but as noted above, such delineation must be made clear and

[91] See Use Case 6.35 in Electronic Health Record Privacy and Security Use Cases.

[92] See Uses Cases 6.42 "Log Invalid Attempts at Authentication", 6.43 "Analyze Log for Intrusions and Misuses", and 6.46 "Notify Information Security Officer" in *Electronic Health Record Privacy and Security Use Cases.*

[93] The Health Information Access Layer (HIAL) is defined in the *EHRS Blueprint* as an interface specification for the EHR Infostructure (OSI Layer 7) that defines service components, service roles, information model and messaging standards required for the exchange of EHR Data and execution of interoperability profiles between EHR Services.

unambiguous as EHRi projects are implemented across Canada if the EHRi is to remain continuously defended against intrusion.

A.3 Consent

1. **Differing Models of Consent**
   Consent requirements vary between provinces and the EHRi must accommodate all these jurisdictional consent models.

   Some uses or disclosures in one province may require express consent, while in another they require implied consent[94]. Depending on a patient/person's location, legislation may require express, implied, or no consent for a particular collection, use, or disclosure of PHI. An EHR architecture that is usable in more than one jurisdiction must be able to accommodate different consent models among jurisdictions, as well as provide interoperability among these differing models. The concept of informed or knowledgeable consent will introduce an additional level of complexity to this issue.

   The issues surrounding consent are addressed in the following requirements:

   - **Privacy Requirement 8**,
   - **Privacy Requirement 9**,
   - **Privacy Requirement 10**,
   - **Privacy Requirement 11**,
   - **Privacy Requirement 12**,
   - **Privacy Requirement 13**,
   - **Privacy Requirement 14**,
   - **Privacy Requirement 15**, and
   - **Privacy Requirement 16**.

   Jurisdictional differences among the type of consent required (e.g.: deemed, express, implied) are not directly addressed in the requirements but the architecture of the EHRi must support all these consent models. These architectural implications are addressed in *Electronic Health Record (EHR) Privacy and Security Services*[95].

2. **Locking and Masking**
   The EHRi, and the systems connected to it, will need to be designed in such a manner that a patient/person can lock/mask specific elements of PHI so as to prevent access and disclosure. Consent directives can be overridden by authorized users in specific situations. All such overrides must be logged and alerts should be created and sent to individuals responsible for

[94] Some jurisdictions, such as Alberta, do not use the notion of implied consent in their health information legislation. Consent is either express and informed, or it is not required in specified circumstances. Alternatively, Ontario's health information legislation allows for implied consent in specified circumstances where the legislation requires consent.
[95] See 2.2.2 (Context for privacy and security requirements analysis).

that individual’s privacy oversight (e.g. a CPO).[96] Patients/persons will need to be able to view all such overrides of their consent directives and the reasons for such overrides.

Locking/masking of access and disclosure of PHI are addressed in **Privacy Requirement 12**, **Privacy Requirement 13**, **Security Requirement 38**, and **Security Requirement 43**.

3. **Opting Out of the EHR**
Whether or not patients/persons can “opt-out” of the EHR, or specific aspects of it (e.g., consent to participate in a client registry), is an outstanding issue in some jurisdictions.

This issue is beyond the scope of Infoway's P&S project.

4. **De-identified/Pseudonymized Data**
If data is irreversibly pseudonymized, individuals will not be able to adjust their consent directives for this de-identified data, although the standard for de-identification varies between provinces and re-identification might be possible in some jurisdictions and under certain circumstances.

Standards for pseudonymization are beyond the scope of this document but are discussed further in *Electronic Health Record (EHR) Privacy and Security Standards Review*.

5. **Who Will be Authorized to Manage Consent Directives?**
Healthcare providers (both individuals and organisations) will be responsible for informing patients/persons of the potential implications of their consent decisions. But would it be reasonable, for example, for an ADT clerk to lock/mask a patient/person’s mental health history or HIV status from future access or disclosure?

This issue is at least partly addressed in **Privacy Requirement 8** and **Privacy Requirement 16**. Policies and best practices for obtaining consent from patients/persons are beyond the scope of this document as is the policy decision that specifies which EHRi user roles will be enabled to record and update consent directives.

6. **Granting Consent**
An ability to "Grant Consent" would need to be included in the consent management functions (along with "Withhold Consent" and "Revoke Consent") to allow for the documentation of express consent, where required.

Consent management functions are discussed fully in *Electronic Health Record (EHR) Privacy and Security Functions and Services*.

7. **Presumption of Implied Consent**
In jurisdictions where implied consent is required for collection, use or disclosure of PHI, it will be presumed that organisations will fulfill the requirements for implied consent (either knowledgeable or informed – e.g. informing patients of their rights) prior to EHRi users accessing, modifying or storing PHI via the EHRi.

The default value for the type of consent gathered will vary by jurisdiction and EHRi consent management functions will need to take these variations into account. The issue is further discussed in *Electronic Health Record (EHR) Privacy and Security Functions and Services.*

[96] Normally the system would inform an institution or organisation's CPO. In the case of a sole practitioner, she/he may be the privacy representative for her/his clinical practice.

8. **Potential Privacy Invasiveness Of Consent Registries And Related Technology**
   While some patients/persons will in principal withhold or otherwise carefully manage their consent to who accesses their PHI, others will do so because they have concerns about protecting the confidentiality of specific information contained in their EHRs. It is essential that technical solutions like consent registries do not themselves become the target of security breaches. If they are not carefully architected, such registries could become tempting targets for hackers; acting in effect as a list of which patients/persons might have — or where to find — the most confidential PHI.

