Canada Health Infoway Inforoute Santé du Canada

Privacy & Security Requirements and Considerations for Digital Health Solutions

Version 2.0

CANADA HEALTH INFOWAY – INFOROUTE SANTE DU CANADA
INFO@INFOWAY-INFOROUTE.CA

Disclaimer

This document represents solely the views of *Infoway*. It is based on *Infoway’s* research and analysis as well as information from various sources. Infoway’s views are based on information and analysis which *Infoway* believes is sound and reliable, as of the publication date of this document. *Infoway’s* views contained in this document may be amended or updated at any time by *Infoway*, without notice.

This document is informative only and cannot be interpreted as providing any indication of *Infoway’s* present or future strategies or investment criteria.

This document is provided as is. No representation or warranty of any kind whatsoever is made by *Infoway* as to the accuracy, infringement of third party intellectual property, completeness, fitness for any reader’s purpose, or correctness of any information or other contents contained in the white paper, and *Infoway* assumes no responsibility or liability if there is any inaccuracy, infringement of third party intellectual property, incompleteness, failure to meet any reader’s purpose or incorrectness with respect to any of the information or other contents contained in the white paper.

Infoway does not assume any responsibility or liability related directly or indirectly to the document, including without limitation with respect to any person who seeks to implement or implements or relies or complies with any part or all of the ideas, recommendations or suggestions set forth in the white paper.

This document does not constitute legal advice in one form or another. Organizations 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.

Infoway does not implicitly or explicitly endorse any particular technology or solution of any vendor or any other person, it does not guarantee the reliability or any proposed results related to the use of such technology or solution and this notwithstanding that reference may be made directly or indirectly to any such technology or solution in the document.

Infoway does not make any implicit or explicit commitment of any kind or nature whatsoever to make any investment in any particular technology or solution, and this notwithstanding that reference may be made directly or indirectly to any such technology or solution in the document.

Anyone using the enclosed material should rely on his/her/its own judgment as appropriate and seek the advice of competent professionals and experts.

Document History

February 2005	Electronic Health Record (EHR) Privacy and Security Requirements V1.1
June 2014	Privacy & Security Requirements and Considerations for Digital Health Solutions V2.0

Table of Contents

1 Executive Summary

The *Privacy and Security Requirements and Considerations for Digital Health Solutions* is an evolution of the original *Electronic Health Record (EHR) Privacy Security Requirements*. This document acknowledges the continued relevance of the previously defined privacy and security requirements for the EHR infostructure as well as additional elements for new digital health solutions and emerging technologies including:

- Consumer health solutions
- Point of service solutions
- Inter-jurisdictional health information sharing
- Secondary use of health information
- Cloud computing
- Mobile devices
- Remote patient monitoring
- Federated identity management

Digital health solutions enabled by emerging technologies have introduced new challenges for privacy and security professionals as well as those responsible for the planning and deployment of these new solutions.

The following is an illustrative scenario: a CIO in a Healthcare delivery Organisation (HDO) has been requested to deploy a new clinical solution on a mobile device platform where the mobile apps and device management are best served by a cloud-based solution. Agility and timelines are essential to meet business needs; therefore, the solution must be operational in several months. Concerned with managing privacy and security risks the CIO mandates his/her privacy and security staff to address appropriate issues and risks at the outset of the initiative.

As emerging technologies may not be well understood, what references do staff use to quickly define the relevant privacy and security requirements? Where do they obtain useful healthcare-specific guidance?

Infoway has created this document to assist in addressing these unique privacy and security challenges. It is a tool that can be used across the healthcare sector by providing a common set of privacy and security considerations allowing digital health solution providers the flexibility to define their solution-specific privacy and security requirements. This tool will reduce project efforts, costs and timelines, in addition to raising the level of protection of Personal Health Information (PHI).

The Canadian digital health ecosystem has evolved in the last 10 years. Alignment with health system transformation initiatives such as e-Referrals and e-Visits require the sharing of PHI across multiple organizations and digital health solutions. The privacy and security needs of collaborative and inter-disciplinary delivery of health care services across and between care settings, organizations, and disciplines are far more complex. More sources of PHI from remote patient monitoring devices and more point of service applications signify an increase in the volume of shared PHI and connection points. Privacy and security are therefore bigger challenges today than with the Electronic Health Record Solution (EHRS) of 2005.

In addition, privacy and security challenges have grown exponentially with the use of emerging technologies, such as cloud computing. While cloud computing has introduced many benefits, it also presents potential risks that must be managed. As an example, cloud computing provides for the virtualization of information storage and processing whereby PHI may be dynamically stored and processed in simultaneous locations across the globe without the knowledge or control of data custodians or patients.

Mobile devices and apps are now a source and consumer of PHI. The protection of PHI on a device that can easily be lost, stolen or compromised is a challenge. The use of trusted mobile apps will also become an increasingly important aspect for consumers, clinicians and HDO's.

As the digital health ecosystem evolves, so too do the risks, vulnerabilities and best practices. This document is intended to be an inventory of 'leading practices' for privacy and security in digital health initiatives. It leverages and references existing sources while providing additional guidance where gaps have been identified.

It will assist in addressing privacy and security in a way that facilitates collaborative and coordinated care across the continuum, clinical disciplines, service delivery programs, and care settings.

The methodology used includes an analysis of relevant best practices to identify gaps or areas for further refinement. A cross-organizational reference group of healthcare privacy and security experts was used to validate topics and content.

2 Introduction

2.1 Context

Since 2002, Canada Health Infoway (*Infoway*) has had the mandate to accelerate adoption of Electronic Health Record (EHR) solutions across the health sector in Canada. The EHR is a lifetime, longitudinal, electronic record of every citizen's health and their encounters and services received from the healthcare system.

As part of this mandate, *Infoway* invested in a large number of digital health projects that are building the technology platforms needed to ensure the secure, safe, and appropriate sharing of a Canadian's individual electronic health records whenever and wherever this information is needed.

To guide investments in EHR solutions *Infoway* developed a number of definitional products including the *Electronic Health Record Solution (EHRS) Blueprint*[1] and the associated *Electronic Health Record (EHR) Privacy and Security Requirements* and the *Electronic Health Record Infostructure (EHRi) Privacy Security Conceptual Architecture*[2]. Since these were produced, there have been many environmental changes affecting the digital health agenda in Canada:

- Implementation of EHR solutions and associated infostructure across the country have resulted in a better understanding of the requirements and the relative merits of different approaches and technology solutions;
- Emerging technologies and new digital health solutions have had a dramatic effect on how people gather and use information in their personal lives and in their occupations;
- *Infoway* has conducted an assessment of healthcare priorities across the country and identified a number of 'opportunities for action' to address these priorities. More information on these activities and outcomes can be found in *Infoway's* website.[3]

The addition of new privacy and security risks associated with the evolution of the digital health ecosystem has mandated additional privacy and security risk management tools.

This document is made up of two major parts distinguished by subject and approach:

1. Sections 3 and 4 define the privacy and security *requirements* for an Electronic Health Record Solution (EHRS). They were originally released in 2005 and were used to help guide the development

[1] https://www.infoway-inforoute.ca/index.php/resources/technical-documents/architecture

[2] https://www.infoway-inforoute.ca/index.php/resources/technical-documents/architecture/cat_view/2-resources/29-technical-documents/30-architecture?limit=5&limitstart=0&order=date&dir=ASC

[3] https://www.infoway-inforoute.ca/index.php/news-media/2013-news-releases/refreshed-strategic-plan-focuses-on-next-steps-in-canada-s-digital-health-journey

of the *Infoway* Privacy and Security Conceptual Architecture for the EHRS. Where appropriate they have been updated for this publication.

2. Section 5 identifies privacy and security *considerations* related to new digital health solutions and emerging technologies. The privacy and security elements presented in Section 5 are framed as considerations that should be taken into account by solution designers where and when applicable.

The reader should note that requirements defined in sections 3 and 4 of this document may also be applicable to the topics in section 5; therefore, both should be taken into account when establishing solution-specific privacy and security requirements.

2.2 Scope, Objectives and Audience

The convergence of emerging technologies enabling new digital health solutions such as cloud computing, mobile, remote patient monitoring, e-visits and e-booking will require organizations to take several topic areas into account when deploying new digital health solutions. By way of example, an 'e-booking' solution fully integrated into an EMR and the patient's consumer health solution may allow both the patient and clinician to view and confirm appointments via their mobile devices. Should the EMR be integrated into a cloud-offered 'e-booking' component and consumer health solution (CHS), the privacy and security considerations for cloud computing, mobile computing, Federated Identity Management (FIdM), Points of Service (PoS) and CHS topics should all be consulted.

This document may be of interest to:

Chief Information Privacy Officers
Chief Information Security Officers
Chief Information Officers
Business leaders/administrators/managers
E-Health portfolio managers
Privacy and Security architects/analysts
Vendors
Privacy oversight offices
Standards Development Organizations
Clinician representatives/organizations
Educational Organizations

2.3 Stakeholder Engagement

Sections 3 and 4 of the document were developed with input from a pan-Canadian panel of experts in EHR privacy and security, as well as a group of EHR privacy and security representatives from Canadian jurisdictions and healthcare provider associations.

The content and relevancy of topics in section 5 has been reviewed by the following stakeholders:

- A Project Reference Group, consisting of privacy/security subject matter experts from multiple provinces across Canada
- Representatives from the pan-Canadian Health Information Privacy Group
- Representatives from *Infoway's* Clinician Reference Panel

Infoway would like to thank the many contributors to this work. Each volunteered their valuable expertise and time; without their involvement this work would not have been possible. Please see Appendix C for a list of Reference Group participants.

3 Privacy Requirements[4]

The privacy requirements for an interoperable EHR are organized according to the 10 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 recognizable, principled approach to data protection in an EHR environment.

3.1 Accountability for Personal Health Information

Organizations 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 organization 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 organization designates an individual or individuals accountable for the organization's overall privacy compliance.

Privacy Requirement 1 – Accountable Person

Organizations connecting to the EHRi and organizations 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.

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[5]. Many healthcare organizations 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 organization, the Chief Privacy Officer is usually the focal point for data protection issues, both internally and externally.

See also Privacy Requirement 27 – Complaint Procedures.

[4] Aside from minor typographical corrections, this section is identical to the material provided in version 1.1 of the EHR Privacy and Security Requirements document. The only exception to this statement is for those areas where references to practices or legislation are no longer applicable. In those cases, the information has been updated to be current and has been identified as such with an Updated icon.

[5] 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 organization's compliance with these privacy laws.

Privacy Requirement 2 – Third-Party Agreements

Organizations connecting to the EHRi and organizations hosting components of the EHRi must use contractual means[6] 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 is 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 of the third party upon termination of the agreement.

Admin Requirement

Rationale: Organizations 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 organizations 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 organization must use contractual or other means to provide a comparable level of protection while any third party is processing the information[7]

See also **Security Requirement 6 – Addressing Security in Third-Party Agreements**.

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

[7] 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), pg. 16. The consultants acknowledge their indebtedness to the authors of this informed commentary on Schedule 1 of PIPEDA (pg. 13-46).

Privacy Requirement 3 – Privacy Policy

Organizations connecting to the EHRi and organizations hosting components of the EHRi must implement privacy and security policies and practices, including:

a) Implementing procedures to protect PHI (see **Security Requirement 2 – Security Policy**);

b) Establishing procedures to receive and respond to privacy-related complaints and inquiries (see **Privacy Requirement 28 – Complaint Procedures**);

c) Training users and communicating to users information about the organization's privacy policies and practices (see **Privacy Requirement 23 –Training Users and Raising Privacy Awareness** and **Security Requirement 14 – Confidentiality Agreements**); and

d) Developing communications materials to explain to the general public the organization's privacy policies and practices (see **Privacy Requirement 24 – Openness**).

Admin Requirement

Rationale: It is necessary for the mutual benefit of all EHRi users, including Point-of-Service (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

Organizations 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.

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[8].

See also **Security Requirement 5 – Assessing Threats and Risks from Third Parties.**

3.2 Identifying Purposes for Collection, Use and Disclosure of 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. This emphasis on openness 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[9], as well as identify any new purposes prior to using information for these new purposes. To satisfy this legal requirement, healthcare organizations must identify the purposes for which they collect, use and disclose a patient/person's PHI.

Privacy Requirement 5 – Identifying Purposes for Collection, Use and Disclosure

Organizations connected to the EHRi and organizations 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[10]; and

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

Admin Requirement

Rationale: This requirement ties together the concepts of obtaining 'knowledgeable' consent and stating purposes for information use (see **Section 4.8 – Communications and Operations Management** below). The goal is to make a reasonable effort to ensure that patients/persons understand the purposes for which organizations connected to the EHRi and organizations hosting components of the

[8] Alberta Health Information Act, section 64.

[9] 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.

[10] 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 collected. In these situations, the purposes for which PHI is collected, used and disclosed must be identified at the first reasonable opportunity.

EHRi collect, use and disclose their PHI[11].

Depending upon the way in which PHI is collected, organizations 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.

Privacy Requirement 6 – Limitation of Collection to Identified Purposes

Organizations connecting to the EHRi or organizations hosting components of the EHRi should only collect PHI necessary to fulfill the purposes they have identified (see **Privacy Requirement 5 – Identifying Purposes for Collection, Use and Disclosure**).

Policy & Procedures

Admin Requirement

Tech 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 care. 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, suspected child abuse or law enforcement.

3.3 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, 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, such as a patient/person presenting himself to a pharmacist, laboratory, emergency department, or physician in private practice[12]. With 'deemed' consent, it does not matter whether the patient/person has actually consented. The law permits organizations 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 organization should be able to demonstrate that it complied with applicable legislative requirements and that the patient/person had a reasonable opportunity

[11] The 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 practical in the circumstances. This would apply as well in an EHRi regime.

[12] 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 organization (Etobicoke, Ontario, December, 1996, ISBN 0-921347-57-X), pg. 11. Ontario, Personal Health Information Protection Act, section 18(2) does not define express or implied consent.

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[13,14].

It is assumed that based on jurisdictional requirements for consent 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 organizations – the so-called "lock box" concept[15]. 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 in Newfoundland and Labrador and New Brunswick. The EHRi must reflect legal obligations in its privacy requirements in all of their relative sophistication in this area. The ultimate obligation is to 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[16].

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

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

[15] 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."

[16] 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.

Privacy Requirement 7 – Obtaining Knowledgeable[17] Consent

Except where inappropriate (e.g., specifically exempted by law or professional code of practice), organizations connecting to the EHRi, and organizations hosting components of the EHRi should obtain the knowledge[18] 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[19].

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 organizations 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 of PHI[20]. 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

[17] 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.

[18] 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.

[19] 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.

[20] The Canadian Nurses Association's "Code of Ethics for Registered Nurses" (pg.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."

restrictions[21]. 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[22].

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

Privacy Requirement 8 – Recording Consent in PoS Systems

Where required by law, PoS systems connected to the EHRi must be able to record a patient/person's consent directives, including the withholding,[23] withdrawal or revocation of consent.[24]

Admin Requirement Tech Requirement

Rationale: Healthcare organizations 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 – Identifying Purposes for Collection, Use and Disclosure**).

The form of the consent sought by organizations 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 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.,

[21] 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.

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

[23] 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.

[24] 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.

auditing or law enforcement).

See also **Privacy Requirement 9 – Associating Consent Directives with PHI in PoS Systems** for the technical implications of handling consent and **Privacy Requirement 10 – Recording Consent in the EHR** for an analogous requirement for recording consent in the EHRi.

Privacy Requirement 9 – Associating Consent Directives 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.

Admin Requirement **Tech Requirement**

Rationale: Not all jurisdictions will require PoS systems 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.

Privacy Requirement 10 – Recording Consent in the EHR

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

Admin Requirement **Tech Requirement**

Rationale: Healthcare organizations must be able to determine if a patient/person has provided or withheld consent as required in their particular jurisdiction. Consequently, those organizations 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 organization). As a practical matter, a healthcare organization 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 organization 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 11 – Associating Consent Directives with PHI in the EHRi**). Before permitting accesses to PHI, the EHRi must ensure that all necessary legal requirements are upheld before transmitting data to a requestor.

See also **Privacy Requirement 11 – Associating Consent Directives with PHI in the EHRi** for the technical implications of handling consent.

Privacy Requirement 11 – Associating Consent Directives with PHI in the EHRi

When consent for receiving, storing, processing or transmitting PHI is required by law, 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 organizations 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 8 – Recording Consent in PoS Systems**.

Privacy Requirement 12 – Logging the Application of Consent Directives

The EHRi **must** be able to:

a) Log when the processing of consent directives (cf. **Privacy Requirement 11, 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

Tech Requirement

the organization where the accessing user works as well as in the organization where the information was collected that such a consent override has occurred.

Rationale: Since some health data protection laws, such as Ontario's Personal Health Information Protection Act, allow 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 37 – Logging Transactions in the EHRi** and **Security Requirement 42 – Minimum Content of Audit Logs**).

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.[25] The individual(s) responsible for facilitating an organization'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 organization where the PHI has been collected and the organization from which the information is being accessed.[26]

As logs will themselves contain confidential information, they must be made both secure and tamper-proof. Their security requirements are discussed in **Security Requirement 49 – Securing Access to EHRi Audit Logs** and **Security Requirement 50 – 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 19 – Notifying Patients/Persons of Inappropriate Access, Use or Disclosure**).

See also **Privacy Requirement 10 – Recording Consent in the EHR** and **Privacy Requirement 11 – Associating Consent Directives with PHI in the EHRi**.

Privacy Requirement 13 – Implications of Consent Directives

Organizations 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.

Admin Requirement

[25]

[26] 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.[27] These implications should be explained by qualified healthcare professionals to patients/persons in order to ensure that their full knowledge and consent is obtained.

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 7 – Obtaining Knowledgeable Consent**.

Privacy Requirement 14 – 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 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

[27] 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 not to 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 territorial laws govern these activities.[28]

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 (i.e. spouse or guardian) can be found, then the custodian must attempt to locate the next potential substitute decision-maker in the ranking process (i.e. sibling). When a suitable substitute decision-maker has been found, the custodian must document the relationship of that substitute decision-maker to the patient/person to ensure that the custodian's selection can later be audited, justified or reappraised.

See also **Privacy Requirement 7 – Obtaining Knowledgeable Consent**.

Privacy Requirement 15 – No Coerced Consent

Organizations connecting to the EHRi and organizations 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.

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 a result, 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.[29]

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

[29] 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

3.4 Limiting Collection of Personal Health Information

As outlined in **Privacy Requirement 5 – Identifying Purposes for Collection, Use and Disclosure**, organizations connecting to the EHRi and organizations 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 16 – Collecting Information by Fair and Lawful Means

Organizations connecting to the EHRi or 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.

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.

3.5 Limiting Use, Disclosure and Retention of Personal Health Information

When organizations identify the purposes for which they collect PHI (**Privacy Requirement 5 – Identifying Purpodses for Collection, Use and Disclosure**) and seek the appropriate consent for these purposes (**Privacy Requirement 8 – Recording Consent in PoS Systems**), it is imperative that they only use, disclose and retain information for these purposes. In many cases in healthcare, the content of records of PHI, as well as record retention periods, are mandated by statute, regulations and various bylaws for healthcare professionals.[30]

In addition, the distinction between use and disclosure is also highly relevant.[31] "Use" refers to any processing and treatment of data within the organization, whereas "disclosure" refers to the release of the information to third parties (outside of the originating organization, even in an EHR environment).[32]

[30] 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).

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

[32] 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 17 – Limiting Use and Disclosure of Personal Health Information to Identified Purposes

Organizations connecting to the EHRi or 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.[33]

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 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.[34] Such legislative provisions vary by jurisdiction.

In **Section 4.9 – Access Control**, a variety of security requirements are stated that provide robust access control to the EHRi and the PHI it contains. These requirements will greatly assist in operationalizing the limiting of use and disclosure of this PHI to authorized users with appropriate roles and privileges.

[33] 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 purposes for which the PHI will be used or disclosed are not consistent with those purposes identified will need to be established.

[34] See, for example, Ontario, Personal Health Information Protection Act, sections 31-33, 37-50 dealing with at least 15 types of uses and disclosures.

Privacy Requirement 18 – 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[35], together with the time and identity of the accessing user; and

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

Tech Requirement

Rationale: Specific legislation requires organizations to record access, modifications and disclosures of PHI.[36] Where such accesses, modifications 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 37** through **Security Requirement 51**. Also see **Privacy Requirement 12 – Logging the Application of Consent Directives** for the logging of consent directives. 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 organization where the PHI has been collected and the organization from which the information is being accessed.[37]

As logs will themselves contain confidential information, they must be made both secure and tamper-proof. Their security requirements are discussed in **Security Requirement 49 – Securing Access to EHRi Audit Logs** and **Security Requirement 50 – Making EHRi Audit**

[35] 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 information unless the information relates directly to the provision of healthcare to an identifiable patient/person.

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

[37] 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 their own privacy compliance.

Logs Tamper-Proof.

In addition to logging overrides of a patient/person's consent directives (item (b) in **Privacy Requirement 12 – Logging the Application of Consent Directives**) and alerting accountable individuals that a consent override has occurred (item (c) in **Privacy Requirement 12 – Logging the Application of Consent Directives**), there is also a related requirement to notify patients/persons when access has been deemed inappropriate (see **Privacy Requirement 19 – Notifying Patients/Persons of Inappropriate Access, Use or Disclosure**).

See also **Privacy Requirement 9 – Associating Consent Directives with PHI in PoS Systems** and **Privacy Requirement 10 – Recording Consent in the EHR**.

Privacy Requirement 19 – Notifying Patients/Persons of Inappropriate Access, Use or Disclosure

Updated

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

Admin Requirement

Rationale: Data protection laws in Ontario, New Brunswick and Newfoundland and Labrador make provision for notification.[38]

Privacy Requirement 20 – Retaining Records

The EHRi, PoS systems connected to the EHRi, organizations connecting to the EHRi, and organizations 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.

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

[38] Ontario, *Personal Health Information Protection Act*, section 12(2); New Brunswick, *Personal Health Information Privacy and Access Act*, section 49(1)(c); and Newfoundland and Labrador, *Personal Health Information Act,* section 15(3)

to hold certain core information about them on a more permanent basis.

See also **Security Requirement 21 – Disposing of or Reusing EHRi Equipment** and **Security Requirement 34 – Disposing of Media Containing PHI**.

3.6 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 organizations a commitment to accuracy in order to ensure efficient and effective delivery of healthcare. The goal for healthcare organizations 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 21 – Accuracy

The EHRi, PoS systems connected to the EHRi, organizations connecting to the EHRi and organizations 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 76 – Validating Input Data**.

3.7 Safeguards for the Protection of Personal Health Information

The EHRi, organizations connecting to the EHRi and organizations 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 4 – Security Requirements** 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 organization may then be subject to complaints to an oversight body, adverse publicity, fines and/or prosecution.[39]

Privacy Requirement 22 – Denoting Patients/Persons at Elevated Risk

The EHRi must provide functions for marking records of selected patients/persons[40] and subsequently making accesses to such data subject to mandatory auditing by the individual accountable for privacy compliance in the organization.

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, 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 is somehow more confidential than that 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 48 – Analyzing EHRi Audit Logs for Patients/Persons at Elevated Risk** for audit logging requirements related to this privacy requirement.

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

[40] 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 with malicious intent.

Privacy Requirement 23 – Training Users and Raising Privacy Awareness

All organizations connecting to the EHRi or hosting components of the EHRi **must** ensure that privacy education and training and regular updates in organizational 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.

Admin Requirement

Rationale: Organizations connecting to the EHRi or 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 organizations such as hospitals may find it relatively easy to design such training, it is more difficult when it comes to small operations such as individual pharmacies, nursing stations in remote communities, and the offices of private physicians, where the physician is often the only healthcare professional on staff. Organizations 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 4.6.2.1 – Information Security Awareness, Education and Training**

3.8 Openness about Practices Concerning the Management of Personal Health Information

This section is closely related to the 'accountability' privacy requirements discussed in **Section 3.1 – Accountability for Personal Health Information** 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 organizations have privacy management plans in place.

Privacy Requirement 24 – Openness

Organizations connecting to the EHRi or hosting components of the EHRi must make specific information about their policies and practices relating to the management of PHI readily available to the public.

At a minimum, these organizations **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

Admin Requirement

for the organization's policies and practices and to whom complaints or inquiries can be forwarded (see **Privacy Requirement 1 – Accountable Person**);

b) The means by which patients/persons can gain access to PHI held by the organization to which they have given authorization to access their PHI (see **Privacy Requirement 25 – Patient/Person Access**);

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

d) General description of the administrative, technical and physical safeguards and practices the organization maintains with respect to PHI; and

e) What PHI is made available to related organizations.

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 organizations connecting to the EHRi or at 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 organizations 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 organizations are reminded by this checklist of the various ways they can reduce anxieties about privacy and security.

3.9 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.[41]

In certain situations, the EHRi, organizations connecting to the EHRi or organizations hosting components of the EHRi may not be able to provide access to all the PHI they hold about a patient/person. Exceptions to the access requirements should be limited and specific.[42] The reason for denying access should be provided

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

[42] 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.

to the patient/person. Exceptions may include information that is prohibitively costly to provide,[43] information that contains references to other individuals (third parties),[44] information that cannot be disclosed for legal, security, or commercial proprietary reasons,[45] information that is subject to solicitor-client litigation privilege[46] and cases where healthcare organizations 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 organizations,[47] 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 25 – Patient/Person Access

Organizations connecting to the EHRi or hosting components of the EHRi **must**, upon request:

a) Inform a patient/person of the existence, use and disclosure[48] of his or her PHI and give the patient/person direct access to that PHI where such access is not prohibited by legislation;[49]

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;

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

d) Make readily available to the public specific information about their policies and practices relating to the management of PHI.

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

[43] 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, pg. 40).

[44] PIPEDA, section 9(1).

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

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

[47] 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…."

[48] The record of uses and disclosures of a patient/person's PHI is made up of information logged in compliance with **Security Requirement 37 – Logging Transactions in the EHRi**.

[49] 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.

rights. This is especially important 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 below, the patient/person also has a right to challenge factual errors in particular (see **Privacy Requirement 26 – Amending Inaccurate or Incomplete Information**).

This right of access includes as well the right of the patient/person to be told what information the organization 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 26 – Amending Inaccurate or Incomplete Information

Organizations connecting to the EHRi or 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 organization 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.

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.[50] 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 appropriately.[51] Fortunately, a developed electronic health record system will automatically distribute the most up-to-date information when it is required for authorized purposes.

3.10 Challenging Compliance

The right of any patient/person to lodge a privacy complaint has been a core fair information practice for more than 30 years.

Privacy Requirement 27 – Challenging Compliance

Organizations connecting to the EHRi or 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 – Accountable Person**.

Admin Requirement

Rationale: To give effect to privacy requirements like **Privacy Requirement 3 – Privacy Policy** and **Privacy Requirement 6 – Limitation of Collection to Identified Purposes**, patients must be able to challenge an organization's compliance with those requirements.

[50] 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).

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

Privacy Requirement 28 – Complaint Procedures

Organizations connecting to the EHRi or 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; and

c) Treat all received complaints as confidential.

Admin Requirement

Rationale: Healthcare organizations 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 place.

Even if healthcare organizations 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).[52]

Privacy Requirement 29 – Investigation

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

Admin Requirement

See also **Section 4.8.10.1 – Audit Logging** for a discussion of the requirements pertaining to audit logging and **Section 4.11.1 – 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 organization to do in specific circumstances. If a complainant wants to change the law, other avenues exist.

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

4 Security Requirements

4.0 Introduction Updated

ISO/IEC 27002:2005 Code of Practice for Information Security Management is a widely adopted international standard for information security management. In December, 2000, ISO/IEC 17799 was adopted by the International Standards Organization (ISO) from an existing British standard (BS 7799) published by the British Standards Institute. It was subsequently revised in 2005 and then renumbered in 2007 to align with other ISO/IEC 27000-series standards. The ISO/IEC 27002 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 organized into 11 sections, each covering a key control area for information security. Together these sections provide the working objectives of the Code of Practice.

In this section on security requirements, the current document follows the format of the revised standard ISO/IEC 27002:2005. All 11 security control objectives are covered in the sections that follow, including:

1. Risk Management
2. Security Policy;
3. Organizing Information Security;
4. Asset Management;
5. Human Resources Security;
6. Physical and Environmental Security;
7. Communications and Operational Management;
8. Access Control;
9. Information Systems Acquisition, Development and Maintenance;
10. Security Incident Management;
11. Business Continuity Management; and
12. Compliance.

At a minimum, five activities need to be carried out by an organization hosting components of the EHRi in order to satisfy the requirements of ISO/IEC 27002:

1. An appropriate management structure within the organization (e.g., a committee, a management forum or a management hierarchy) must assume responsibility for setting and enforcing organizational security policy and for managing privacy, security and business continuity risks (see see **Section 4.4 – Organizing Information Security**);

2. A security policy must be created, promulgated and enforced by administrative and technical means (see **Section 4.3 – Security Policy**);

3. Privacy, security and business continuity risks must be analyzed by means of a Threat and Risk Assessment (see **Section 4.2 –Risk Management**) and those risks must be managed against the objectives set by the security policy;

4. Compliance with the security policy must be assessed on an ongoing basis (see **Section 4.13 – Compliance**); and

5. Privacy, security and business continuity risks must be re-analysed when significant changes are made to the components of the EHRi that the organization is hosting (see **Section 4.2 –Risk Management**).

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

4.1 Risk Management

Risk assessment is an essential feature of ISO/IEC 27002. The interested reader can find examples of risk-assessment methodologies in ISO/IEC 27005:2011 (Security Techniques: Information security risk management).

An organization needs to implement a risk-management process within the organization. This process needs to have the support and commitment of the highest levels of management within the organization, otherwise it will be difficult to implement and enforce. Responsibilities for information risk management throughout the organization will need to be assigned. Key organizational 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

Policy & Procedures

Admin Requirement

Organizations hosting components of the EHRi must – and origanizations 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, 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 and 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; and

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 organization.

Rationale: A Threat and Risk Assessment (TRA) is needed to 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 and changes in the risk situation, and when significant changes occur.

4.2 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 27002 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

Organizations 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 organizations that are health information custodians, trustees and/or suppliers of health infostructure services. It also follows directly from **Privacy Requirement 3 – Privacy Policy**.

4.3 Organizing Information Security

The objectives of organizing information security are to:

- Manage information security within an enterprise;
- Maintain the security of organizational information processing facilities and information assets accessed by third parties; and
- Maintain the security of information when the responsibility for information processing has been outsourced to another organization.

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

4.3.1 Internal Organization

4.3.1.1 Management Commitment to Information Security, Co-ordination and Allocation of Responsibilities

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

Organizations connecting to the EHRi or 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 organization who have relevant roles and job functions.

Admin Requirement

Privacy Requirement 1 – Accountable Person effectively addresses the need to assign responsibility for privacy within organizations that are health information custodians and/or suppliers of health interoperability infostructure. It also addresses the need to assign responsibility for security within organizations whose employees are accessing PHI. The requirement above does the same for security[53].

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

Rationale: In addition to complementing **Privacy Requirement 1 – Accountable Person**, this security requirement is necessary to meet the legal requirements of several jurisdictions for accountability (see the discussion above in **Section 3.1 – Accountability for Personal Health Information**).

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

- Performing security assessments and evaluating the organization's information security risks (see **Security Requirement 1 – Threat and Risk Assessment**);
- Developing appropriate security policies (see **Security Requirement 2 – Security Policy**); 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 15 – Training Users and Raising Security Awareness**);
- 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 organization's privacy and security policies;
- Reviewing audit logs (see Security Requirement 51);
- Maintaining effective business continuity and disaster recovery plans (see **Security Requirement 85 – Managing Business Continuity**); and
- Serving as an information security expert for the executive staff of the organization.

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

4.3.1.2 Independent Review of Information Security

Security Requirement 4 – Independent Review of Security Policy Implementation

Organizations 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 organization's Chief

Admin Requirement

Executive Officer or Board of Directors.

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 the jurisdiction in which the information is found. This requirement also follows from the accountability requirements in **Section 3.1 – Accountability for Personal Health Information**.

Third-party review can and should occur at many levels, including: policy reviews, organizational 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.

4.3.2 External Parties

4.3.2.3 Identification of Risks Related to External Parties

Security Requirement 5 – Assessing Threats and Risks from Third Parties

Organizations 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 managed by external parties and must implement appropriate security controls where necessary to mitigate identified risks.

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 – Third-Party Agreements**.

See also **Section 3.1 – Accountability for Personal Health Information** for a discussion of the legal requirements concerning third-party service delivery management (e.g., PIPEDA and Ontario's Personal Health Information Protection Act).

4.3.2.4 Addressing Security in Third-Party Agreements

Security Requirement 6 – Addressing Security in Third-Party Agreements

Organizations 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.

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

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

Admin Requirement

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

There are several technical requirements related to the transmission of PHI, including:

Security Requirement 30 – Encrypting PHI During Transmission

Security Requirement 31 – Protecting Source and Destination Integrity During Transmission of PHI

Security Requirement 32 – Acknowledging Receipt of Transmitted PHI

Security Requirement 33 – Protecting PHI on Portable Media

Security Requirement 40 – Logging EHRi Transmissions of PHI

Security Requirement 69 – Restricting Connection Times to EHRi Applications

Security Requirement 70 – Robustly Authenticating Users

Security Requirement 74 – Protecting Wireless Networks

See also:

Privacy Requirement 1 – Accountable Person

Privacy Requirement 2 –Third-Party Agreements

Privacy Requirement 11 – Associating Consent Directives with PHI in the EHRi

Privacy Requirement 17 – Limiting Use and Disclosure of Personal Health Information to Identified Purposes

4.4 Asset Management

The objectives of information asset management are to achieve and maintain appropriate protection of organizational 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.).

4.4.1 Responsibility for Assets

Security Requirement 8 – Responsibility for Information Assets

Organizations 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.

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 – Accountable Person**. Acceptable-use follows directly from **Privacy Requirement 3 – Privacy Policy**.

See also **Privacy Requirement 5 – Identifying Purposes for Collection, Use and Disclosure**, **Privacy Requirement 6 – Limitation of Collection to Identified Purposes**, **Privacy Requirement 10 – Recording Consent in the EHR** and **Privacy Requirement 14 – Recording Identity of Substitute Decision-Makers**.

4.4.2 Information Classification

4.4.2.1 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 related to 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 change 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 even more confidential today than it would have been 20 years ago.