The definition of PHI in section 1.6.1 clearly includes consent directives and such data is therefore included in the provisions of all the requirements that address PHI.

A.4 Other Issues

1. **Usability**
   Consultations by Infoway on end user acceptance strategy for the EHR were held with stakeholders on October 14-15, 2004.[97] One of the barriers to adoption identified by stakeholders was the difficulty users have juggling access to multiple information systems, each with its own log in procedures. User authentication schemes (and other security mechanisms that users are exposed to) must not become a barrier to deployment and use.

   All of the privacy and security requirements have been carefully crafted to ensure that they can be met without constructing barriers against use. The authors are confident that a privacy and security architecture for the EHRi can meet all the requirements above. Construction of the P&S conceptual architecture is discussed in section 2.2.

2. **Supporting the Custodial Responsibilities of Healthcare Providers**
   Privacy and data stewardship issues will be barriers to adoption of EHR solutions if such solutions do not support custodial responsibilities of healthcare providers to protect the privacy of patients/persons and maintain the confidentiality of their data. At the very least, EHR solutions must honour the legislative requirements imposed on providers. Privacy protective EHR solutions can be a positive benefit to healthcare providers in ensuring these custodial responsibilities are continuously met.

If the EHRi and POS systems meet the P&S requirements, they will help to ensure that the custodial responsibilities of healthcare providers using these systems will also be met. All of the requirements taken together therefore address this issue.

3. **Obtaining an Unbiased Second Opinion**
   A fully interoperable EHR might block Canadians from achieving a cherished goal in the provisioning of their healthcare: obtaining a completely unbiased second opinion from a healthcare provider unacquainted with their care and current records. Today, an unbiased second opinion is easily obtained: one need merely make an appointment with a primary care provider not previously seen and then not provide the name of one's current family physician. The effect of a fully interoperable EHR on this "right to an unbiased second opinion" is currently unknown. For example, if a patient/person is labelled in their EHR as a hypochondriac, can that person ever fully escape this diagnosis if their EHR follows them from physician to physician within and even across Canadian healthcare jurisdictions?

[97] End User Acceptance Strategy – British Columbia Consultation Session, Canada Health Infoway, October 14, 15, 2004

Individuals in jurisdictions that legally mandate that patients/persons have the legal right to comprehensively block or mask their data can use this ability to suppress access to their EHR prior to seeking a second opinion. In the majority of Canadian jurisdictions, no such legal mandate exists.

As an alternative, an individual might seek to have a second EHR created that was unconnected to the first. Although nothing in the requirements prevents a patient/person from intentionally having more than one EHR, neither do they explicitly guarantee such a capability. The issue is discussed further in *Electronic Health Record (EHR) Privacy and Security Functions and Services.*

APPENDIX B Canadian Data Protection Related Legislation – Catalogue And Comparison

Two tables follow. The first briefly describes legislation in Canada that is relevant to the privacy and security of the EHR.

The second table provides a high-level comparison of the four provincial health data protection statutes and the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*. All five of these statues are predicated in some way on the ten privacy principles of the Canadian Standards Association's *Model Code for the Protection of Personal Information,* which is included in Schedule 1 of *PIPEDA*. However, the statutes each interpret and apply the ten privacy principles differently. This chart is designed to serve as a high-level illustration of these differences.

These tables are for discussion purposes only and should not be construed as legal advice. Readers should consult legal counsel before drawing conclusions about their legal rights and responsibilities.

Table 3: Canadian Health Information Legislation that is Relevant to the Privacy and Security of an EHR

Province	FOIPP	Health Information	Other Privacy Legislation	Other Legislation
Yukon	*Access to Information and Protection of Privacy Act*, S.Y. 1995, c. 1 http://www.canlii.org/yk/sta/pdf/ch1.pdf	None	None	*Health Act*, S.Y. 1989-90, c.36, *s43(2)* http://www.canlii.org/yk/sta/pdf/ch106.pdf *Mental Health Act, s.42(7)* http://www.canlii.org/yk/sta/pdf/ch150.pdf
British Columbia	*Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm	None	*Personal Information Protection Act*, SBC 2003, c.63 http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm *Personal Information Protection Act Regulations*, B.C. Reg. 473/2003 http://www.qp.gov.bc.ca/statreg/reg/P/PersonalInformation/473_2003.htm *Privacy Act*, R.S.B.C. 1996, c. 373 * http://www.qp.gov.bc.ca/statreg/stat/P/96373_01.htm	*Pharmacists, Pharmacy Operations and Drug Scheduling Act,* R.S.B.C. 1996, c.363 *s.37(1), 38.1, 39* http://www.qp.gov.bc.ca/statreg/stat/P/96363_01.htm