Because one cannot predict the sensitivity of a given element of PHI through all uses and phases of its lifecycle, 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 organizations and their staff. The identification and labelling of information assets is also an essential component of ISO/IEC 17799[54]. 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

[54] See References at the end of this document

counter to the three characteristics discussed above, but also run counter to jurisdictional legislation that defines PHI in broad terms.

Security Requirement 9 – Classifying PHI

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

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 graduated shades of confidentiality (e.g., lab data more confidential than medication profile, or patient address data less confidential than billing data) and concomitant graduated 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 48 – Analyzing EHRi Audit Logs for Patients/Persons At Elevated Risk.**

4.4.2.2 Classification of PHI

Security Requirement 10 – Labelling Personal Health Information as Confidential

All PoS systems connected to the EHRi **must** be capable of informing each PoS system user of 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

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

Admin 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 that may contain a mixture of confidential and non-confidential information.

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).

4.5 Human Resources Security

The objectives of human resources security are to:

- Reduce risks of human error, theft, fraud or misuse of facilities;
- 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;
- Minimize the damage from security incidents and malfunctions; and
- Learn from such incidents.

4.5.1 Information Classification

4.5.1.1 Roles and Responsibilities

Security Requirement 11 – Addressing User Responsibilities in Job Descriptions

All organizations 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 organization's information security policy.

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

Admin Requirement

Rationale: This ISO/IEC 27002 requirement is intended to reinforce the formalization 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 42 – Minimum Content of Audit Logs**, **Security Requirement 57 – Granting Access to Users by Role** and **Security Requirement 58 – Selecting a Single Role Per Session**.

4.5.1.2 Terms and Conditions of Employment

Security Requirement 12 – Addressing User Responsibilities in Terms of Employment

All organizations 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.

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 – Third-Party Agreements** and **Privacy Requirement 3 – Privacy Policy** 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 54 – Assigning Idrntifiers to Users**, **Security Requirement 63 – Acceptable-Use Agreements**, and **Security Requirement 70 – Robustly Authenticating Users**); and
- Following appropriate procedures when using mobile devices or when working off-site or at home (see **Security Requirement**

20 – Protecting EHRi Equipment Off-Premises and During Maintenance, Security Requirement 33 – Protecting PHI on Portable Media, Security Requirement 72 – Acceptable Use of Mobile Devices, and Security Requirement 73 – Acceptable Use of Teleworking).

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

Terms of Employment involving maintaining confidentiality should survive employment termination (see provisions for confidentiality agreements in **Security Requirement 14 – Confidentiality Agreements**). Termination of employment is discussed further in section **Security Requirement 16 – Terminating User Access when Terminating Employment**.

4.5.1.3 Screening

Security Requirement 13 – Verifying the Identity of Users

All organizations connecting to the EHRi or hosting components of 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 system connected to the EHRi or who will have access to hosted components of the EHRi.

Admin Requirement

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

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 (e.g. driver's license) 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 (e.g. banking, finance), verification checks are often not a part of healthcare hiring (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 53 – Registering Users**, **Security Requirement 54 – Assigning Identifiers to Users**, and **Security Requirement 56 – Reviewing User Registration Details** for a discussion of EHRi user registration. User authentication is dealt with in **Security Requirement 70 – Robustly Authenticating Users**.

4.5.1.4 Confidentiality Agreements

Security Requirement 14 – Confidentiality Agreements

All organizations connecting to the EHRi or hosting components of 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 system 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.

Admin Requirement

Rationale: The signing of confidentiality agreements is widely adopted in other industrial sectors (e.g. banking, finance) and its adoption in healthcare is rapidly increasing. A recent *Infoway* survey found that about nine out of 10 Canadian healthcare organizations have their employees sign confidentiality agreements.[55] This requirement is intended to provide a legal means of seeking redress against staff who violate the confidentiality of PHI[56].

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

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

[56] 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 organizations and regulatory bodies.

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.

4.5.2 During Employment

4.5.2.1 Information Security Awareness, Education and Training

Security Requirement 15 – Training Users and Raising Security Awareness

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

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 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 23 – Training Users and Raising Privacy Awareness**, there is an obvious expectation that privacy and security training be treated together in a coherently and consistent fashion.

4.5.3 Employment Termination

Security Requirement 16 – Terminating User Access when Terminating Employment

All organizations connecting to the EHRi or hosting components of 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 system connected to the EHRi or who has access to hosted components of the EHRi upon termination of their employment with the organization.

Admin 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 78 – Providing Digital Signatures for Users**).

See also the requirement for time limited user registrations (**Security Requirement 55 – Time-Limited User Registration)** and the requirement that confidentiality agreements survive the termination of employment mandated by **Security Requirement 14 – Confidentiality Agreements**.

4.6 Physical and Environmental Security

The objectives of physical and environmental security are to:

- Prevent unauthorized access, damage and interference to business premises and information;
- Prevent loss, damage or compromise of assets and interruption to business activities; and
- Prevent compromise or theft of information and information processing facilities.

4.6.1 Secure Areas

Security Requirement 17 – Physically Securing EHRi Systems

All organizations 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.

Admin 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 requires 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.

4.6.2 Equipment Security

4.6.2.1 Equipment Siting and Protection

Security Requirement 18 – Protecting EHR Systems from Hazards

All organizations 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.

4.6.2.2 Supporting Utilities

Security Requirement 19 – Protecting EHR Systems from Disruption

All organizations 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.

4.6.2.3 Equipment Maintenance and Security of Equipment Off-Premises

Security Requirement 20 – Protecting EHRi Equipment Off-Premises and During Maintenance

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

a) Is not used outside their premises without appropriate safeguards and prior authorization by the organization's management; and

b) Is repaired or serviced by authorized personnel only.

Admin Requirement

Examples of off-site use include:

- Temporary siting of servers off-site during renovations to premises;
- Relocation of operations during disaster recovery;
- 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 4.9.8 – Mobile Computing and Teleworking**.

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 3.5 – Limiting Use, Disclosure and Retention of Personal Health Information**.

4.6.2.4 Secure Disposal and Reuse of Equipment

Security Requirement 21 – Disposal/Reuse of EHRi Equipment

All organizations connecting to the EHRi or hosting components of the EHRi **must** securely overwrite or 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 3.5 – 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 34 – Disposing of Media Containing PHI**.

4.6.2.5 Removal of Property

Security Requirement 22 – Removing EHRi Equipment, Data or Software

All organizations hosting components of the EHRi **must not** allow equipment, data or software supporting the EHRi to be removed without authorization by the organization'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 3.5 – Limiting Use, Disclosure and Retention of Personal Health Information**.

4.7 Communications and Operations Management

The objectives of communications and operational management security are to:

- Ensure the correct and secure operation of information processing facilities;
- Minimize the risk of system failures;
- Protect the integrity of software and information;
- Maintain the integrity and availability of information processing and communications;
- Ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- Prevent damage to assets and interruption to business activities; and
- Prevent loss, modification or misuse of information exchanged between organizations.

4.7.1 Operations Procedures and Responsibilities

4.7.1.1 Change Management

Security Requirement 23 – Controlling Changes to the EHRi

All organizations 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.

Admin Requirement

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

4.7.1.2 Segregation of Duties

Security Requirement 24 – Segregating Duties

All organizations 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.

Admin Requirement

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

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

4.7.1.3 Separation of Development, Test and Operational Facilities

Security Requirement 25 – Separating Development and Testing from Operations

All organizations 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 organization hosting the affected application(s).

Admin Requirement **Tech Requirement**

This requirement may not affect organizations that do not develop applications in-house, although 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.

4.7.2 Third-Party Service Delivery Management

Third-party service delivery is dealt with in **Security Requirement 5 – Assessing Threats and Risks from Third Parties** and in **Security Requirement 6 – Addressing Security in Third-Party Agreements**.

4.7.3 System Planning and Acceptance

Security Requirement 26 – Maintaining Capacity

All organizations 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.

Admin Requirement Tech Requirement

As stated in ISO/IEC 27002:2011, "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 27 – Upgrading the EHRi

All organizations 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.

Admin Requirement Tech Requirement

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

4.7.4 Protection Against Malicious and Mobile Code

Security Requirement 28 – Protecting Against Malware

All organizations connecting to the EHRi or hosting components of 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.

4.7.5 Backup

Security Requirement 29 – Securely Backing Up Data

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

a) Back up[57] 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 4.7 – Physical and Environmental Security**).

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.

4.7.6 Network Security Management

Security Requirement 30 – 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

Tech Requirement

[57] 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.

to maintain the confidentiality and integrity of this data whenever it is transmitted outside the physical security perimeter[58] that protects information processing facilities supporting EHRi servers, applications or data.

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 direction regarding protection of information during transmission, but there are some general requirements. For example, Ontario's health information legislation requires custodians to "transfer PHI in a secure manner". Manitoba's health information legislation requires that a trustee who uses electronic means to request disclosure and respond to requests for disclosure implement procedures to prevent the interception of information by unauthorized persons.

Security Requirement 31 – 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 32 – Acknowleging 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

[58] Requirements for maintaining a physical security perimeter are found in **Security Requirement 17 – Physically Securing EHRi Systems**.

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

4.7.7 Media Handling

4.7.7.1 Management of Removable Computer Media

Security Requirement 33 – Protecting PHI on Portable Media

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

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

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

Admin Requirement Tech Requirement

Rationale: This requirement protects information stored on removable media. Mobile devices are covered in **Security Requirement 72 – Acceptable Use of Mobile Devices**.

4.7.7.2 Disposal of Media

Security Requirement 34 – Disposing of Media Containing PHI

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

Admin Requirement Tech Requirement

Rationale: This is a minimum requirement. Legal requirements follow from the Manitoba regulations pursuant to the 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 has been copied to other media or exists in other systems prior to media disposal). Note also the discussion in **Section 3.5 – Limiting Use, Disclosure and Retention of Personal Health Information**on the legal requirements for safe disposal.

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

See also **Security Requirement 21 – Disposal/Re-use of EHRi Equipment**.

4.7.7.3 Protecting PHI on storage Media

Security Requirement 35 – Protecting Data Storage

All organizations 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 17 – Physically Securing EHRi Systems**;

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 3.5 – Limiting Use, Disclosure and Retention of Personal Health Information**. Encryption of data stores is still uncommon in healthcare and healthcare organizations 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 who have gained 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 36 – Protecting Storage of Unencrypted PHI in the EHRi

All organizations 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.

Admin Requirement

Rationale: This requirement follows directly from the privacy requirements in **Section 3.5 – Limiting Use, Disclosure and Retention of Personal Health Information** and complements **Security Requirement 35 – Protecting Data Storage** in ensuring the confidentiality and availability of EHRi data.

4.7.8 Exchange of Information

4.7.8.1 Information Exchange Policies and Procedures

The policies and procedures required of organizations hosting components of the EHRi are discussed in **Privacy Requirement 2 – Third-Party Agreements** and in **Security Requirement 7 – Transmitting PHI**.

4.7.8.2 Exchange Agreements

Information exchange agreements should be executed between (among) jurisdictions operating EHRi components prior to PHI flowing across provincial/territorial borders. Such agreements should 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/IEC standard 22857: "Health Informatics: Guidelines on data protection to facilitate trans-border flows of personal health information".

4.7.9 Electronic Commerce Services

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

4.7.10 Monitoring

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

4.7.10.1 Audit Logging Updated

Security Requirement 37 – Logging Transactions in the EHRi

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

a) Accesses, creates or updates[59] 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:

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

This requirement follows from **Privacy Requirement 12 – Logging the Application of Consent Directives** and **Privacy Requirement 18 – Logging Access, Modification and Disclosure** and is also required for effective compliance with legislation in some jurisdictions.[60] It also follows secondarily from **Privacy Requirement 6 – Limitation of Collection to Identified Purposes** and **Privacy Requirement 25 – Patient/Person Access**. Legal requirements also arise from the

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

[60] 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.

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 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, *DICOM Supplement 95 – Audit Trail Messages*[61] is widely used and describes a schema for reporting information necessary for privacy and security auditing of healthcare applications and is endorsed in the IHE IT Infrastructure Technical Framework – Volume 2a: Transactions Part A - Audit Trail and Node Authentication Profile (ITI-20).[62] These two specifications are also referenced within the recently published ISO 27789:2013 – Audit trails for electronic health records.

[61] The DICOM Supplement 95 specification is available at: ftp://medical.nema.org/medical/dic _ft.pdf

[62] The latest version of the IHE IT Infrastructure Technical Framework – Volume 2a: Transactio iciation is available at: http://www.ihe.net/technical_frameworks/#IT.

Tech Requirement

Security Requirement 38 – 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.

Rationale: Such a capability 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 necessitates 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 concerning the accuracy or inaccuracy of a data element.

Security Requirement 39 – 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 as 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 40 – 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 26 – Amending Inaccurate or Incomplete Information.

Though the storage required for logging 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 organizations.

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 who discloses PHI to make a note of the name of the person to whom the information was disclosed, 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 met when the requirement above is taken together with the other audit logging requirements in this section.

Security Requirement 41 – 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 18 – Logging Access, Modification and Disclosure**.

Security Requirement 42 – 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[63];

c) The organization of the accessing user (at least in those cases where

Tech Requirement

[63] A user may be assigned more than one role, but **Security Requirement 58 – Selecting a Single Role Per Session** mandates that the user can only exercise one role at a time.

an individual accesses information on behalf of more than one organization);

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

e) The function performed by the accessing user;

f) A timestamp;

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.

Rationale: This requirement follows from **Privacy Requirement 18 – Logging Access, Modification and Disclosure**, **Privacy Requirement 19 – Notifying Patients/Persons of Inappropriate Access, Use or Disclosure** and **Privacy Requirement 20 – Retaining Records**.

Note that Alberta's health information legislation requires a custodian who discloses PHI to make a note of the name of the person to whom the information was disclosed, 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 45 – Detecting Patterns of Misuse**, **Security Requirement 46 – Reporting Every Access to a Patient/Person's EHR**, **Security Requirement 47 – Reporiting Every Access by a User** and **Security Requirement 48 – Analyzing EHRi Audit Logs for Patients/Persons at Elevated Risk**.

Security Requirement 43 – Retaining Audit Logs

All organizations connecting to the EHRi or hosting components of the EHRi **must** retain[64] the audit log for the entire retention period of the records audited in order to enable investigations to be carried out when necessary and to provide evidence where necessary.

Rationale: This requirement follows from **Privacy Requirement 18 – Logging Access, Modification and Disclosure**, **Privacy Requirement 19 – Notifying Patients/Persons of Inappropriate Access, Use or Disclosure** and **Privacy Requirement 20 – Retaining Records**.

Note that Alberta's health information legislation requires a custodian who discloses PHI to make a note of the name of the person to whom the information was disclosed, 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 45 – Detecting Patterns of Misuse**, **Security Requirement 46 – Reporting Every Access to a Patient/Person's EHR**, **Security Requirement 47 – Reporiting Every Access by a User** and **Security Requirement 48 – Analyzing EHRi Audit Logs for Patients/Persons at Elevated Risk**.

4.7.10.2 Monitoring System Use

Security Requirement 44 – 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.

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

Tech Requirement

Security Requirement 45 – 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).

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 46 – Reporting Every Access to a Patient/Person's EHR

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

Tech Requirement

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 54 – Assigning Identifiers to Users**.

Security Requirement 47 – 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 54 – Assigning Identifiers to Users**.

Security Requirement 48 – 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 22 – Denoting Patients/Persons at Elevated Risk**, the records of certain patients/persons (e.g. celebrities, politicians, 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 patients/persons is 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 22 – Denoting Patients/Persons at Elevated Risk** for the requirement to provide a facility to denote which patients/persons are at elevated risk.

4.7.10.3 Protection of Log Information

Security Requirement 49 – 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 50 – 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.

4.7.10.4 Review of System Logs and Audit Trails

Security Requirement 51 – Regularly Reviewing EHRi Audit Logs

All organizations 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 logs are of questionable utility if not reviewed, and so periodic review ought to be a minimum requirement. Note that analysis tools that facilitate audit log review are mandated in **Security Requirement 45 – Detecting Patterns of Misuse**, **Security Requirement 46 – Reporting Every Access to a Patient/Person's EHR**, **Security Requirement 47 – Reporting Every Access by a User** and **Security Requirement 48 – Analyzing EHRi Audit Logs for Patients/Persons at Elevated Risk**. Review of audit logs should be done by one or more responsible individuals assigned the task as in **Security Requirement 3 – Information Security Management, Co-ordination and Allocation of Responsibilities**. 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.”

4.8 Access Control

The objectives of this section of ISO/IEC 27002 are to:

- Control access to information;
- Prevent unauthorized access to information systems;
- Ensure the protection of networked services;
- Prevent unauthorized computer access;
- Detect unauthorized activities; and
- Ensure information security when using mobile computing and tele-networking facilities.

4.8.1 Requirements for Access Control

Security Requirement 52 – Policy for Access Control

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

Policy & Procedures

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.

4.8.2 User Access Management

4.8.2.1 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 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 53 – Registering Users

All organizations 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) 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) Each potential user has a legitimate relationship with the organization; and

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

Admin Requirement

Rationale: This requirement follows directly from **Privacy Requirement 12 – Logging the Application of Consent Directives** 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 accessanonymized data, for example,.

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.

Security Requirement 54 – Assigning Identifiers to Users

All organizations 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), 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 55 – Time-Limited User Registration

All organizations 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 must be renewed).