Province	FOIPP	Health Information	Other Privacy Legislation	Other Legislation
Alberta	*Freedom of Information and Protection of Privacy Act,* R.S.A. 2000, c. F-25 http://www.qp.gov.ab.ca/documents/Acts/F25.cfm?frm_isbn=0779729218	*Health Information Act,* R.S.A. 2000, c. H-5 http://www.qp.gov.ab.ca/documents/Acts/H05.cfm?frm_isbn=0779719352 *Designation Regulation,* AR 69/01 http://www.qp.gov.ab.ca/documents/Regs/2001_069.cfm?frm_isbn=077329225X *Health Information Regulation*, AR 70/01 http://www.qp.gov.ab.ca/documents/Regs/2001_070.cfm?frm_isbn=0773292241	*Personal Information Protection Act,* S.A. 2003, c.P-6.5 http://www.qp.gov.ab.ca/documents/Acts/P06P5.cfm?frm_isbn=0779726316	*Mental Health Act,* R.S.A. 2000, *s.17(1.1), 17(9)* http://www.qp.gov.ab.ca/documents/Acts/M13.cfm?frm_isbn=0779727134
Saskatchewan	*Freedom of Information and Protection of Privacy Act,* S.S. 1990-91, c. F-22.01 http://www.qp.gov.sk.ca/index.cfm?fuseaction=publications.details&p=527 *Local Authority Freedom of Information and Protection of Privacy Act,* S.S. 1990-91, c. L-27.1 http://www.qp.gov.sk.ca/index.cfm?fuseaction=publications.details&p=605	*Health Information Protection Act,* S.S. 1999, c. H-0.021 http://www.qp.gov.sk.ca/index.cfm?fuseaction=publications.details&p=4523 Draft *Health Information Protection Act Regulations*, released for comment http://www.health.gov.sk.ca/mc_hipa_reg_draftforconsultation.pdf	*Privacy Act*, R.S.S. 1978, c. P-24 * http://www.qp.gov.sk.ca/index.cfm?fuseaction=publications.details&p=767	*Mental Health Services Act,* S.S. 1984-85-86, *s.38(4)* http://www.qp.gov.sk.ca/index.cfm?fuseaction=publications.details&p=626

Province	FOIPP	Health Information	Other Privacy Legislation	Other Legislation
Manitoba	*Freedom of Information and Protection of Privacy Act*, S.M. 1997, c. 50; C.C.S.M., c. F175 http://web2.gov.mb.ca/laws/statutes/ccsm/f175e.php	*Personal Health Information Act*, C.C.S.M., c. P33.5 http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php *Personal Health Information Regulation*, Man. Reg. 245/97 http://web2.gov.mb.ca/laws/regs/pdf/p033-5-245.97.pdf	*Privacy Act*, C.C.S.M., c. P125 * http://web2.gov.mb.ca/laws/statutes/ccsm/p125e.php	*Mental Health Act*, C.C.S.M., c. .M110, s.36 http://web2.gov.mb.ca/laws/statutes/ccsm/m110e.php
Ontario	*Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31 http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90f31_e.htm *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90m56_e.htm	*Personal Health Information Protection Act, 2004,* S.O. 2004, c.3, Schedule A (not in force until November 1,2004) http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm *General Regulation*, published in the Ontario Gazette for comment on July 3, 2004		*Mental Health Act*, R.S.O. 1990, c.M.7, ss.29(1.1), 35(2)(4) http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90m07_e.htm#BK26 *Nursing Homes Act,* R.S.O. 1990, c.N.7, s.20.2 http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90n07_e.htm *Health Care Consent Act,* *Smart Systems for Health Agency*, O.Reg. 43/02, s.15 http://www.e-laws.gov.on.ca/DBLaws/Regs/English/020043_e.htm *General Regulation, Medicine Act, 1991*, O.Reg. 114/94, s.20 http://www.e-laws.gov.on.ca/DBLaws/Regs/English/940114_e.htm#P273_29608

Province	FOIPP	Health Information	Other Privacy Legislation	Other Legislation
Quebec	*An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, R.S.Q., c. A-2.1 http://www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1_A.html	None	*Charter of Human Rights and Freedoms,* R.S.Q., c. C-12, ss. 4, 5, 9. http://www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_12/C12_A.html *An Act Respecting the Protection of Personal Information in the Private Sector,* R.S.Q., c. P-39.1 http://www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html Civil Code of Quebec, articles 35-41	*An Act Respecting Health Services and Social Services,*R.S.Q.,c.S-4.2, *ss.19, 24.* http://www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/S_4_2/S4_2_A.html *An Act to Establish a Legal Framework for Information Technology,* R.S.Q. C-1.1 http://www.canlii.org/qc/laws/sta/l.html
New Brunswick	*Protection of Personal Information Act*, S.N.B. 1998, c. P-19.1 http://www.gnb.ca/0062/acts/acts/p-19-1.htm *Right to Information Act*, S.N.B. 1978, c. R-10.3 http://www.gnb.ca/0062/acts/acts/r-10-3.htm	None	None	*General Regulation – Hospital Act,* Regulation 92-48, s.21(1)(a),(b),(c) http://www.gnb.ca/0062/regs/h-6-1reg.htm *Mental Health Act*, c.M-10, s.17(4),(5)(a),(b),(c) http://www.gnb.ca/0062/acts/acts/m-10.htm
Prince Edward Island	*Freedom of Information and Protection of Privacy Act*, S.P.E.I. 2001, c. F-15.01 http://www.gov.pe.ca/law/statutes/pdf/f-15_01.pdf	None	None	*Hospital Management Regulations – Hospitals Act*, P.E.I. Reg. EC 574/76, s.47(1),(5)(a),(b),(g) http://www.gov.pe.ca/law/regulations/pdf/H&10-2.pdf *Mental Health Act*, s.31(2)(d),(e) and 31(15) http://www.gov.pe.ca/law/statutes/pdf/m-06_1.pdf

Province	FOIPP	Health Information	Other Privacy Legislation	Other Legislation
Nova Scotia	*Freedom of Information and Protection of Privacy Act*, R.S.N.S. 1993, c. C- 5 http://www.gov.ns.ca/legislature/legc/ *Freedom of Information and Protection of Privacy Regulations*, N.S. Reg. 105/94, s. 9 http://www.gov.ns.ca/just/regulations/regs/foiregs.htm	None	None	*Hospitals Act*, R.S.N.S. 1989, c. 208, s.71(5)(a),(b) and 71(6)(b) http://www.gov.ns.ca/legislature/legc/ *Pharmacy Act*, S.N.S. 2001, c.36, s.27(4)(a),(b) http://www.gov.ns.ca/legislature/legc/
Newfoundland	*Freedom of Information Act*, R.S.N.L. 1990, c. F-25, s. 10; to be replaced by *Access to Information and Protection of Privacy Act*, S.N.L, 2002, c. A-1.1. (not in force) http://www.gov.nf.ca/hoa/sr/	None	*Privacy Act,* R.S.N.L. 1990, c. P-22 * http://www.gov.nf.ca/hoa/sr/	*Centre for Health Information Act,* S.N.L. 2004, c.C-5.1 (not in force) http://www.gov.nf.ca/hoa/sr/ *Hospitals Act,* R.S.N.L. 1990, c.H-9, *s.35(3)(d)* http://www.gov.nf.ca/hoa/sr/ *Pharmaceutical Association Regulations, 1998,* N.L.R. 80/98, s.37(2)(c) http://www.gov.nf.ca/hoa/sr/
Northwest Territories and Nunavut (all legislation in force in both Territories except as otherwise noted)	*Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c.20 http://www.justice.gov.nt.ca/PDF/ACTS/Access_to_Information.pdf *Access to Information and Protection of Privacy Act Regulations*, R-206-96, s. 8 http://www.justice.gov.nt.ca/PDF/REGS/ACCESS_TO_INFO_(ATIPP)/ATIPP.pdf	None	None	*Hospital Standards Regulations,* R.R.N.W.T. 1990, c.T-6. ss.73-74 http://www.justice.gov.nt.ca/PDF/REGS/HOS_INSUR_&_HEALTH_&_SS_ADMIN/Hospital_Stand.pdf Mental Health Act, s.48(3)(c),(d),(e) http://www.justice.gov.nt.ca/PDF/ACTS/Mental_Health.pdf

Province	FOIPP	Health Information	Other Privacy Legislation	Other Legislation
Federal	*Privacy Act*, R.S.C. 1985, c. P-21 http://laws.justice.gc.ca/en/P-21/index.html *Access to Information Act*, R.S.C. 1985, c. A-1 http://laws.justice.gc.ca/en/A-1/index.html	None	*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 http://laws.justice.gc.ca/en/P-8.6/index.html	

Table 4: PIPEDA and Health Data Protection Legislation Comparison Chart

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Scope of the privacy legislation	Applies to health information custodians that collect, use and disclose personal health information. Legislation also includes rules for non-custodians, such as their agents or health data institutes.	Applies to custodians that collect, use and disclose health information. Legislation also contains rules for non-custodians, such as information managers.	Applies to trustees that collect, use and disclose personal health information. Legislation also contains rules for non-custodians, such as information managers.	Applies to trustees that collect, use, and disclose personal health information. Legislation also contains rules for non-custodians, such as information management service provider.	Applies to personal information about customers or employees that is collected used or disclosed by the federally regulated sector in the course of commercial activities, or to personal information about customers at provincial organisations performing commercial activities, unless such organisations are already covered by privacy legislation that is "substantially similar"[98] to PIPEDA.[99]

[98] The Alberta *Personal Information Protection Act*, S.A. 2003, c. P-6.5,and British Columbia *Personal Information Protection Act,* S.B.C. 2003, c. 63, were declared substantially similar by the Minister of Industry on October 12, 2004.

[99] Excerpted from the Office of the Privacy Commissioner of Canada's Frequently Asked Questions, available at: www.privcom.gc.ca

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Personal Health Information must relate to identifiable individual for the statute to apply	No, the act has specific provisions regarding de-identifying personal health information for the purpose of analysis of the health system. [100] However, generally, the act only applies to identifiable personal health information.[101]	No, the act states that a custodian may collect, use or disclose non-identifying health information for any purpose. Also, when a custodian discloses non-identifying health information to a person that is not a custodian, the custodian must inform the person that the person must notify the Commissioner of an intention to use the information for data matching before performing the data matching.[102]	Yes, the act does not apply to de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified.[103]	Yes, this Act does not apply to anonymous or statistical health information that does not, either by itself or when combined with other information available to the custodian, permit individuals to be identified.[104]	Yes, the act applies to personal information about an identifiable individual.[105]

[100] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 47.
[101] *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, ss. 4(1), 4(2) and 7(1)(a).
[102] *Health Information Act*, R.S.A. 2000, c. H-5, ss. 19, 26 and 32.
[103] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 3(2)(a).
[104] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 3.
[105] Personal Information and Electronic Documents Act, S.C. 2000, c.5, s. 2.

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Separate rules for Mental Health Information and other "sensitive" information.	Yes, an officer in charge of psychiatric facility may collect, use and disclose personal health information without patient's consent for purposes of examining, assessing, observing or detaining patient in accordance with *Mental Health Act.*[106]	No, the act does not create special exceptions for mental health or other information. This information is provided with the same protection as other health information protected by the act.	Yes, provisions in the act governing consent for collection use, and disclosure and right of access, do not apply to information collected for the purpose of the *Mental Health Services Act.*[107]	Yes, the *Mental Health Act* prevails over *Personal Health Information Act.*[108] Also, the act requires that in determining the reasonableness of security safeguards, a trustee shall take into account the degree of sensitivity of the personal health information to be protected. [109]	No, however, the act does require that the type of consent obtained (e.g. opt-out, implied or express) and level of security employed by the organisation should be appropriate to the sensitivity of the information.[110]

[106] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 40(2).
[107] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 4(4).
[108] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 19
[109] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 4(3)
[110] Personal Information and Electronic Documents Act, S.C. 2000, c.5, Schedule 1, ss. 4.3.4 and 4.7.2.