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 60 – Timely Revocation of Access Privileges**. 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 56 – Reviewing User Registration Details

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

Admin Requirement

This requirement, together with requirement **Security Requirement 55 – Time-Limited User Registration** ensures that user registration details (for example, a contact phone number or email address) remain current.

Rationale: This requirement facilitates accountability.

4.8.2.2 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 or 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 patients/persons seen by other 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); or
- 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 (e.g.a family physician) to confer access to other users who have no previously established relationship to that patient/person's EHR (e.g. a specialist).

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 57 – 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.

Security Requirement 58 – 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 he/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 organization of roles, accommodating users who frequently switch between dual roles that are both related to clinical care, would greatly reduce user frustration caused by having to switch between one role and the other. Properly designed roles will ensure that users rarely, if ever, have to 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) Organizations (e.g., a primary care clinic or a primary healthcare team in a rural community);

b) Organizational units (e.g. hospital emergency department); 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 (e.g.nurses' association) 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 (e.g. family physician) to exercise the access privileges of that role upon all the records accessible by members of the working group, such as patients/persons in a primary care clinic.

Security Requirement 59 – Granting Access to Users in Workgroups

The EHRi and all PoS systems connected to the EHRi **must** be capable of assigning users to working groups and 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-protection feature that all Canadians might reasonably expect to be in place 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.).

Security Requirement 60 – 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. 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 (e.g. a responsible physician) may need to rapidly grant access to a user who has never had a previous legitimate relationship with the patient (e.g. a specialist). 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 61 – Granting Access By Association

The EHRi and all PoS systems connected to the EHRi:

a) **Must** be capable of associating users (i.e. 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); and

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.

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

Tech Requirement

Rationale: This requirement is essential if **Security Requirement 59 – Granting Access to Users in Workgroups** 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 (e.g. a specialist) full access to one of his/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, since role-based access control would typically prevent nurses from exercising such a function.

Security Requirement 62 – 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(s) the user can access; and

c) Which privileges (e.g. viewing, modification) the user has with respect to each of these records.

Policy & Procedures

Admin Requirement

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.

4.8.3 User Responsibilities

Security Requirement 63 – Acceptable-Use Agreements

Organizations 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.

Policy & Procedures

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 15 – Training Users and Raising Security Awareness**) 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.

4.8.4 Network Access Control

Security Requirement 64 – Authenticating EHRi Network Access

Organizations 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 65 – Controlling Access to EHRi Network Diagnostics and Network Management Services

Organizations 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 66 – Segregating EHRi Network Users, Services and Systems

Organizations 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.

Tech Requirement

Security Requirement 67 – Controlling Routing on EHRi Networks

Organizations hosting components of the EHRi **must** have routing controls[65] on networks hosting those components to ensure that data flows across the network perimeter do not breach the organization's access-control policy.

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.

4.8.5 Operating System Access Control

Security Requirement 68 – Controlling Access to EHRi System Utilities

Organizations 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 69 – 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 connection 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 than a few minutes.

[65] Firewalls are a common example of routing controls.

4.8.6 Application and Information Access Control

Security Requirement 70 – 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 such as:

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., so users do not need to be authenticated twice).

4.8.7 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 4.9.8 – Mobile Computing and Teleworking** and in more detail in the Privacy and Security Considerations section that follows.

Security Requirement 71 – Restricting Access to Unattended Workstations

All PoS systems connected to the EHRi **must** protect unattended workstations against an unauthorized person using the workstation while the PoS is active, such as with an automatic timeout after a period of inactivity. Thed best approach is to place workstations in a physically secure area in the first place.

Tech Requirement

Rationale: Most systems already implement 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 other people's records.

4.8.8 Mobile Computing and Teleworking

As noted in ISO/IEC 27002, 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 when back-ups are scheduled.

Security Requirement 72 – Acceptable Use of Mobile Devices

Organizations 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.

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.

Security Requirement 73 – Acceptable Use of Teleworking

Organizations connecting to the EHRi **should**:

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

b) Prohibit teleworking by a PoS system user unless the user agrees to abide by this policy.

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 74 – Protecting Wireless Networks

Organizations connecting to the EHRi or hosting components of 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 attack vectors 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 30 – Encrypting PHI During Transmission** implies that all wireless communication of PHI be encrypted. The requirement above makes this implicit requirement explicit.

4.9 Information Systems Acquisition, Development and Maintenance

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

- Ensure security is built into operational systems;
- Prevent loss, modification or misuse of user data in application systems;
- Protect the confidentiality, authenticity, availability and integrity of information;
- Ensure IT projects and support activities are conducted in a secure manner; and
- Maintain the security of application system software and data.

4.9.1 Security Requirements of Information Systems

Section 4 of this document contains base security requirements of the EHRi.

4.9.2 Correct Processing of Information

Security Requirement 75 – 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) 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 anonymization and pseudonymization is outside the scope of this document.

4.9.2.1 Input Data Validation

Security Requirement 76 – 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:

i. out-of-range values;

ii. invalid characters in data fields;

iii. missing or incomplete data;

Tech Requirement

iv. exceeding upper and lower data volume limits;

v. unauthorized or inconsistent control data.

b) Procedures for responding to validation errors.

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

4.9.2.2 Output Data Validation

Security Requirement 77 – Validating Printed Data

All PoS systems connected to the EHRi **should** ensure it is possible to check that hardcopy printouts 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.

4.9.3 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, since Canadian law requires that prescriptions be signed.[66] 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 (e.g. 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, such as 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

[66] 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."

methodology as per **Security Requirement 70 – Robustly Authenticating Users**, and so can fulfill this function as well as provide for signature capability.

Security Requirement 78 – 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 system users to apply a digital signature that satisfies the requirements under PIPEDA and its regulations[67] 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.

Security Requirement 79 – 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;

Tech Requirement

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

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 (i.e., that the associated signature certificate had not been revoked);

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

4.9.4 Security of System Files

Security Requirement 80 – Implementing Software and Upgrades in the EHRi

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

Admin Requirement

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

4.9.5 Security in Development and Support Processes

Security Requirement 81 – Protecting EHRi Software

Organizations 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 organization.

Tech Requirement

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

4.9.6 Vulnerability Management

Security Requirement 82 – Managing Known Vulnerabilities

Organizations 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 components.

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 that fix known security problems either be applied when available or 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.

4.10 Information Security Incident Management

The objectives of security incident management are to:

- Build a reporting infrastructure for reporting incidents and weakness; and
- Manage incidents and institute improvements to prevent their future occurrence.

4.10.1 Reporting Incidents and Weaknesses

Security Requirement 83 – 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 – Information Security Management, Co-ordination and Allocation of Responsibilities** of every detected pattern of system misuse (see **Security Requirement 45 – Detecting Patterns of Misuse**).

Tech Requirement

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

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 19 – Notifying Patients/Persons of Inappropriate Access, Use or Disclosure**.

4.10.2 Management of Incidents and Improvements

Security Requirement 84 – Responding to Security Incidents Involving the EHRi

Organizations 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.

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 minimize 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.

4.11 Business Continuity Management

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

Security Requirement 85 – Managing Business Continuity

Organizations hosting components of the EHRi **must** put in place a managed process for developing and maintaining business continuity throughout the organization, 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

Admin Requirement

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

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.

Organizations 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 86 – Testing Business Continuity Plans

Organizations 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.

Admin Requirement

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

4.12 Compliance

The objectives of compliance in information security management are to:

- Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations, and of any security requirements;
- Ensure compliance of systems with organizational security policies and standards; and
- Maximize the effectiveness of, and minimize interference with/from, the system audit process.

4.12.1 Compliance with Legal Requirements

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

4.12.2 Compliance with Security Policies and Standards

Security standards for the EHRi are based on ISO 27002 and ISO 27799. Readers are encouraged to consult with their jurisdictional standard setting bodies to determine which standards are applicable to a specific initiative. Compliance to jurisdictional IT security polices and standards is outside the scope of this document.

4.12.3 Information Systems Audit Considerations

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

5 Privacy and Security Considerations

5.1 Introduction

The preceding requirements sections identify specific privacy and security aspects that an organization must or should put in place when building or connecting to an interoperable EHR.

Infoway feels that a digital health future-state objective is to achieve seamless integration of emerging e-health solutions and access to relevant PHI by authorized clinicians, consumers and caregivers. Access by multi-platform devices and use of emerging technologies will become the norm.

As a result of the adoption of emerging technologies such as mobile and cloud computing, *Infoway* has developed a series of privacy and security considerations to assist in the deployment of emerging digital health solutions. Health Delivery Organizations (HDOs) and e-health portfolio managers may wish to take the following series of privacy and security considerations into account as they plan and deploy emerging technologies within the digital health ecosystem.

The update to this document entails a repositioning of the subsequent sections. For the following topics, *Infoway* has identified a series of '*considerations'* rather than 'requirements'. This approach is based on the following rationale:

- Jurisdictions are ultimately responsible for choosing the level of P&S risk acceptable to them;
- This tool will facilitate the management of privacy and security risk by providing jurisdictions with considerations for privacy enhanced and secure e-health solutions (both current and future); and
- Not all requirements are applicable to every solution context, given the broadening of scope.

In this section, the reader will find privacy and security considerations that have arisen since the release of Version 1.1 of the Privacy & Security Requirements document as a result of:

- The general expansion of the e-health mandate to encompass many additional IT-enabled functions beyond the interoperable EHR; and
- The ever-increasing pace of adoption of emergent technologies in the healthcare space, which introduces new privacy- and security-related challenges and solutions.

This section is divided into health system functions, such as CPOE, and emerging technology topics. For each sub-section within each topic, the following is provided:

- A definition of the topic, in order to scope the discussion;
- A discussion of issues specific to the topic; and
- Identification of a set of considerations specific to the topic.

The reader should note that requirements defined in the previous sections of this document may also be applicable to the e-health topics described below. Both the Requirements and the Considerations should be taken into account when establishing privacy and security requirements for solutions employing elements of the topic areas in the document.

The convergence of emerging technologies enabling new digital health solutions such as cloud computing, mobile patient remote monitoring, e-visits and e-scheduling will require organizations to take several of the following sections into account when deploying new digital health solutions. By way of example, an 'e-booking' solution fully integrated into an EMR and the patient's consumer health solution may allow both the patient and clinician to view and confirm appointments via their mobile devices. Should the EMR be integrated into a cloud-offered 'e-booking' component and consumer health solution (CHS), the privacy and security considerations for cloud and mobile computing as well as the Federated Identity Management (FIdM), PoS and CHS topics should be consulted.

The privacy and security considerations described in the subsequent chapters are organized according to the 10 privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96) and the revised standard, ISO 17799-1:2004.

In an attempt to guide the reader, certain considerations have been identified with an exclamation point symbol.

⚠

Considerations so marked are considered to be leading practices and are considered highly desirable.

5.2 Health System Topics

The health system topics covered by this document deal with those areas where *Infoway* and its stakeholders are experiencing increased planning, funding and deployment of healthcare solutions to individuals or populations using the listed health information technologies, thus creating the need to enhance the privacy and security considerations since the previous publication.[68]

The topics in this section include:

- Consumer Health Solutions;
- Point-of-Service Solutions;
- Cloud Computing;
- Mobile Computing;
- Remote Patient Monitoring;
- Federated Identity Management;

[68] Canada Health Infoway Electronic Health Record (EHR) Privacy and Security Requirements, Version 1.1, February 7, 2005

- Secondary Uses of health information and associated analytics; and
- Inter-Jurisdictional Data Sharing.

5.2.4 Consumer Health Solutions

Consumer Health Solutions (CHS) are seen as a broad range of health IT systems that serve the patient or individual, and allow them to access the health system via some computing device. The device could be a person/patient's home computer, laptop, tablet, mobile phone or other networked computing device. *Infoway* has defined both Consumer Health Applications (CHA) and Consumer Health Platforms (CHP). For the purposes of this document, a Consumer Health Solution could be either of those, separately or combined.

"*A consumer health application is an electronic solution that enables the consumer to collect, retrieve, manage, use and share personal information and other health-related data. A consumer health application could include applications commonly known as personal health records and patient portals. If connected to a consumer health platform, the consumer health application provides access to the services provided by the platform and the personal information stored in the platform.*"[69]

"*A consumer health platform is an electronic system that provides a secure, interoperable environment and personal health information database. The platform enables a range of consumer health applications, most often from different vendors, to run and interoperate.*"

The consumer health platform also facilitates the sharing of data by the consumer with clinicians, family members and other authorized individuals, as well as with other applications and health information systems (Electronic Health Records (EHRs), Electronic Medical Records (EMRs) and Hospital Information Systems (HIS))."[70]

It should be noted that while several sources were used for the content of this section, a great deal of the material is sourced from the COACH document *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, which can be obtained from the COACH Web site at: http://www.coachorg.com/en/practices/2012-Special-Edition-Patient-Portals.asp.

5.2.4.1 Scope

Figure 1 below describes the taxonomy[71] of Consumer Health Solutions. The discussion that follows will be focused on CHSs that are publicly funded, or those that have a combination of provider and patient funding.

[69] Infoway website: https://www.infoway-inforoute.ca/index.php/programs-services/certification-services/what-infoway-certifies/consumer-health-application accessed 2013-01-23

[70] Infoway website: https://www.infoway-inforoute.ca/index.php/programs-services/certification-services/what-infoway-certifies/consumer-health-platform accessed 2013-01-23

[71] Jens Weber, Anissa St Pierre, James Williams, **Consumer health informatics services – a taxonomy**, Report for the Privacy Commissioner of Canada, March, 2011

These include tethered and un- tethered[72] CHSs. Marketing- or research-funded CHSs are out of scope for this section.

5.2.4.2 CHS Functions and Models

CHSs are being used to support patients in a number of areas, including:

- Patient well-being – preventative healthcare, self-assessments, life transition information and support forums;
- Patient access to the health system – locations and services of providers, appointment scheduling, etc.;
- Provision of care – information provisioning, coordination of care (e.g. online care plans);
- Health system efficiency – allowing patients and providers new ways to communicate and interact (e.g. e-mail, online prescription renewals, online consultations); and
- Health system performance and quality of care – feedback from patients on the care that they receive, and comparison to published best practices.

[72] An un-tethered CHS is one in which patient information is contained solely within the CHS itself.

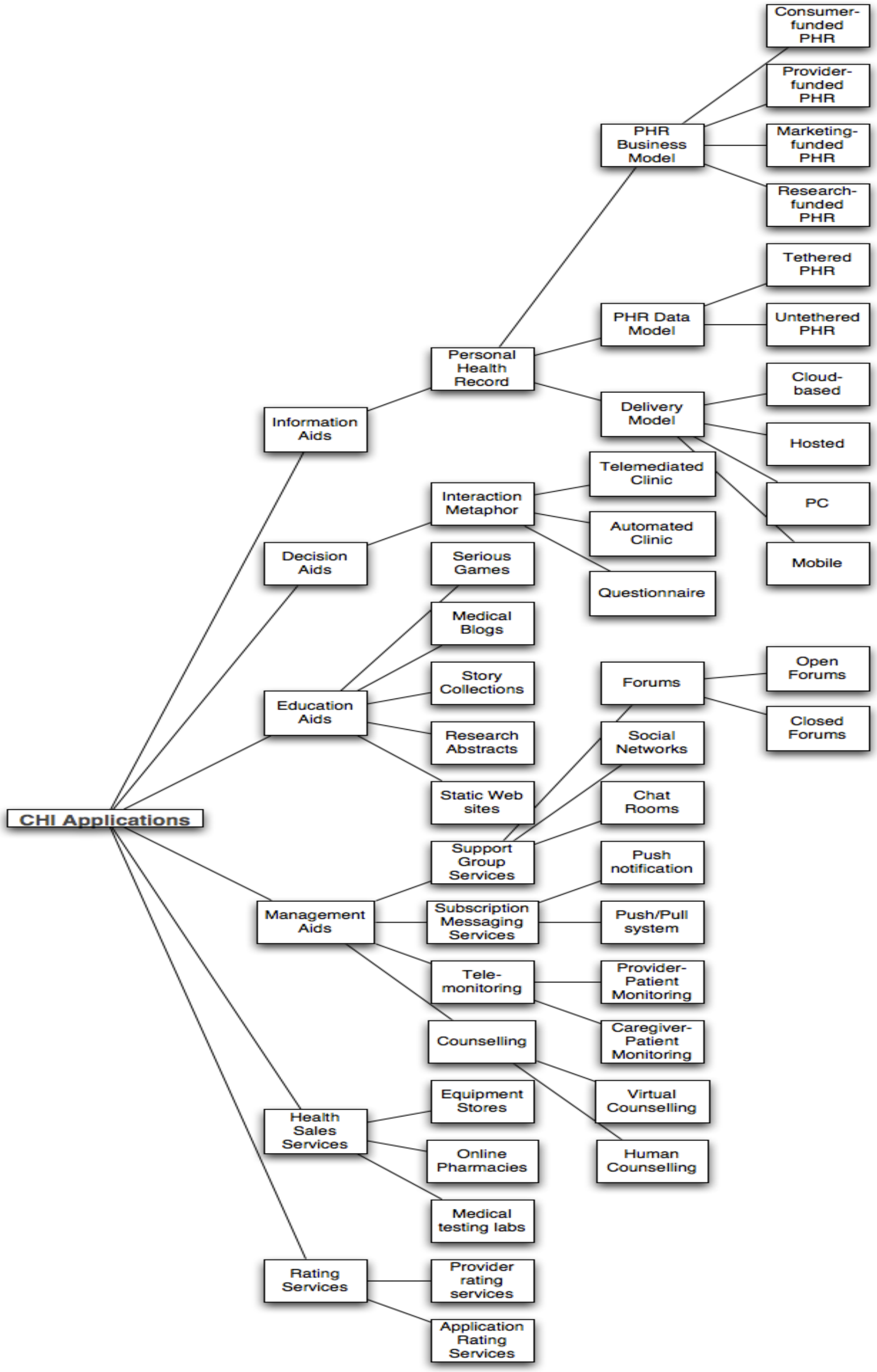


Figure 1. Consumer Health Informatics Taxonomy (Jens Weber, Anissa St Pierre, James Williams, *Consumer health informatics services – a taxonomy*, *Report for the Privacy Commissioner of Canada*, March, 2011)

Data Sources

As the taxonomy in Figure 1 indicates, there are two models that can be employed in terms of the source of patient information (i.e. the data model):

- Tethered, where patient information is primarily sourced from an organizational or jurisdictional Clinical Information Systems (CIS) or EHR; and
- Untethered, where patient information is contained solely within the CHS itself. Population of the information is generally done by the patient or a proxy, although that is not necessarily always the case.