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Commissioner / Ombudsman Powers	Commissioner has powers to investigate complaints from individuals or on own motion, compel disclosure of information, books, records or information practices relevant to an investigation, and make orders, comments, or recommendations. The Commissioner may also conduct research, receive complaints and comment on the act.[111]	Commissioner has powers to investigate potential breaches of the act, to hold full inquiry, and make orders.[112]	Commissioner has powers to review, compel disclosure of personal health information, summon testimony under oath, comment and make recommendations in response to a complaint.[113]	Ombudsman may conduct investigations and audits, make recommendations and commission research.[114]	Commissioner has powers to investigate complaints from individual or on own motion. Commissioner has broad audit powers, can issue report and make recommendations, but cannot make orders.[115]
Commissioner / Ombudsman has power to conduct audits	No, but may offer comments on custodian's actual or proposed information practices at the custodian's request.[116]	No, but may give advice and recommendations of general application to a custodian on rights or obligations under HIA.[117]	Yes, may carry out investigations with respect to personal health information in the custody or control of trustees to ensure compliance with act.[118]	Yes, the ombudsman may conduct investigations and audits and make recommendations to monitor and ensure compliance with the act.[119]	Yes, if Commissioner has reasonable grounds to believe organisation is in contravention of PIPEDA or not following Commissioner's recommendation.[120]

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Appeals of orders or court review of recommendations	A health information custodian subject to an order may appeal to the Divisional Court on a question of law.[121]	Commissioner's decision is final. Custodians subject to an order has a limited right of review in the event of a conflict of interest between Commissioner and custodian.[122]	Trustee may choose not to comply with recommendations of the Commissioner, in which case there is a right of appeal for the individual who filed the complaint.[123]	Trustee's refusal to grant access can be appealed by the individual who filed the complaint or the Ombudsman to the court. Such an appeal may only be filed once a complaint has been filed with the Ombudsman and the Ombudsman has provided a report.[124]	A complainant may, after receiving the Commissioner's report, apply to the court for a hearing. Commissioner may also apply for a hearing.[125]

[111] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 66.
[112] *Health Information Act*, R.S.A. 2000, c. H-5, ss. 77 and 80.
[113] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 46.
[114] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 28.
[115] Personal Information and Electronic Documents Act, S.C. 2000, c.5, ss. 12, 13 and 18.
[116] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 66(d).
[117] *Health Information Act*, R.S.A. 2000, c. H-5, s. 84(h)
[118] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 52(d).
[119] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 28(a).
[120] Personal Information and Electronic Documents Act, S.C. 2000, c.5, s. 18(a).
[121] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 64(4).
[122] *Health Information Act*, R.S.A. 2000, c. H-5, s. 81
[123] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, ss. 49 and 50.
[124] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, ss. 49 and 50.
[125] Personal Information and Electronic Documents Act, S.C. 2000, c.5, s. 14(1).

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Consent Model[126]	Where the act requires consent, the consent must be knowledgeable and not be obtained through deception or coercion. The consent may be express or implied.[127]	Where the act requires consent, the consent must be informed and must be provided in writing or electronically.[128]	Where the act requires consent, the consent must be informed and must not be obtained through deception or coercion. A consent may be given that is effective only for a limited period and may be express or implied. Lastly, the act deems consent[129] for some disclosures of personal health information (see below).[130].	Manitoba *Personal Health Information Act* does not outline what constitutes a valid consent.	Knowledgeable consent is required for the collection, use or disclosure of personal information, except where inappropriate. The type of consent (e.g. opt-out, express or implied) may vary, depending on the circumstances, and must take into account the sensitivity of the information.[131]

[126] A consent is considered knowledgeable under section 18(5) of Ontario *Personal Health Information Protection Act* if it is reasonable in the circumstances that the patient/person knows: (a) the purposes of the collection, use and disclosure, as the case may be, and (b) that the individual may give or withhold consent; "knowledgeable consent is also required under *PIPEDA*. "Knowledgeable consent" is a different standard from "informed consent." The latter typically requires that the patient/person: (a) receives information about the purposes of the collection use and disclosure, the expected benefits of the collection, use and disclosure, the material risks of the collection, use and disclosure, alternative to the collection, use and disclosure, and the likely consequences of not permitting the collection, use and disclosure that a reasonable person in the same circumstances would encounter in order to make a decision about the treatment; and (b) receives responses to his or her requests for additional information about those matters.

[127] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 18.

[128] *Health Information Act*, R.S.A. 2000, c. H-5, s. 34.

[129] With "deemed" consent it does not matter whether the patient/person has actually consented; the law permits organisations to act as if the patient/person has consented; there is no right to withdraw or withhold consent. In contrast, all of those rights are present with express and implied consent.

[130] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, ss.6 and 27(2)

[131] Personal Information and Electronic Documents Act, S.C. 2000, c.5, Schedule 1, s. 4.3.

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Direct collection without Consent for treatment and care purposes	Yes, a health information custodian may collect personal health information about an individual directly from the individual, even if the individual is incapable of consenting, if the collection is reasonably necessary for the provision of health care and it is not reasonably possible to obtain consent in a timely manner.[132]	Yes, a custodian may collect individually identifying health information if that information relates directly to and is necessary to enable the custodian to carry out the provision of health services.[133]	Yes, a trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.[134]	Yes, a trustee shall not collect personal health information about an individual *unless* the information is collected for a lawful purpose connected with a function or activity of the trustee, such as the provision of healthcare, and the collection of the information is necessary for that purpose. [135]	No, specific exceptions to consent for treatment and care purposes are not made under the act.

[132] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 36(2).
[133] *Health Information Act*, R.S.A. 2000, c. H-5, s. 20.
[134] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 24(1).
[135] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 13.