It should be noted that discussion in the taxonomy paper[73] includes a definition of an *Integrated PHR*, which combines data from multiple sources.

Given the two models, we generally understand the tethered model to be one that can potentially provide all of the functions described in the taxonomy, while untethered CHSs are more limited in their capabilities.

5.2.4.3 Issues

Providing individuals with electronic access to their records (or records of individuals that they provide care for) introduces a number of issues, some of which are common to all CHS services and models, while others pertain only to a particular service offering or data source models.

User Education and Awareness

A common issue with any CHS implementation is one of user education and awareness in respect of privacy and security issues. With individual patients or their caregivers accessing consumer health solutions, healthcare organizations will have a new class of users that most likely will not have much, if any, awareness of privacy and security issues or protections. Organizations sponsoring consumer health solutions will need to develop and provide appropriate privacy and security awareness materials specifically designed for consumers.

The breadth of the awareness program will depend on the types of functions being offered by the solution. For example, a solution that offers social networking or support group functions may need to provide additional privacy and security information for consumers because of the potential for unintended disclosure of information about themselves or their family members.[74]

Custodianship

Consumer health solutions need to address the issue of who has custody and control of Personal Information (PI) or PHI at any point in time. One facet of the issue is identifying where the transfer of obligation occurs in the case where an individual is viewing or printing PI/PHI that the sponsoring

[73] *Consumer Health Informatics taxonomy* (Jens Weber, Anissa St Pierre, James Williams, Consumer health informatics services – a taxonomy, Report for the Privacy Commissioner of Canada, March, 2011), pg. 12

[74] J. Williams and J. Weber-Jahnke, *The Regulation of Personal Health Record Systems in Canada* – Canadian Journal of Law and Technology, Vol 8, No. 2, 2012 - pg. 249

organization has custody of. In the case of publically funded, un-tethered CHSs, consumers should be made aware of their custodial responsibilities.

Another facet is related to the amount of control an individual has, especially in non-tethered CHSs, over the PHI they enter into the solution. Once PHI is entered into the system, is the sponsor deemed to have collected it? If the sole use of the PHI is by the individual, what mechanisms are available for the individual to control the use and disclosure of their PI/PHI? These mechanisms would be more akin to access-control policies than consent directives, although they may look very similar to the individual user. While the individual may have custody of their information in this situation, they would not be considered a custodian in law. Organizations that are sponsoring a CHS will need to assess this issue to assess legal authorities and responsibilities for both individuals and the organization.

Deployment

Discussion of consumer health solutions in this document is limited to those provided or sponsored by the publicly funded health system in Canada. As a result of the limitation on scope, deployment options are most likely also limited to cloud-based and hosted models. As cloud computing issues vary from the traditional hosting environment , readers are encouraged to consult the Cloud computing privacy and security issues and considerations explored later in this document in **Section 5.3.1 Cloud computing** .

Accuracy

Solutions that include functions that enable individual users to enter PHI intended to be used for clinical decision making may not provide organizations with mechanisms to establish the provenance and veracity of that information

In the CHS context, information provided in a form intended for a healthcare professional may not be considered complete or provided with adequate context for non-professional users to interpret correctly.

Identity and Trust

Ensuring that the person who established an account is the person they are claiming to be (identity-proofing), and ensuring that the person signed on to a specific account is the person to which the account has been assigned (authentication) are common issues for every computer system. The addition of patients/consumers as system users, combined with the sensitive nature of the information contained in CHSs, raises the importance of identity management authentication and trust since solutions for employees, agents and consumers may differ. By way of example, the solution for verifying a consumer's identity may vary when compared to that for a clinician's. This is primarily due to the potentially large number of consumers.

In situations where an integrated CHS is in use, the use of multiple source applications to provide data to the CHS may introduce differing identity and authorization requirements, policies and solutions. From a user perspective, this may lead to a requirement to keep track of multiple credentials, which will lead to a reduction in usability and potentially security. The additional complexity introduces privacy and security risks since the administrative burden increases and the ease of tracking activities decreases. Readers are encouraged to consult the FIdM privacy and security issues and considerations explored later in this document.

Where solutions provide mechanisms for an individual user to identify and/or modify their care team or circle of care, ensuring that those users are able to accurately and consistently identify providers is critical to ensuring that inappropriate disclosure of PI or PHI does not take place. The user interface should include mechanisms that limit the potential for erroneous disclosure of PHI, such as displaying clinician demographic information and/or speciality.

5.2.4.4 Privacy Considerations

The considerations that follow are organized according to the 10 privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), followed by security issues.

Accountability

Consideration CH1 – Perform a Privacy Impact Assessment

A Privacy Impact Assessment (PIA) should be considered whenever new or changed functionality involves personal information or personal health information.

Admin Consideration

Rationale: For a tethered/integrated solution, this may be a legal requirement; however, untethered solutions may not have the same legal constraints. Regardless, the use of Privacy Impact Assessments is considered to be a best practice when dealing with systems that collect, use or disclose PI or PHI.

This consideration is consistent with **Privacy Requirement 4 – Privacy Impact Assessment**. The use of a Privacy Impact Threshold Analysis can assist in determining whether a PIA is warranted.

Consideration CH2 – Identify and communicate where the transfer of accountability occurs

Organizations should develop and provide educational material that makes individuals who are users of the CHS aware of the point at which they become responsible for any of the PHI that was obtained from the CHS.

Admin Consideration

Rationale: Without prior education, individual users may assume that the organization will continue to be accountable for the appropriate safeguarding of their PHI even after it has been transferred to the individual (e.g., when the patient prints information on their local printer).

While the organization remains accountable for the information in its custody, only appropriate education will allow individuals to recognize when they become accountable for the PHI they have obtained from the CHS and what controls they can use to continue to safeguard their information.

Consideration CH3 – Develop and provide appropriate user privacy training and guidance

Organizations should develop and provide privacy training and guidance material appropriate for the users of the solution being offered.

Admin Consideration

Rationale: Potentially unsophisticated users accessing a CHS over the Internet via desktop PC, tablet or other mobile device may be unintentionally exposing themselves and other CHS users to attack. Providing appropriate security and privacy training and guidance helps to manage privacy risks to PHI.

Consideration CH4 – Provide mechanisms for individual users to remain accountable

In the case of non-tethered solutions, where the individual is storing PHI in the solution, the sponsors should provide the individual user with both administrative and technical mechanisms to control (preferably fine-grained) the use, disclosure and retention of that information.

Admin Consideration

Tech Consideration

Rationale: In cases where the organization would not be considered to have collected the information, the individual is still responsible for safeguarding their own PHI. The CHS solution should provide individuals with the necessary mechanisms to control their PHI, allowing them to maintain accountability for its use, disclosure and retention.

In CHSs that provide individuals the ability to identify trusted relationships with other individuals who are not providers (e.g. family members, other caregivers), the CHS must include facilities that allow individuals to maintain those relationships, and might even go so far as to verify those relationships with the individuals at regular intervals.

Identifying Purposes

⚠ **Consideration CH5 – Publish purpose(s)**

A Consumer Health Solution should provide registrants and current users with an easily obtainable, comprehensive list of purposes for which a user's PI and PHI contained in, or collected via, the solution will be used by the organization or designated caregiver.

Policy & Procedures

Admin Consideration

Rationale: Aside from being a fundamental privacy principle, identifying the purpose(s) for which information is being collected, used, disclosed or retained provides the user with information necessary to make an informed choice. In addition, unclear or non-specific purposes effectively disable the limiting principle.

Organizations should attempt to differentiate the custody and control of an individual's PHI as offered by the organization versus a privately funded CHS. In the former case, the organization retains custodial obligations, while in the latter there may be no custodian from a legal perspective. It will be important to ensure that consumers are aware of the difference between the two. In either case, organizations should note that the individual is free to use or disclosure PHI pertaining to themself for whatever purposes the individual sees fit; however, those uses or disclosures are not protected by any custodial obligation of the organization.

This consideration is consistent with **Privacy Requirement 5 – Identifying Purposes for Collection, Use and Disclosure**.

Consideration CH6 – Communicate if and when individual-entered information will be reviewed by a provider[75]

Provider organizations should provide information to patients to make it clear when or if patient-entered information will be reviewed by a provider.

Admin Consideration

Rationale: A patient's assumption regarding how and when clinicians may use patient-entered information in a CHS may not align with current clinical process or practice.

Consent

Consideration CH7 – Obtain consent and agreement to participate separately[76]

As a best practice, the CHS provider may wish to obtain express consent from the individual for the collection, use and disclosure of both PI and PHI as it applies to the CHS, even if express consent is not legally required.

In addition, and as a separate component of the registration process, the CHS provider should obtain an agreement to participate in the CHS from the registrant. The agreement should identify the registrant's and CHS provider's responsibilities and obligations.

Admin Consideration

Rationale: Where required by law, express consent must be obtained for the collection, use and disclosure of PHI; however, in the many jurisdictions where implied consent can be legally relied upon, organizations may want to consider obtaining express consent for the identified purposes of the CHS.

An agreement to participate helps to ensure that individuals understand their obligations and opportunities as well as those of the CHS provider; therefore, organizations should consider requiring that consumers provide this agreement as a prerequisite to using the CHS.

[75] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 61

[76] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 29

Providing for, and differentiating between, consent for collection, use and disclosure, and agreement to participate provides a basis for trust in the solution that may not otherwise be there.

Consideration CH8 – Educate users on the scope of consent directives[77]

If a CHS provides registered users with a facility to establish consent directives via the CHS, it should be made clear to the user what the scope of those directives is.

Admin Consideration

Rationale: Consent directives entered into a tethered CHS may only apply to an individual's PI/PHI in relation to accesses via the Clinical Information System (CIS) to which the CHS is tethered, not accesses via another system. Similarly, it may only apply to accesses that occur within the organization's boundaries (physical or logical), but not by related providers (e.g. referred consultants).

Jurisdictional CHSs may be able to manage and apply those consent directives to all healthcare transactions or only to those that are operated by the jurisdiction (or an agency).

In either case, the individual should be made aware of the scope of any consent directive that they are allowed to place.

Consideration CH9 – Obtain consent from family members prior to linking information[78]

Collection, use and disclosure of an individual's disease history, social history and genetic information can have impact on the privacy of family members. Where family members, who are users, are identified to the CHS provider, their consent should be obtained and formally recorded prior to any linking of data.

Admin Consideration

[77] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information, Special Edition*, pg. 65

[78] Jens Weber, James Williams, Anissa St Pierre, Consumer health informatics services – privacy risk assessment & mitigation, Report for the Privacy Commissioner of Canada, March, 2011, pg. 18

Rationale: Consent is one of the basic privacy principles and it takes a variety of forms in existing health data privacy laws. The consented disclosure of personal health information of one individual can result in an effective disclosure regarding several related individuals if their familial relationship is identified.

Linking in this case refers to any data linkage that allows one individual to be identified as a result of access to another individual's record. This can be especially sensitive when social networking features are included in the functionality of the CHS. This linking can take the form of having an individual identify and group family members or friends.

Consideration CH10 – Generate automatic electronic consent requests prior to linking individuals

When individuals identify other users as family members, organizations should automatically generate consent requests for that linkage and include the purposes for the linkage.

Admin Consideration

Rationale: Establishing an automated, recorded mechanism to request and collect consent for linkages helps to ensure that consent requests are consistent in language and always generated prior to linkage actually taking place.

Limiting Collection

There are no specific considerations related to limiting collection; however, please see **Consideration CH5 – Publish purpose(s)** for a discussion on the lack of a clear set of identified purposes negating the principle of limiting collection.

Limiting Use, Disclosure and Retention

Consideration CH11 – Publish retention periods for PI/PHI[79]

Organizations should identify how long certain classes of information will be available for view/download and how long information will be retained.

Admin Consideration

[79] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 23

Rationale: As part of legislative requirements, CHS providers should identify any legislative obligations with regard to PI and PHI retention periods. Consumers, as custodians, should be given notice as to the retention periods supported by the CHS.

Accuracy

Consideration CH12 – Flag patient-entered information[80]

In a tethered or integrated CHS that supports self-entered or proxy-entered information, that information should be tagged as such in order to inform the provider of the provenance of that information.

Admin Consideration

Rationale: There is a risk to patient safety if there is no mechanism for a provider to separate information that was collected by interactions with health system professionals that will have controls in place to ensure accuracy, and information that was collected by direct input from the patient or a patient proxy, where no such controls may exist.

Consideration CH13 – Review and confirm patient-entered information[81]

In a tethered or integrated CHS that supports self-entered or proxy-entered information, that information should be reviewed and confirmed with the individual prior to clinical use.

Admin Consideration

Rationale: There is a risk to patient safety if there is no mechanism to confirm the veracity of information with the patient or their assigned proxy.

[80] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 61

[81] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 61

Consideration CH14 – Ensure that a timestamp is displayed with PHI[82]

Ensure that information viewed by patients has a timestamp that indicates when the information was last updated.

Admin Consideration

Rationale: Users may be using and sharing outdated information, especially if printing information and presenting that information to other providers not associated with the CHS. Having a record timestamp displayed on any viewed or printed PHI helps anyone reading the information to understand how recent it is and whether it is likely to be out of date.

Consideration CH15 – Assist individual users in interpreting PHI [83]

Organizations should provide materials that will allow individuals accessing their medical information to correctly interpret that data where possible. Where not feasible to do so, consider marking potentially confusing information to indicate to the individual that they should seek provider support to assist them.

Admin Consideration

Rationale: Providing information in an unclear manner, out of context or without supporting information may result in patients misinterpreting information, resulting in potential safety issues.

Safeguards

Consideration CH16 – Treat tethered solutions as extensions to the CIS[84]

A tethered CHS, which is, at a minimum, an extension of a CIS, should be subject to the privacy and security policies, practices and controls of that CIS.

Admin Consideration

[82] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 50

[83] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 54

[84] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 18

Rationale: The PHI that is contained in the source CIS of a tethered or integrated CHS is more likely to have the same or more stringent privacy and security requirements when being accessed through a CHS than it does when being accessed through another mechanism. The organization has the same accountability to appropriately safeguard the information regardless of the access mechanism.

Openness

Consideration CH17 – Make PIA and TRA summaries available[85]

In order to assist in establishing and maintaining individual user trust in the CHS, sponsor organizations should make appropriate disclosures on the privacy or security risks of using the CHS. These disclosures can take multiple forms, including making the summaries of any privacy or security risk assessments easily available to registrants and existing users.

Admin Consideration

Rationale: In keeping with the principle of Openness:

> "Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals should be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable."[86]

Consideration CH18 – Publish plain-language privacy and security policies that target the individual user[87]

Organizations should publish plain-language privacy and security policies that are easily understandable by registrants and existing users.

Admin Consideration

[85] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 46

[86] *CSA Model Code for the Protection of Personal Information* (Q830-96), http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code/article/openness

[87] Jens Weber, James Williams, Anissa St Pierre, Consumer health informatics services – privacy risk assessment & mitigation, Report for the Privacy Commissioner of Canada, March, 2011, pg. 23

Rationale: Multi-level policies require the user to read all of them in context in order to gain a complete understanding of the privacy position of the CHS. Having a plain-language, single-level privacy policy enables the user to more readily understand their privacy risks.

Organizations only need to publish privacy and security policies that are appropriate for user consumption. Not all policies fall into this category. For example, the details of an organization's cryptographic key management policy will most likely not need to be made public.

Individual Access

Consideration CH19 – Provide secure mechanisms to request and receive access reports[88,89]

Organizations providing CHSs should consider giving individual users the ability to securely request and/or generate reports that detail the use and disclosure of the individual's PI and PHI contained within the CHS. In integrated CHSs, these reports could be scoped to include use and disclosure of PI and PHI within the network of data sources interoperating with, and consuming information from, the CHS.