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Use without consent for treatment and care purposes	Yes, a health information custodian may use personal health information about an individual for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, but not if the individual expressly instructs otherwise.[136]	Yes, a custodian may use individually identifying health information in its custody or under its control for the purpose of the provision of health services;[137]	Yes, a trustee may use personal health information for a purpose that will primarily benefit the subject individual.[138]	Yes, a trustee may use personal health information only for the purpose for which it was collected or received.[139]	No, specific exceptions to consent for treatment and care purposes are not made under the act.

[136] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 37(1)(a).
[137] *Health Information Act*, R.S.A. 2000, .c H-5, s. 27(1)(a).
[138] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 26(2)(c).
[139] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 21.

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Disclosure without consent for treatment and care purposes	Yes, but only as permitted under the act or if it is not reasonably possible to obtain the individual's consent in a timely manner and the individual has not expressly instructed otherwise.[140]	Yes, but custodian must consider express wishes of patient in deciding how much to disclose.[141]	Yes, an individual is deemed to consent to a disclosure of personal health information for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose. However, an individual can opt-out of access to and disclosure of his or her comprehensive health record.[142]	Yes, unless individual instructs otherwise.[143]	No, specific exceptions to consent for treatment and care purposes are not made under the act.
Allow individuals to restrict use or disclosure of their personal health information for care and treatment purpose	Yes. An individual may restrict the uses and disclosures of his or her personal health information.[144]	No, but providers must consider express wishes of patients when deciding how much personal health information to disclose, but there is no requirement to abide by patients' wishes.[145]	Yes, only in the context of a comprehensive health record. The individual may require the comprehensive record not be disclosed.[146]	Yes, the act provides that a custodian may disclose without consent to a person providing healthcare to the individual unless the individual instructs otherwise.[147]	No, specific provisions allowing individuals to restrict use or disclosure of their personal health information are not made under the act.

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Requires consent for research	Yes, consent is required unless research ethics board determines it is impractical. [148]	Yes, consent is required unless research ethics board determines it is unreasonable, impractical or not feasible.[149]	Yes, consent is required unless research ethics board determines it is not reasonably practicable.[150]	Yes, consent is required unless research ethics board determines it is unreasonable or impractical.[151]	Disclosure permitted without consent for research, where the research can not be achieved without disclosing the information, it is impracticable to obtain consent and the organisation informs Commissioner before the information is disclosed.[152]

[140] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 38(1)(a).

[141] *Health Information Act*, R.S.A. 2000, c. H-5, ss. 35(1) and 58(2).

[142] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, ss. 8 and 27(2).

[143] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 22(2)(a).

[144] *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, ss. 37(1)(a), 38(1)(a), and 50(1)(e)

[145] *Health Information Act*, R.S.A. 2000, c. H-5, s. 58(2).

[146] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 8.

[147] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 22(2)(a).

[148] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 44.

[149] *Health Information Act*, R.S.A. 2000, c. H-5, s. 50(1).

[150] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 29.

[151] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 24.

[152] Personal Information and Electronic Documents Act, S.C. 2000, c.5, s. 7(3).

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Duty to take reasonable steps to ensure accuracy	Yes, health information custodians must take reasonable steps to ensure that personal health information is as accurate. complete, and up-to-date as is necessary for the purposes for which it is used or disclosed.[153]	Yes, custodians must make a reasonable effort to ensure information is accurate and complete before it is collected or used.[154]	Yes - in collecting personal health information, custodians must take reasonable steps to ensure that the information is accurate and complete.[155]	Yes, trustees must take reasonable steps to ensure that information is accurate, up to date, complete and not misleading.[156]	Yes, information shall be as accurate, complete and up-to-date as is necessary for which it is to be used.[157]
Procedure for correction of records	With written request, individuals can require correction where they demonstrate that information is incomplete or incorrect; custodian must give reasons for refusal; where custodian refuses, individual can complain to Commissioner.[158]	Individuals can request in writing that correction be made; custodian must give reasons for refusal; can ask for statement of disagreement or review by Commissioner.[159]	Individual may request an amendment orally or in writing. Where correction refused, custodian must make notation of refusal.[160]	Individuals can request in writing that correction be made; custodian must make correction or give reasons for refusal, and inform the individual of right to complain to the Ombudsman.[161]	Individuals have the right to challenge the accuracy and completeness of the information and have it amended appropriately. Individuals may complain to Commissioner if amendment is not made.[162]

[153] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 11.

[154] *Health Information Act*, R.S.A. 2000, c. H-5, s. 61.

[155] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 19.

[156] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 16.

[157] [157] Personal Information and Electronic Documents Act, S.C. 2000, c.5, Schedule 1, s. 4.6.

[158] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 55.

[159] *Health Information Act*, R.S.A. 2000, c, H-5, s. 13.

[160] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 40.

[161] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s. 12.

[162] Personal Information and Electronic Documents Act, S.C. 2000, c.5, Schedule 1, s. 4.6.

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Duty to collect, use or disclose in a limited manner	Yes, health information custodians may not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure.[163]	Yes, custodians must only collect, use or disclose the amount of health information that is essential to enable the custodian to carry out the intended purpose.[164]	Yes, personal health information may only be collected, used or disclosed on a need-to-know basis.[165]	Yes, trustees may only collect, use and disclose as much as is reasonable necessary to accomplish the purpose.[166]	No
Duty to collect, use or disclose with the highest degree of anonymity	Yes, health information custodians may not collect, use or disclose if other information will serve the purpose.[167]	Yes, custodians must collect, use or disclose with highest degree of anonymity possible.[168]	Yes, custodians must use or disclose only de-identified information if it will serve the purpose.[169]	No	No

[163] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 30(2).
[164] *Health Information Act*, R.S.A. 2000, c. H-5, s. 58(1).
[165] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 23(1)
[166] *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, ss. 13(2) and 20(2).
[167] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 30(1).
[168] *Health Information Act*, R.S.A. 2000, c. H-5, s. 57.
[169] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 24.