Admin Consideration

Rationale: Allowing individual users to securely request and retrieve information on who has accessed their PI and PHI accomplishes three objectives:

1. It allows the individual an opportunity to identify inappropriate access to their PI/PHI. For certain types of unauthorized disclosures, the individual may be in the best position to perform that initial identification;

2. In providing a mechanism that is convenient for the individual, it embodies further trust in the CHS and helps to encourage greater use (and potentially result in greater health benefits); and

[88] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 80

[89] Jens Weber, James Williams, Anissa St Pierre, Consumer health informatics services – privacy risk assessment & mitigation, Report for the Privacy Commissioner of Canada, March, 2011, pg. 23-24

3. It can reduce the administrative burden on those who are responsible for responding to user requests for access reports and monitoring access and disclosure of PHI to ensure compliance, assuming the reports can be generated automatically and online. The organization will have to carefully consider whether the risks of automatic online generation can be mitigated appropriately.

Challenging Compliance

Consideration CH20 – Provide mechanisms for users to challenge compliance

Individuals have the right to challenge an organization's compliance with its own policies. Individuals should be made aware of this as part of the registration process, and the mechanism should be easily accessible by the user when using the CHS.

Admin Consideration

Rationale: Publicly funded CHSs are generally subject to the same health information or privacy sector privacy laws as provider-centric solutions. The individual generally has the right to take any challenge to compliance to the privacy commissioner or ombudsperson.

When the CHS solution is subcontracted to third-party information managers, organizations need to ensure that those information managers can assist in supporting the organization's obligations.

5.2.4.5 Security Considerations

The considerations that follow are organized to follow the Security Requirements section of this document and the security clauses contained in *ISO 27002:2008 - Information technology — Security techniques — Code of practice for information security management*.

Risk Assessment and Treatment

Consideration CH21 – Perform a threat and risk assessment for all CHS initiatives where PI or PHI is involved[90]

Organizations providing CHSs should consider providing individual users the ability to securely request and/or generate reports that detail the use and disclosure of the individual's PI and PHI contained within the CHS. In integrated CHSs, these reports could be scoped to include use and disclosure of PI and PHI within the network of data sources interoperating with the CHS.

Policy & Procedures

Admin Consideration

Rationale: As a legislative requirement in some jurisdictions, individuals have the right to request information with regard to who has accessed their PHI. This information must be provided to consumers in a timely manner. This is a consideration for tethered and integrated CHSs (See **Security Requirement 1 – Threat and Risk Assessment**). It should also be considered for untethered solutions, regardless of whether or not the sponsoring organization is considered the custodian of the information contained within the solution.

Security Policy

Consideration CH22 – Clearly delineate individual and organization responsibilities via policy

As part of any security policy that is shared with individual users, the individual must be made aware of their obligation to adequately protect computing resources (e.g. laptops, mobile devices, desktops, software) that connect to the CHS.

Rationale: While the CHS operator has a responsibility to protect the information and resources under their control, they can and should require individuals to accept accountability for protecting the individual's information and resources that are under the individual's control.

[90] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 62

Organization of Information Security

No considerations specific to consumer health solutions were identified; however, all of the security requirements identified in **Section 4.3 – Organizing Information Security.**

Asset Management

Consideration CH23 – Segment information with different classifications[91]

Consider establishing mechanisms to segment information with different classifications.

Admin Consideration
Tech Consideration

Rationale: As a vital risk-management tool and best practice, information is typically classified by level of sensitivity. Mechanisms for segmentation include physical separation of information and access-control policy based on classification tags.

Human Resources Security

No considerations specific to consumer health solutions were identified; however, all of the security requirements identified in Section 4.5 – Human Resources Security are applicable.

Physical and Environmental Security

No considerations specific to consumer health solutions were identified; however, all of the security requirements identified in **Section 4.6 - Physical and Environmental Security** are applicable.

Communications and Operations Management

Consideration CH24 – Log accesses to CHS functions and data[92]

Solutions should securely log all access to administrative and user functions as well as access to PI and PHI.

Tech Consideration

[91] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 40

[92] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 29, 65

Rationale: This is a requirement for tethered or integrated CHS solutions (see **Security Requirement 37 – Logging Transactions in the EHRi**). It is a best practice for untethered CHSs where custodian responsibility lies with the individual users.

Consideration CH25 – Provide a secure user-notification mechanism[93]

In the case of tethered or integrated CHSs, organizations should provide mechanisms to inform users when significant events occur.

Tech Consideration

Rationale: Significant events for individual users will generally be non-technical in nature. The same mechanism may be used to notify the user of privacy and/or security events as well as health-related events. This may include such events as:

- A consent directive or user-access policy has been changed;
- The user's PHI has been amended or a new instance of PHI has been received (e.g. a lab report);
- A requested report is available for their review; and
- They have received a message from another user or provider.

The mechanism should not require the user to log into the CHS in order to receive a notification, and it should not allow any confidential information to be leaked.

An example of such a mechanism might be to send an e-mail message to the user's registered e-mail address to indicate that a message is waiting for them on the CHS. The user can then log into the CHS to retrieve the message.

[93] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 42, 53

Access Control

Consideration CH26 – Select identity-proofing level of assurance by role[94]

Consider what robust mechanism(s) should be used to initially prove the identity of the registrant and whether that level of assurance is required and/or adequate for all roles accessing the solution.

Admin Consideration

Rationale: Selecting an appropriate level of assurance for ensuring the identity of an individual is a risk assessment issue. For access to an untethered CHS or where the user's role is one where PHI is not involved, a low level of assurance (e.g., Internet registration with e-mail confirmation) may be all that is required. For PHI-access to their own information in a tethered CHS, a medium or high level may be appropriate (e.g., present a health card in person at a provider's office), and for access to another user's PHI (i.e., as a proxy or a provider/user), a high level of assurance may be required.

Consideration CH27 – Use a single identity credential where possible[95]

Consider the use of a single identity (i.e. single sign-on) for users (i.e. patients or providers) where the portal provides access to other applications/services that have separate authentication mechanisms.

Admin Consideration

Rationale: Individual users accessing CHSs will most likely need to remember the credentials to log into their PC, laptop, tablet or other mobile device. They will then need to know what credentials to use to access the CHS. If the CHS requires different credentials for different functions, it may become a barrier to the adoption of the CHS due to usability issues, or it may become a confidentiality risk

[94] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 22

[95] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 23

since users may use other methods to help them remember their credentials (e.g. sticky notes on their monitor, password files on mobile devices). Please refer to the FIdM section for more information.

Consideration CH28 – Allow granular assignment of privileges[96]

When a solution allows individual users to assign PHI access privileges to other users, such as other members of their care team, the individual user should have some ability to limit that access to a subset of their privileges.

Tech Consideration

Rationale: It may not be necessary for, and users may not be comfortable with, those who are assisting with the user's care delivery to have access to the user's entire medical history. Having a granular, discretionary, access-control mechanism allows the individual to assign PI/PHI access privileges they are comfortable with to non-provider members of their care team.

Information Systems Acquisitions, Development and Maintenance

Consideration CH29 – Ensure individuals are made aware of consequences of CHS change of ownership

As part of the registration process, and easily accessible to individual users at any time, organizations should have clearly defined policies that inform the users of the way their information will be handled in the event of a transfer of ownership (e.g. merger, acquisition) of the CHS.

Admin Consideration

Rationale: Individuals should be informed beforehand about what might happen to the information in the CHS if the CHS provider company terminates operation, is acquired or any other significant business event occurs. The policy should identify items such as the mechanism(s) that would be used to notify the individual and indicate whether they will have the option of 'opting out' and whether or how long the policy might survive any transfer of

[96] COACH - *Privacy & Security for Patient Portals – 2012 Guidelines for the Protection of Health Information Special Edition*, pg. 48

ownership.

Information Security Incident Management

No considerations specific to consumer health solutions were identified; however, all of the security requirements identified in **Section 4.10 - Information Security Incident Management** are applicable.

Business Continuity Management

No considerations specific to consumer health solutions were identified; however, all of the security requirements identified in **Section 4.11 Business Continuity Management** are applicable.

Compliance

No considerations specific to consumer health solutions were identified; however, all of the security requirements identified in **Section 4.12 Compliance** are applicable.

5.2.5 Point-of-Service Solutions

Traditional Point-of-Service (PoS) solutions are extremely wide-ranging and may include Electronic Medical Record systems and Hospital Information Systems, as well as health monitoring, departmental, chronic disease management and pharmacy systems. For the purpose of this topic, they are healthcare systems that interact with a clinician, collect or store PI/PHI and provide clinical or business functions.

While traditional PoS solutions have been available for decades, newer abilities of these systems to share information with each other and with regional solutions, and to integrate newer business functions provides opportunities for them to provide additional value. The new functions identified above all involve sharing information between the PoS and other systems.

There are many sources of information relating to point-of-service solutions in Canada. Two of these sources provide specific privacy and security guidance for PoS solutions:

- COACH – *Putting it into Practice: Health Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition.* Available from www.coachorg.com; and

- Canada Health Infoway – InfoCentral - https://infocentral.infoway-inforoute.ca/1_EMR_Programs

Rather than reiterating the guidance from those sources, this section will provide an overview of the newer business functions relating to point-of-service solutions and a synopsis of the guidance materials.

e-Referrals

The Canadian Medical Association (CMA) defines a referral as “a request from one physician to another to assume responsibility for the management of one or more of a patient’s specified problems. This may be for a specified period of time until the problem is resolved, or on an ongoing basis. It represents a temporary or partial transfer of care to another physician for a particular condition."[97]

Although most commonly thought of as being from physician to physician, referral patterns can more broadly be from any provider to any provider; from care setting to care setting, from provider to an organization (e.g. specialist group) and from a provider to a service (e.g. cancer care).

An e-Referral Management solution is one that supports standardized electronic referrals to enable activities such as:

- The provision of information to assist the requested provider to determine if they can meet the patient's needs;
- The booking and confirmation of the patient's appointment with the requested provider;
- The actual encounter between the patient and the consulting provider; and
- The consultation report back to the referring provider.

e-Referral deployment scenarios may include the provider-to-provider direct form, where the referrer's system (e.g., Cinical Information System or other non-clinical Point-of-Service system) generates and routes the referral form and associated information to the receiver's CIS (or other non-clinical PoS) system, where it is consumed and some type of patient scheduling workflow initiated. Another deployment scenario may have both sending and receiving PoS solutions use a set of regionally centralized services that may include a service registry (or extensions to an existing provider registry), a referral form repository, e-referral routing logic, or other services defined in the EHRi Blueprint.

PoS solutions with e-referral functionality may have varying degrees of integration with the information that is being sent and received. This can range from providing an e-referral viewer and a basic electronic document as a fillable form, with little ability for data validation and little or no integration with PoS clinical data, to a fully integrated e-referral solution, where forms and e-referral information are tightly integrated with the PoS data.

Referrals and consultation summaries are moved between provider PoS solutions by leveraging the existing interoperability infostructure including the business process orchestration capabilities of the HIAL, as shown in Figure 3 below.

Users of e-referral solutions need to be assured that in addition to normal clinical system privacy and security requirements, the following issues can be addressed:

1. The confidentiality and integrity of PHI communicated between sending and receiving systems is maintained while in transit;

[97] *MD Lounge*, September 2008, pg. 3 – Published by: Canadian Medical Association, The College of Family Physicians of Canada and The Royal College of Physicians and Surgeons of Canada

2. Patient identifiers that are used by the sending PoS system can be resolved to the same patient by the receiving PoS system;

3. Where possible, PoS systems federate identities and access-control roles with the systems interoperability infostructure;

4. PoS systems are able to mutually authenticate to the interoperability infostructure and services;

5. The authenticity of any clinical document transmitted as part of the referral or resulting consultation reports and PHI can be ascertained by the receiving system (or user thereof); and

6. The providers involved in exchanging information have mechanisms to ensure that their counterpart is the individual and/or organization that they are intending to communicate with.

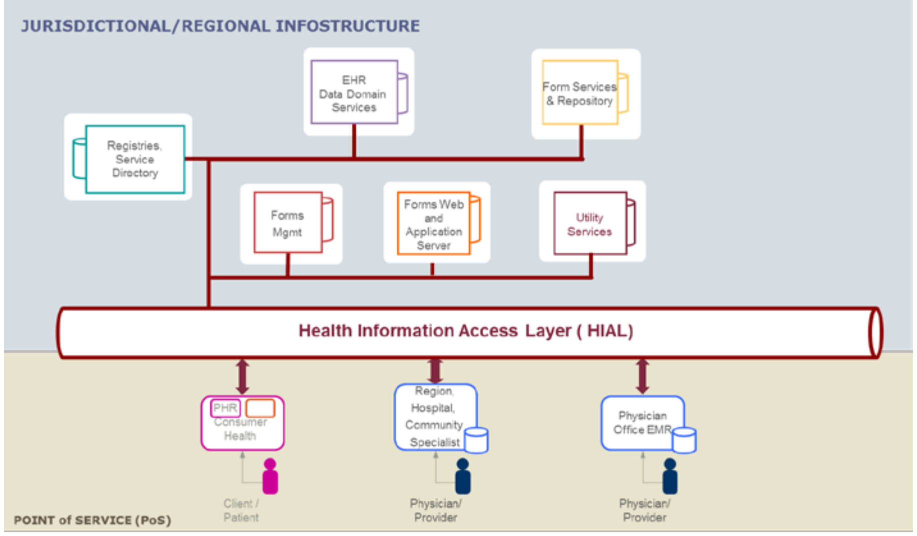

JURISDICTIONAL/REGIONAL INFOSTRUCTURE
EHR Data Domain Services
Form Services & Repository
Registries, Service Directory
Forms Mgmt
Forms Web and Application Server
Utility Services
Health Information Access Layer (HIAL)
PHR
Consumer Health
Region, Hospital, Community Specialist
Physician Office EMR
Client / Patient
Physician/ Provider
Physician/ Provider
POINT of SERVICE (PoS)

Figure 3. e-Referral PoS - EHR Infostructure

e-Prescribing

Health Canada defines e-prescribing as "a means of streamlining the prescription process by enabling prescriptions to be created, signed and transmitted electronically."[98]

[98] Health Canada – *Policy Statement on E-prescribing* - accessed 2013-03-05. *Link no longer available*. Please see: Saskatchewan College of Pharmacists – Electronic Transmission of Prescriptions Policy Statement and Guidelines for Pharmacists - https://scp.in1touch.org/uploaded/58/web/refmanual/Electronic-Transmission-of-Prescriptions-Policy-Statement-and-Guidelines-for-Pharmacists.pdf

Infoway has expanded upon this by defining e-prescribing as the secure, electronic creation and transmission of a prescription from an authorized prescriber, using pan-Canadian standard messages/ nomenclatures, through a jurisdictional Drug Information System (DIS), to be electronically accessible at the patient's pharmacy of choice.

e-Prescribing provides an opportunity for a number of quality and productivity benefits over traditional prescribing, including elimination of illegible handwriting, advanced clinical decision-support and reduced provider call-backs.[99]

From a deployment perspective, e-prescribing solutions include a prescriber portion (allows authorized providers to author, digitally sign and transmit an e-prescription), a pharmacy portion (able to receive or retrieve the e-prescription) and secure network routing components (ensuring that the e-prescription is delivered to the correct location and is not tampered with, duplicated or diverted). More complete solutions would include, for example: the management and tracking of prescriptions, a centralized patient profile or regional DIS integrated with e-prescribing functions contained within PoS solutions and utilizing centralized registries (e.g. patient, provider); privacy and security services; secure network routing logic; and data analysis and reporting capabilities.

In 2009, the Canadian Association of Chain Drug Stores released its *Recommendations for the Implementation of Electronic Prescriptions in Canada*, in which several principles for e-prescribing were identified. These are[100]:

1. The process must maintain patient confidentiality;
2. The process must be able to verify the authenticity of the prescription (i.e. the prescriber initiating the prescription);
3. The accuracy of the prescription must be able to be validated, and the process must include a mechanism to prevent forgeries;
4. The process must incorporate a mechanism to prevent diversion, so that the prescription authorization cannot be transmitted to more than one pharmacy;
5. Patient choice must be protected; that is, the patient must determine the practitioner to receive the prescription authority by having the prescription stored in a provincial DIS; and
6. Pharmacists must have the access and ability to write to the patient profile and other clinical decision-support tools.

[99] *National Impacts of Generation 2 Drug Information Systems*, Deloitte, Technical Report, September, 2010

[100] *Recommendations for the Implementation of Electronic Prescriptions in Canada* – Presented by Canadian Association of Chain Drug Stores (CACDS) and Canadian Pharmacists Association (CPhA) on behalf of the National e-Pharmacy Task Force – pg. 5

The National Association of Pharmacy Regulatory Authorities (NAPRA) has published a document that describes the minimum requirements for PoS pharmacy practice management systems (PPMS) used by pharmacists and pharmacy technicians in their delivery of quality care and services. The proposed requirements address technical, functional and administrative requirements of PPMS and include e-prescribing[101].

5.2.5.6 Considerations

The privacy and security requirements from Sections 3 and 4 have applicability to PoS solutions that interact with components of EHRs as identified in **Appendix A -**. Organizations should consider all of the requirements in Sections 3 and 4 that are applicable to PoS systems connecting to an EHR whenever they are consider connecting a PoS system to any other clinical system. They are especially encouraged to do so when the other clinical system is controlled by another organization.

As mentioned previously, the two major sources for privacy and security guidance for point-of-service solutions in Canada are the COACH material[102] and *Infoway's* InfoCentral[103]

5.2.5.7 COACH PoS Considerations

COACH's *Putting it into Practice* material is intended to act as a supplement to the COACH *Guidelines for the Protection of Health Information*[104] and is focused on providing guidance to community healthcare providers to allow them to make "*better and more informed decisions on how to implement privacy and security best practices in the office setting when using electronic record systems as the collect, use, access, share and store personal health information.*"[105]

The COACH material is a primer that can be used by any organization that is establishing its first point-of-service system, as well as by those organizations that are expanding their practice to include communication with external parties. The material is presented as a series of short reference fact sheets that provide: a high-level overview of a particular topic; usually a short section on best practices for that topic; and a recommendation on how to plan and implement a topic within the reader's organization.

The introductory material covers topics at a high level, including: privacy best practices; privacy and security policies; legislation in Canada; fair information principles as set out in the CSA Model Code for the Protection of Personal Information[106]; information sharing; and risk-management practices.

[101] Pharmacy Practice Management Systems: Requirements to Support NAPRA's "Model Standards of Practice for Canadian Pharmacists", National Association of Pharmacy Regulatory Authorities (2013). Available at: http://napra.ca/pages/Practice_Resources/ppms.aspx

[102] *Putting it into Practice: Health Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* – COACH - http://www.coachorg.com

[103] Canada Health Infoway EMR wiki - https://infocentral.infoway-inforoute.ca/1_EMR_Programs

[104] The *Guidelines* from 2011 is the most current version as of this writing

[105] COACH – *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records* – pg. 6

[106] http://www.csa.ca/cm/ca/en/privacy-code - accessed 2013-03-15

The second section deals with selecting an electronic record solution and discusses: information-sharing agreements; deployment model considerations; and privacy and security conformance standards.

Section 3 of the COACH document is focused on the initial establishment of an operational Electronic Record System (ERS) and discusses: access control; audit logging and reporting; staff training; staff confidentiality agreements; recording patient consent; masking; patient education; physical safeguards; technical safeguards; IT and network operations strategies; and data conversion.

Next, the document deals with issues likely to emerge during ongoing operation of the ERS. Topics discussed at a high level include: establishment and operation of an audit program; ongoing system maintenance; data retention; and ongoing user account management.

The penultimate chapter deals with potential problems that an organization may encounter during operation of an ERS and provides approaches to developing solutions for those problems. Problem areas include: privacy breach management; third-party agreements for information sharing; privacy complaints; service provider support; and patient access and correction.

Finally, *Putting it into Practice* provides general guidance for other selected topics that may be applicable to healthcare organizations. Topics covered include: staff and family record protection; release of information; e-prescribing; authority to collect PHI; e-mail; consumer health solutions; wireless devices and networks; faxing; secondary use of PHI; and practice closure.

5.2.5.8 Infoway EMR Privacy and Security Requirements

The *Infoway* InfoCentral (https://infocentral.infoway-inforoute.ca/1_EMR_Programs) provides detailed requirements that are intended to be used in combination with the privacy and security requirements contained in Sections 3 and 4 of this document for point-of-service (specifically EMR) solutions.

Infoway created a baseline EMR specification that contains privacy and security requirements. Many jurisdictions have created their own EMR specifications that are based on, or are aligned with, the *Infoway* specification. Organizations should use the specification appropriate to their needs.

Interested stakeholders are encouraged to access InfoCentral directly for the most recent version of the specifications. These specifications should be considered when developing, maintaining or deploying any PoS solution.

The specifications contain the business, functional and technical requirements of the *Infoway* EMR Program that extend the privacy and security requirements from Sections 3 and 4 of this document. They contain the following privacy and security related categories:

- Access Control;
- Audit Logging;
- User and Node Authentication;

- Digital Signatures;
- Encryption;
- General Security;
- Identity Management;
- Integrity and Authenticity of Prescriptions; and
- Other Privacy and Security Service Requirements.

5.3 Emerging Technology Topics

5.3.1 Cloud Computing

Cloud computing is quickly becoming a viable option for many organizations in a wide variety of industries. The public cloud computing marketplace was estimated by industry analyst firm Gartner to be $89 billion in 2011, with a compound annual growth rate of 19%. Forrester Research estimated that the public cloud computing market would be $249 billion by the year 2020.

5.3.1.1 Definitions

Wikipedia defines cloud computing as "the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet)"[107]; however, for the purposes of this document, the definition of cloud computing that has been identified by the U.S. Department of Commerce National Institute of Standards and Technology (NIST)[108] will be used:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g.*
>
> *networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

A cloud service is characterized, from NIST's perspective, by:

- *On-Demand, Self-Service*[109] facilities that allow consumers to provision, maintain and decommission services without any human intervention from the cloud provider;
- *Broad Network Access* that provides for standard mechanisms, generally some kind of Application Programming Interface (API), for consumers to access cloud services over the network;

[107] http://en.wikipedia.org/wiki/Cloud_computing, accessed 2013-02-04

[108] *"The NIST Definition of Cloud Computing",* NIST Special Publication 800-145, September, 2011

[109] Virtualization technologies, while common to many cloud offerings as a means of achieving some of the characteristics of a cloud computing infrastructure, are not specifically required nor addressed within this topic.

- *Resource Pooling* that allows the cloud provider to dynamically reconfigure resources to match consumer demand. This characteristic contributes to the sense of location-independence since the consumer cannot determine where, physically or virtually, the resources they are consuming are located;

- *Rapid Elasticity* that allows the consumer to expand or contract the capacity of the provisioned services quickly to match demand; and

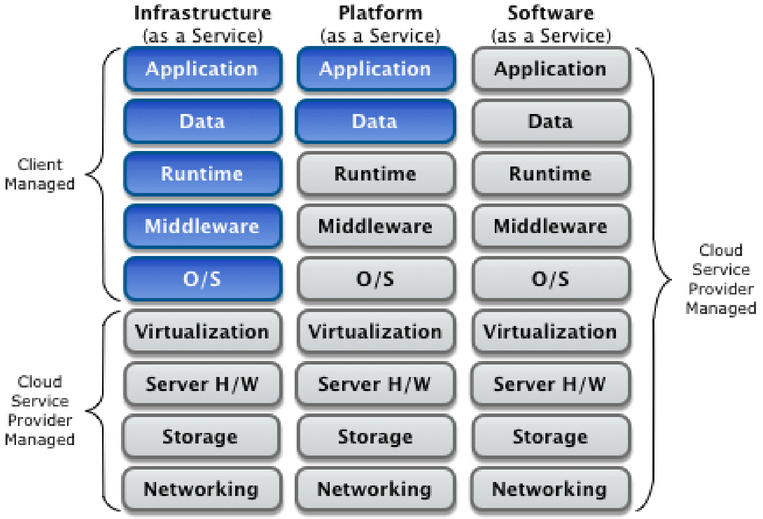
- *Measured Service* that allows the cloud provider to monitor, measure and report on service utilization and consumption.

Further characterization depends on two factors: what services are being offered (the service model); and how those services are delivered (the deployment model).

Service Models

The following diagram illustrates the three cloud computing service models in terms of three identical computing 'stacks'. Each stack has a foundation consisting of basic networking, storage and server hardware, the addition of operating systems, middleware and runtime components, such as databases or Web application services, and finally, the application (or service) and information that a user interacts with at the top. The difference between these stacks is based on which organization is responsible for providing and managing each component of the stack.[110]

The Infrastructure-as-a-Service (IaaS) model provides a client organization with a set of raw computing resources (physical or virtual processors, disk storage and networking capabilities) that are controlled by the Cloud Service Provider (CSP). The client organization is responsible for, and has control over, the operating system and every component above it in the stack. Examples of commercial IaaS offerings include Q9 Networks, OnX, Amazon Web Services (AWS), IBM SmartCloud Enterprise, Rackspace Cloud and Joyent Cloud, among many others.



Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Application	Application	Application
Data	Data	Data
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Server H/W	Server H/W	Server H/W
Storage	Storage	Storage
Networking	Networking	Networking

Client Managed
Cloud Service Provider Managed
Cloud Service Provider Managed

(derived from: CIO Research Center)

Figure 4. Cloud Service Models

The Platform-as-a-Service (PaaS) model shifts the costs of providing and managing the operating system, middleware and runtime components from the client to the CSP, while the CSP maintains responsibility for all the components listed for the IaaS service model. PaaS models usually provide

[110] Please refer to The Infoway ETG Cloud Computing in Health White Paper for a more complete discussion of cloud computing in the Canadian health care space.

a specific environment for the deployment of client applications. The particulars vary by offering, where some CSPs offer 'delivery-only' solutions (where the client deploys its application ready for production use), while others include full development, debugging and test facilities. Examples of PaaS solutions include Google App Engine, Windows Azure, IBM SmartCloud Application Services and the Oracle Cloud Platform.

In the Software-as-a-Service (SaaS) model, the CSP provides and manages all aspects of the solution stack, including the application and data. Examples of SaaS offerings include Google's Gmail, Salesforce.com and Microsoft Office 365. In addition, many U.S.-based Clinical Information System vendors provide SaaS-based offerings.[111]

Readers are encouraged to refer to The *Infoway* Cloud Computing in Health White Paper for a more complete discussion of cloud computing in the Canadian healthcare space.

From a service model perspective, the cloud client generally has less control over security and privacy issues using the SaaS service model and more control using the IaaS service model, with the PaaS model falling somewhere in between. As Figure 4 indicates, IaaS models have the client managing the majority of the identified components, and thus the privacy and security aspects of those components, while SaaS models have the CSP managing all of the components. In the SaaS model, some of the supporting privacy and security services are, or could be, functionality of the software provided by the CSP. Examples of these services might be patient consent or authorization mechanisms (e.g. role-based or attribute-based access control) for access to PHI.

Deployment Models

An organization's chosen cloud deployment option has a significant impact on the privacy and security considerations that should be taken into account during planning, implementation and ongoing operations.

Each of the cloud computing service models can be deployed in any of the four ways described below:

Private Cloud Deployment

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units). It may be owned, managed and operated by the organization, a third party or some combination of both, and it may reside on or off premises.

The emphasis here is that one organization governs and controls the use of the Cloud for its own purposes. Accountability, implementation, operation and use of the Cloud is the responsibility of that organization alone.

An example of a Private Cloud might be the conversion of all the computing infrastructure (services, network and CPU) for a hospital to an IaaS solution.

[111] KLAS Research – "Software as a Service EMR Model Garners Greater Appeal" - http://www.klasresearch.com/News/PressRoom/2012/SaaS - accessed 2012-12-21.

Community Cloud Deployment

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy and/or compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of both, and it may reside on or off premises.

The scope of this implementation model is typically defined by the user/customer base of the community of organizations served. The services provided are typically focused on the shared 'business' of that community.

An example of a Community Cloud might be the implementation of a common e-referral and/or e-scheduling service for a regional health authority or an entire province/territory.

Public Cloud Deployment

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organization, or some combination thereof. It resides on the premises of the cloud provider.

This implementation model is well suited for generalized capabilities that are not specific to any one sector, community of users or organization.

Examples of applications that might benefit from a Public Cloud implementation might be the use of clinical decision-support solutions such as IBM's Watson, e-mail or office applications, or the supply of general computing infrastructure for application development and/or testing purposes.

Hybrid Cloud Deployment

The Hybrid Cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

The Hybrid implementation model is most often found in environments where the services provided have varying privacy, governance and deployability requirements. In a Hybrid model, an organization may have some aspects of its technology deployed in a Private model, other aspects of its business needs met by participating in one or more Community models and the most generic of its needs met by use of Public Cloud services. An example of a Hybrid Cloud is one where an organization has implemented a Private Cloud for its mission-critical applications, but also participates in a Community Cloud for collaboration with business partners and has chosen to consume generic office services from a Public Cloud.

Another example might be the integration of two Community Cloud service implementations to meet the needs of a regional health authority to provide a community service (such as e-referral) that utilizes Federated Identity Management services provided by a Community Cloud run by a provincial e-health interoperability infostructure organization.

Cloud Strengths and Opportunities in Healthcare

Some of the stated advantages of cloud computing include:

- Lower cost – because resources are owned and managed by the cloud service provider (CSP), the cloud client only pays for the services allocated to it[112];

- Increased flexibility – since resources are elastic, sudden increases or decreases in computing resource requirements can be satisfied quickly;

- Location independence – cloud services are available using standard mechanisms that are not location-dependent, resulting in an ability to consume those services from any connected location and have the services hosted at any location;

- Device independence – the set of standard mechanisms for accessing cloud services generally requires only that the device consuming those services be compliant with those mechanisms, generally some kind of API or other standardized interface such as Web browsers. The same cloud services can be consumed by any client device that is capable of invoking the mechanism, allowing PCs, tablets, smartphones and other non-traditional devices access to cloud resources; and

- Increased availability – because components used in the cloud deployment are generally standardized and can be 'swapped out' easily, usually with little or no downtime.

Whether these advantages can be realized by healthcare cloud clients in Canada is dependent upon many factors, including: the end use of the cloud service; the deployment model selected; and the terms and conditions of service that are agreed to between the CSP and cloud client.

Cloud computing can be leveraged by health care organizations for many purposes, including, but not limited to: provisioning on-demand application development and testing facilities; secure organizational e-mail capabilities; providing Clinical Information System (CIS) functionality; e-referrals; and e-booking. For a more complete discussion of potential opportunities for cloud computing in health care, please refer to The *Infoway* Cloud Computing in Health White Paper.

5.3.1.2 Issues

Organizations considering the use of cloud services may have to deal with a number of issues that do not exist in traditional computing environments. Some of these issues arise from the technology itself, while others may be based on the relationship that the consuming organization has with the cloud provider, and

[112] While a 'stated advantage', use of cloud strategies may not always be true in private and community deployment models where the resources may well be capitalized by the entity using it.

still others are based on a specific deployment model. The use of cloud computing resources raises issues in the following areas:

- Privacy and Security Governance and Control;
- Agreements;
- Multi-tenancy;
- Due Diligence;
- Physical Location (data storage and processing); and
- Confidentiality

Privacy and Security Governance and Control

Use of cloud services can push the externalization of identifiers, security infrastructure and privacy and security processes and services outside of the organization, leading to a potential loss of control of the security perimeter. Many privacy and security controls can be rendered opaque by this externalization, resulting in a challenge to privacy and security governance in the Cloud.

Information custodians have an obligation to monitor and audit access to PHI in order to satisfy patient/person access requests and to monitor for potential breaches. Cloud offerings that remove the ability for cloud clients to perform monitor and audit functions expose custodians and information managers to additional business risk unless those functions can be effectively managed in accordance with a custodian's obligations.

Agreements

Agreements that bind a CSP, especially one that operates a Public Cloud service offering, may be more difficult to tailor to the specific needs of health care organizations in Canada. Depending on the CSP's implementation details, some of the strengths of the cloud paradigm may actually result in privacy or security risks that cannot be mitigated in a cost-effective manner by either party. For example, while location-independence is considered a strength and fundamental characteristic of a cloud environment, a cloud provider that has datacentres in multiple countries may not be able to guarantee that PHI will remain within the jurisdiction in which it was collected. The transferred information can then additionally be subject to the laws of the jurisdiction where it resides. In some jurisdictions, or in some situations, this may require the express consent of the individual whose PHI is being considered in order for it to be transmitted to or stored in the cloud service.

As information is moved into the Cloud, the increased risk of data loss, accuracy and reliability must be assessed and any additional risk mitigated, either by transferring the risk to the CSP via agreement or by additional controls that the data custodian can put in place.

Agreements for cloud services that involve PHI will need to address issues that include:

- Data ownership, including an exit strategy that addresses data capture, migration, persistence and destruction;
- A CSP's use of a client organization's data;
- Notification, where not prohibited, of a legal request for client organization information;
- Ensuring access log records are created, protected and are accessible by the client organization;
- CSP liability for privacy and/or security breaches;
- CSP indemnification responsibilities;
- Roles and responsibilities of CSPs, any third parties and the client organization with respect to privacy and security incident management; and
- Hardware and software change management processes.

Multi-tenancy

The resource pooling characteristic of a cloud service implies that every cloud implementation supports multi-tenancy in some form or other.

The nature of a cloud client's co-tenants is dependent on the deployment model that is being adopted. Cloud clients that choose Private Cloud deployments have few, if any, additional concerns with respect to multi-tenancy compared to what they would with traditional hosted computing models.

A Community Cloud deployment generally involves co-tenant organizations with similar goals and privacy and security requirements. However, there is a still an increased risk of unauthorized disclosure that each organization should be aware of.

Public Cloud service offerings have been criticized for a lack of rigour in the identification and verification of their customer's identity. At least initially, only a valid credit card is necessary to establish services with a large number of Public Cloud service providers. If a Public Cloud model is used by an HDO, this lack of rigour increases the risk that another service consumer may be attempting to use the service to attack legitimate cloud clients.

The greater challenge in the case of PHI stored in a Public Cloud deployment is based on the potential for misalignment of privacy and security requirements between cloud clients. This can result in a risk that the controls in place to ensure the security and privacy of information for the majority of industries are not adequate to protect PHI in the health care industry, and that simply adding clauses in service level agreements to close those gaps may not be sufficient.

Due Diligence

In choosing appropriate service and deployment models, and the particular service provider, organizations should go through a due diligence process just as they would for the evaluation of any new technology or service provider. The level and type of due diligence activities may vary based on the cloud deployment model being considered and/or the data and application classifications (a minimal process may be required for the use of a Private Cloud). While due diligence is not a cloud-specific issue, there are many cloud-specific considerations that should be taken into account when performing an evaluation of this type.