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Duty to protect information	Yes, health information custodians must take reasonable steps to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure, and against unauthorized copying, modification or disposal.[170]	Yes, custodians must take reasonable steps to protect against any reasonably anticipated threat or hazard to security or integrity or loss of the health information, or unauthorized use, disclosure, modification or access.[171]	Yes, custodians must establish policies and procedures to maintain administrative, technical, and physical safeguards.[172]	Yes, trustees must establish and comply with written policies and procedures to ensure the security of personal health information, including provisions for the recording of security breaches.[173]	Yes, personal information must be protected by security safeguards appropriate to the sensitivity of the information.[174]
Duty to notify individual if information is stolen, lost, or accessed by an unauthorized person	Yes, the act requires that a health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.**[175]**	No	No	No	No

[170] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 12.
[171] *Health Information Act*, R.S.A. 2000, c. H-5, s. 60.
[172] *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 16
[173] Personal Health Information Regulation, Man. Reg. 245/97, s. 2.
[174] Personal Information and Electronic Documents Act, S.C. 2000, c.5, Schedule 1, s. 4.7.
[175] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 12(2).

ISSUE	Ontario Personal Health Information Protection Act	Alberta Health Information Act	Saskatchewan Health Information Protection Act	Manitoba Personal Health Information Act	Federal Personal Information Protection and Electronic Documents Act
Duty to prepare Privacy Impact assessments or Threat and Risk Assessments	Yes, the act requires "health information network providers.[176] to perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to, threats, vulnerabilities and risks to the security and integrity of the personal health information, and how the services may affect the privacy of the individuals who are the subject of the information.[177]	Yes, a custodian must prepare a privacy impact assessment for proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information.[178] The act also requires the department of health and wellness to undertake privacy impact assessments in certain circumstance.[179]	No	No	No
Quality of care policies and procedures	Detailed rules in *Quality of Care Information Protection Act, 2004*	Detailed rules found in *Evidence Act*. Access to certain information not permitted in Health Information Act	Detailed rules found in *Evidence Act*. Access to certain information not permitted in Health Information Protection Act	Detailed rules found in *Evidence Act.*	No protection for quality assurance records.

[176] A health information network provider is defined in section 6(2) of the regulations to the Ontario *Personal Health Information Protection Act* as, "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians."

[177] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, O. Reg. 329/04, s. 5.

[178] *Health Information Act*, R.S.A. 2000, c. H-5, s. 64.

[179] *Health Information Act*, R.S.A. 2000, c. H-5, s. 46(5)(a)..

APPENDIX C Confidentiality, Integrity, Availability and Accountability

For the convenience of the interested reader, the table that follows show whether each security requirement in section 5 addresses confidentiality, data integrity, system integrity, system availability, or accountability.

Table 5: Summary of security requirements and what they address

	Confidentiality	Data Integrity	System Integrity	System Availability	Accountability
Requirement 1 Threat and Risk Assessment	√	√	√	√	√
Requirement 2 Security Policy	√	√	√	√	√
Requirement 3 Information Security Management, Co-ordination, and Allocation of Responsibilities	√	√	√	√	√
Requirement 4 Independent Review of Security Policy Implementation	√	√	√	√	√
Requirement 5 Assessing Threats and Risks from Third Parties	√	√	√	√	√
Requirement 6 Addressing Security in Third Party Agreements	√	√	√	√	√
Requirement 7 Transmitting PHI	√	√			√
Requirement 9 Responsibility for Information Assets	√	√	√	√	√
Requirement 10 Classifying PHI	√				√
Requirement 11 Labelling Personal Health Information As Confidential	√				√
Requirement 12 Addressing User Responsibilities In Job Definitions					√
Requirement 13 Addressing User Responsibilities In Terms of Employment					√
Requirement 14 Verifying the Identity of Users					√
Requirement 15 Confidentiality Agreements	√				√
Requirement 16 Training Users and Raising Security Awareness	√	√	√	√	√
Requirement 17 Terminating User Access When Terminating Employment	√	√	√	√	√
Requirement 18 Physically Securing EHRi Systems	√	√	√	√	
Requirement 19 Protecting EHRi Systems from Hazards				√	
Requirement 20 Protecting EHRi Systems from Disruptions				√	
Requirement 21 Protecting EHRi Equipment Off-Premises	√	√	√	√	√

	Confidentiality	Data Integrity	System Integrity	System Availability	Accountability
Requirement 22 Disposing of or Reusing EHRi Equipment	√				
Requirement 23 Removing EHRi Equipment, Data or Software	√		√	√	√
Requirement 24 Controlling Changes to the EHRi		√	√	√	√
Requirement 25 Segregating Duties	√	√	√	√	√
Requirement 26 Separating Development and Testing from Operations	√	√	√	√	
Requirement 27 Maintaining Capacity			√	√	
Requirement 28 Upgrading the EHRi	√	√	√	√	
Requirement 29 Protecting Against Malware	√	√	√	√	
Requirement 30 Securely Backing Up Data		√	√	√	
Requirement 31 Encrypting PHI During Transmission	√	√			
Requirement 32 Protecting Source and Destination Integrity During Transmission of PHI	√	√			
Requirement 33 Acknowledging Receipt of Transmitted PHI		√			√
Requirement 34 Protecting PHI on Portable Media	√	√			
Requirement 35 Disposing of Media Containing PHI	√				
Requirement 36 Protecting Data Storage	√	√			
Requirement 37 Protecting Storage of Unencrypted PHI in the EHRi	√	√			
Requirement 38 Logging Transactions in the EHRi		√			√
Requirement 39 Preserving the History of PHI in the EHRi		√			√
Requirement 40 Preserving the History of PHI in POS Systems		√			√
Requirement 41 Logging EHRi Transmissions of PHI		√			√
Requirement 42 Logging Access to PHI in POS Systems		√			√
Requirement 43 Minimum Content of Audit Logs		√			√
Requirement 44 Retaining Audit Logs		√			√
Requirement 45 Continuously Logging the EHRi					√
Requirement 46 Detecting Patterns of Misuse					√
Requirement 47 Reporting Every Access To A Patient/Person's EHR					√
Requirement 48 Reporting Every Access By A User					√

	Confidentiality	Data Integrity	System Integrity	System Availability	Accountability
Requirement 49 Analyzing EHRi Audit Logs for Patients/Persons At Elevated Risk	√	√			√
Requirement 50 Securing Access to EHRi Audit Logs					√
Requirement 51 Making EHRi Audit Logs Tamper-Proof		√			√
Requirement 52 Regularly Reviewing EHRi Audit Logs	√	√			√
Requirement 53 Policy for Access Control					√
Requirement 54 Registering Users					√
Requirement 55 Assigning Identifiers to Users		√	√		√
Requirement 56 Time Limited User Registration	√	√			√
Requirement 57 Reviewing User Registration Details					√
Requirement 58 Granting Access to Users by Role	√	√	√		√
Requirement 59 Selecting A Single Role Per Session					√
Requirement 60 Granting Access to Users in Work Groups	√	√			√
Requirement 62 Timely Revocation of Access	√	√	√		√
Requirement 63 Granting Access By Association	√	√			√
Requirement 63a Reporting the Access Privileges of a User	√	√	√	√	√
Requirement 64 Acceptable use agreements					√
Requirement 65 Authenticating EHRi Network Access			√	√	
Requirement 66 Controlling Access to EHRi Network Diagnostics and Network Management Services			√	√	
Requirement 67 Segregating EHRi Network Users, Services and Systems	√	√	√	√	
Requirement 68 Controlling Routing on EHRi Networks	√	√	√	√	
Requirement 69 Controlling Access to EHRi System Utilities	√	√	√	√	
Requirement 70 Restricting Connection Times to EHRi Applications			√	√	
Requirement 71 Robustly Authenticating Users	√	√	√	√	√
Requirement 72 Restricting Access to Unattended Workstations	√	√	√	√	√
Requirement 73 Acceptable Use of Mobile Devices	√	√	√		
Requirement 74 Acceptable Use of Teleworking	√	√	√		
Requirement 75 Protecting Wireless Networks	√	√	√		

	Confidentiality	Data Integrity	System Integrity	System Availability	Accountability
Requirement 76 Assigning Identifiers to Patients/Persons	√	√	√		
Requirement 77 Validating Input Data		√			
Requirement 78 Validating Printed Data		√			
Requirement 79 Providing Digital Signatures for Users		√			√
Requirement 80 Validating and Preserving Digital Signatures On PHI		√			√
Requirement 81 Implementing Software and Upgrades in the EHRi	√	√	√	√	
Requirement 82 Protecting EHRi Software	√	√	√	√	
Requirement 83 Managing Known Vulnerabilities	√	√	√	√	
Requirement 84 Reporting Security Incidents Involving the EHRi					√
Requirement 85 Responding to Security Incidents Involving the EHRi	√	√	√	√	√
Requirement 86 Managing Business Continuity				√	
Requirement 87 Testing Business Continuity Plans□				√	

References

Statutes and Regulations

- Alberta, *Health Information Act*, 2001.
- Canada, *Personal Information Protection and Electronic Document's Act* (PIPEDA), 2001
- Manitoba, Regulations to the *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5
- Ontario, *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3.
- Ontario, *Medicine Act*, 1991 - O. Reg. 114/94

Privacy

- Dr. Ann Cavoukian and Don Tapscott, *Who Knows: Safeguarding your Privacy in a Networked World* (Random House, Toronto, 1995)
- Canadian Standards Association (CSA), *Model Code for the Protection of Personal Information*, 1996.
- Canadian Standards Association, *Making the CSA Privacy Code Work for You. A Workbook on applying the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830) to your organisation* (Etobicoke, Ontario, December, 1996, ISBN 0-921347-57-X)
- Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980.
- Information and Privacy Commissioner of Ontario, *Privacy Assessment: The University Health Network's Response to Recent Breaches of Patient Privacy*, July 30, 2002.
- Stephanie Perrin, Heather H. Black, David H. Flaherty, and T. Murray Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Irwin Law, Toronto, 2001)

Security

- *ISO/IEC 17799 – Code of Practice for Information Security, 2004*
- *ISO 22857 - Health Informatics: Guidelines on data protection to facilitate trans-border flows of personal health information,* 2004

Infoway

- Canada Health Infoway, *EHRS Blueprint: An Interoperable EHR Framework*, July 2003
- Canada Health Infoway, *Electronic Health Record Privacy and Security Use Cases,* 2004
- Canada Health Infoway, *Electronic Health Record Privacy and Security Services,* 2005 (forthcoming)

Other

- Internet Engineer Task Force, *RFC 2119, Keywords for use in RFCs to Indicate Requirement Levels*, March, 1997