Location

The location-independence benefit of cloud computing can also be an issue. Location-independence means that PHI could be stored, processed in and subject to the laws of a different jurisdiction than those of the jurisdiction in which the PHI was collected.

Confidentiality

In moving from a single-tenant environment to a multi-tenant one, the issue of confidentiality becomes critical. Historically, organizations have maintained the confidentiality of PHI in transit by using encryption technologies, while leveraging administrative controls to protect PHI that is at rest. In a multi-tenant environment, this approach may not be effective, especially in a Public Cloud deployment.

The concept of resource pooling, a core characteristic of cloud computing, implies that resources that contained PHI may be released into the general resource pool for reuse by other tenants when no longer required by the original tenant. Without adequate controls on either the way that PHI is managed on the resource or the mechanism to securely remove PHI from the resource prior to its return to the resource pool, the risk of unauthorized access to that PHI is higher than with a traditional single-tenant, non-pooled environment.

5.3.1.3 Cloud Lifecycle

The introduction of any new technology will go through stages that include planning, acquisition, operation and decommissioning. The exact stages, and details of each stage, are normally determined by each organization, and a more fulsome discussion of the methodologies is out of scope for this document. Regardless of the methodology used, some of the considerations identified in the following sections are more appropriate for a specific phase of an organization’s interactions with cloud computing.

5.3.1.4 Planning

In the planning or initiation phase, the organization is generally identifying its requirements and performing some type of benefits assessment.

In this phase, considerations should be reviewed that help an organization to:

- Focus on whether privacy and security policy updates are necessary in order to support operating within the cloud context;

- Identify privacy and security requirements that will be appropriate for a cloud computing environment; and
- Map the types of applications and data that the organization holds into appropriate cloud service and deployment models.

Considerations most appropriate for this phase are:

- CC-SE1 – Establish cloud client risk tolerance;
- CC-SE3 – Determine client privacy and security requirements;
- CC-SE34 – Classify resources as 'cloud-appropriate';
- CC-SE6 – Select appropriate deployment/service models;
- CC-SE8 – Plan for cloud service termination;
- CC-SE36 – Use data classifications to inform cloud decisions;
- CC-PR1 – Asses compliance impact;
- CC-SE35 – Establish policies regarding location of processing and storage of information.

5.3.1.4.1. *Acquisition*

Once a decision has been made to leverage cloud computing technologies, an organization will most likely perform some type of 'buy vs. build' analysis and a due-diligence exercise on the candidate solutions and providers, including an initial risk assessment. The result of those analyses will be the identification of an internal or external CSP with which to negotiate a service agreement. Considerations relating to the service agreement are included in this phase.

A large number of considerations are appropriate for this phase of activity. They are:

- CC-PR2 – Ensure appropriate CSP PIA and TRA handling;
- CC-SE11 – Identify a client-specific security perimeter;
- CC-SE12 – Evaluate Service Level Agreements with respect to compliance;
- CC-SE44 – Leverage CSP monitoring mechanisms;
- CC-SE13 – Evaluate Cloud Service Provider (CSP) privacy and security requirements;
- CC-SE14 – Ensure appropriate limitations on liability;
- CC-SE15 – Assess CSP third-party relationships;

- CC-SE16 – Assess CSP risk management approach;
- CC-SE17 – Assess CSP privacy and security governance, structure and processes;
- CC-SE18 – Ensure appropriate privacy and security accountability within the CSP organization;
- CC-SE19 – Include incident response processes in Service Level Agreements;
- CC-SE20 – Perform cloud solution assessment;
- CC-SE21 – Assess Cloud Service Provider;
- CC-SE22 – Evaluate certifications and audit statements;
- CC-SE23 – Evaluate CSP authentication level of assurance;
- CC-SE24 – Evaluate CSP authentication and authorization capabilities;
- CC-SE25 – Engage appropriate cloud client areas during SLA negotiations;
- CC-SE26 – Evaluate CSP risk management documents;
- CC-SE27 – Evaluate CSP business continuity planning;
- CC-SE28 - Evaluate CSP event and incident management processes and data;
- CC-SE59 – Control processing and storage locations;
- CC-SE54 – Design cloud applications for multi-tenancy;
- CC-SE4 – Assess appropriate use of virtualization technologies;
- CC-SE7 – Reduce multi-tenancy threats;
- CC-SE10 – Evaluate security policy differences;
- CC-SE29 – Evaluate SaaS application partitioning;
- CC-SE49 – Evaluate PaaS security interoperability;
- CC-SE30 – Evaluate IaaS co-tenant risks;
- CC-SE31 – Conduct an on-site visit;
- CC-SE32 - Assess CSP availability goals;
- CC-SE33 – Assess critical CSP operating and service management processes;

- CC-SE40 – Implement collaborative governance structures and processes;
- CC-SE43 – Plan for data migration;
- CC-SE47 – Evaluate CSP-provided security policy management capabilities;
- CC-SE48 – Evaluate CSP-provided security policy management and maintenance tools;
- CC-SE52 – Use multi-tenant-aware PaaS application development frameworks;
- CC-SE53 – Assess SaaS applications support for privacy and security; and
- CC-SE58 – Mitigate risk of CSP business failure.

5.3.1.4.1. Deployment

At this point in the cloud computing lifecycle, a CSP has been identified and service agreements have been finalized. This phase involves creating and executing a migration and/or deployment plan and performing ongoing day-to-day operations.

Considerations appropriate for this phase are:

- CC-SE44 – Leverage CSP monitoring mechanisms;
- CC-SE5 – Use cloud-specific controls;
- CC-SE9 – Protect cloud-client devices and systems
- CC-SE56 – Prevent data leakage in hybrid deployment models;
- CC-SE45 – Monitor cloud activities;
- CC-SE55 – Manage cryptographic keys;
- CC-SE42 – Ensure secure deletion of data
- CC-SE4 – Assess appropriate use of virtualisation technologies;
- CC-SE50 – Use mutually authenticated communications channels;
- CC-SE51 – Restrict administrative access to cloud resources;
- CC-SE37 – Separate data with differing sensitivities;
- CC-SE38 – Ensure cloud client and CSP segregation of duties;
- CC-SE41 – Encrypt PHI at rest;

- CC-SE60 – Evaluate the use of dedicated Identity Management services;
- CC-SE61 – Assess the use of a Federated Identity Management (FIdM) scheme;
- CC-SE62 – Use standards-based authentication mechanisms;
- CC-SE46 – Consolidate access logs;
- CC-SE58 – Mitigate risk of CSP business failure;
- CC-SE39 – Create or update operating procedures; and
- CC-SE57 – Request use of content discovery tools.

5.3.1.4.2. *Termination*

This phase of the cloud computing lifecycle is concerned with the cessation of operations supported by a particular CSP. The operation may no longer be needed by the cloud client organization or may be migrated to a new CSP.

Considerations appropriate for this phase are:

- CC-SE43 – Plan for data migration; and
- CC-SE42 – Ensure secure deletion of data.

5.3.1.5 *Introduction to Cloud Considerations*

Having discussed some of the issues that cloud computing raises in the Canadian health care context, we present privacy and security considerations that organizations may want to take into account when planning for, procuring and implementing a cloud-based solution. The considerations are meant to assist the reader in identifying and mitigating those previously discussed issues and are organized into separate privacy and security areas, similar to how the EHRS privacy and security requirements have been organized.

Cloud computing is a very broad topic with many dimensions. As a result, some considerations are more applicable to certain deployment and/or service models than others.

As an example, a consideration that suggests that organizations consider encryption for data at rest is more applicable to IaaS and PaaS service models. The rationale is that SaaS models normally do not allow an organization to make that choice, unless designed to offer this capability. This consideration is very applicable to Public Cloud deployments and somewhat applicable to Community deployments, while Private Cloud deployments may have more cost-effective mechanisms to provide an equivalent or better level of protection for the data.

Applicability does not include risk, since risk can only be assessed based on the particular application of the cloud service and the set of controls established by the organization.

In the considerations that follow, a simple Applicability Matrix, as illustrated by Figure 5, is included for each consideration. The matrix is intended to guide the reader in assessing the relevance of a particular consideration to the service/deployment model combination that they may be considering. The Applicability Matrix uses a legend of H(High), M(Medium) and L(Low) to indicate the relative applicability of the consideration to a specific service/deployment model.

Applicability

	Public	Community	Private
IaaS	L	M	H
PaaS	L	M	H
SaaS	L	M	H

Figure 5. Consideration Applicability Matrix

5.3.1.6 Privacy Considerations

This section deals with privacy considerations that are specific to a cloud computing environment. There are some areas where there are no cloud-specific considerations. The reader should understand that whether considerations have been identified or not, all of the requirements identified in **Section 3 Privacy Requirements** still apply.

5.3.1.7 Accountability

Many of the considerations identified are related to accountability, but are primarily concerned with security controls that provide sufficient operational oversight that ensures Data Custodian responsibilities and obligations are met. Those considerations are identified in **Section 5.3.1.12 Security Considerations** below.

Consideration CC-PR1 – Assess compliance impact[113]

Consideration should be given to determining how existing compliance requirements will be impacted by the use of cloud services for each workload (i.e. set of applications and data), in particular as they relate to privacy legislation and policy, as well as information security requirements and regulations.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Admin Consideration

[113] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 48

Rationale: As with any outsourced solution, organizations need to understand how the solution may impact the organization's compliance with legislation, regulations and policy.

Consideration CC-PR2 – Ensure Appropriate CSP PIA and TRA Handling[114]

Cloud clients should ensure that Privacy Impact Assessments (PIAs) and Threat Risk Assessments (TRAs) are performed and risk managed appropriately by both the CSP and the client as part of a larger risk management framework, where warranted.

Applicability

	Public	Community	Private
IaaS	L	H	H
PaaS	L	H	H
SaaS	L	H	H

Admin Consideration

Rationale: This consideration serves to highlight the alignment of risk management processes, where possible and appropriate between the cloud client and the CSP. An alignment effort allows a cloud client to identify gaps that can be closed by adjustments to the framework, agreements, processes, procedures or technical controls. See **CC-SE26 - Evaluate CSP risk management documents.**

5.3.1.8 Identifying Purposes

No cloud-specific considerations were identified; however, all of the privacy requirements identified in **Section 3.2 – Identifying Purposes for Collection, Use and Disclosure of Personal Health Information** still apply. Please refer to that section for privacy requirements as they may apply to cloud computing.

5.3.1.9 Consent

No cloud-specific considerations were identified; however, all of the privacy requirements identified in **Section 3.3 – Consent** still apply. Please refer to that section for privacy requirements as they may apply to cloud computing.

[114] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 126

5.3.1.10 Limiting Collection

No cloud-specific considerations were identified; however, all of the privacy requirements identified in Section 3.4 – Limiting Collection of Personal Health Information still apply. Please refer to that section for privacy requirements as they may apply to cloud computing.

5.3.1.11 Limiting Use, Disclosure and Retention

No cloud-specific considerations were identified; however, all of the privacy requirements identified in Section 3.5 – Limiting Use, Disclosure and Retention of Personal Health Information still apply. Please refer to that section for privacy requirements as they may apply to cloud computing.

5.3.1.11.1. Accuracy

No cloud-specific considerations were identified; however, all of the privacy requirements identified in Section 3.6 – Accuracy of Personal Health Information still apply. Please refer to that section for privacy requirements as they may apply to cloud computing.

5.3.1.11.2. Safeguards

Consideration CC-PR3 – Use Privacy-Enhanced Identifiers[115]

Cloud clients should consider the use of enterprise client identifiers (eCIDs) as defined in the *Infoway* Blueprint, where health information has identifiers replaced with eCIDs prior to being placed in a Public or Community Cloud. The eCID concept is sometimes referred to as "tokenization". The client maintains a reference that maps the eCID to identifiers only in their private cloud or facility.[116]

As described in the *Infoway* Blueprint, the eCID is used "above the HIAL" and never disclosed publicly. As a result, the privacy-enhanced identifiers used in the Cloud should not be the same identifiers as used above the HIAL in mixed or hybrid deployment scenarios.

PbD Feature

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Tech Consideration

Rationale: Replacing identifiers with tokens effectively de-identifies any information stored in the Cloud. As with any de-identification

[115] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §6.3.2

[116] Cloud Security Alliance – *Security Guidance for Critical Areas of Focus in Cloud Computing, V3.0*, pg. 130

scheme, however, care must be taken to ensure that re-identification is not easily performed without the token-to-identifier map. See **Security Requirement 75 – Uniquely Identifying Patients/Persons**.

This consideration supports the Privacy by Design[117] principles of Privacy Embedded into Design, and is proactive, not reactive. Replacing key personal identifiers with tokens is a proactive measure to reduce the likelihood that unauthorized access to that information will reveal personal information.

While this consideration is applicable to all deployment and service models, it provides additional value in Public and Community deployment settings.

Many of the considerations identified are related to safeguards but are primarily concerned with security controls. They are described in Section 5.3.1.12 - **Security Considerations** below.

5.3.1.11.3. *Openness*

No cloud-specific considerations were identified; however, all of the privacy requirements identified in **Section 3.8 – Openness about Practices Concerning the Management of Personal Health Information** still apply. Please refer to that section for privacy requirements as they may apply to cloud computing.

5.3.1.11.4. *Individual Access*

No cloud-specific considerations were identified; however, all of the privacy requirements identified in **Section 3.9 – Individual Access to Personal Health Information** still apply. Please refer to that section for privacy requirements as they may apply to cloud computing.

5.3.1.11.5. *Challenging Compliance*

No cloud-specific considerations were identified; however, all of the privacy requirements identified in **Section 3.10 – Challenging Compliance** still apply. Please refer to that section for privacy requirements as they may apply to cloud computing.

5.3.1.12 *Security Considerations*

This section is organized in a similar manner to the Security Requirements section, which is based on the ISO 27002:2005 security control objectives.

[117] See http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/ s.

5.3.1.13 Risk Management

This section contains a great many considerations for cloud computing. The intent is to address cloud-specific concerns in respect of the assessment and treatment of risks. There are some considerations that overlap other security and/or privacy areas and are referenced in those sections.

5.3.1.13.1.1. Assessing Security Risks

Consideration CC-SE1 – Establish Cloud Client Risk Tolerance[118]

Admin Consideration

Cloud clients should consider whether their own management has defined risk tolerances with respect to cloud services and accepted any residual risk associated with using cloud services.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: Organizations that have not identified their risk tolerances will have a difficult time determining whether additional risks associated with a particular cloud service or deployment scenario have been mitigated appropriately.

Section 5.1 of *ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems –* Requirements and Section 7.1 of *ISO/IEC 27005:2005 – Information technology – Security techniques – Information security risk management* both discuss the need for an organization to establish a risk-management program and identify its risk-tolerance profile as part of that exercise.

This consideration is applicable to all cloud deployment and service models.

[118] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 33.

Consideration CC-SE2 – Assess Data Confidentiality Controls[119]

Admin Consideration

Cloud clients should consider what minimum controls are required to prevent, where necessary, breaches and unintended use of information as a result of an aggregation or consolidation of information that might be available from multiple tenants. Where possible, cloud clients should retain control over access to their information. It should not be possible for other tenants of a CSP to have access to their data. Various control mechanisms, such as virtualization of cloud client data storage, should be considered.

This includes specifying contractual limits on aggregation or consolidation of information and limiting purposes for which data can be used, as well as establishing processes, roles and responsibilities for breach monitoring and notification.

Applicability

	Public	Community	Private
IaaS	H	M	L
PaaS	H	M	L
SaaS	H	M	L

Rationale: In the Public or Community Cloud context, there is a higher probability that data aggregation or consolidation can occur. An example of this might be a cloud-based mail service that is used by hundreds or thousands of organizations. The value of this consolidated e-mail-related information is far greater than that contributed by an individual organization and care should be taken to limit uses of that information appropriately.

The overall impact associated with a breach increases as the breadth and volume of data increases.

This consideration is consistent with the Privacy by Design[120] principle of privacy embedded into design and applies to the design of policies and procedures as well as to the technical solution.

[119] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §6.3.2

[120] See http://www.privacybydesign.ca

Consideration CC-SE3 – Determine Client Privacy and Security Requirements[121]

Admin Consideration

Cloud clients should clearly articulate their privacy and IT security requirements prior to choosing to use cloud computing, a particular cloud computing deployment model or a CSP.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: Clearly identifying privacy and information security requirements allows the prospective cloud client to perform a comparative analysis to identify any requirement gaps in the combination of services, deployment models and provider capabilities. Requirements should address areas such as loss and availability of data, infrastructure, platforms and services.

Using tools such as the *Cloud Security Alliance's Consensus Assessments Initiative Questionnaire* or the *Information Assurance Framework recommended by ENISA's Cloud Computing Security Risk Assessment, November 2009* can assist a cloud client in establishing cloud-specific privacy and security requirements.

Consideration CC-SE4 – Assess Appropriate Use of Virtualization Technologies[122]

Tech Consideration

Where appropriate, organizations should consider supporting virtualization technologies[123] as a significant part of their cloud infrastructure.

Applicability

	Public	Community	Private
IaaS	L	H	H
PaaS	L	H	H
SaaS	L	H	H

[121] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §6.3.3

[122] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §6.3.6

[123] Virtualization is the creation of a virtual, rather than physical, version of something, such as a hardward platform, storage device or network resource. The usual goal of virtualization is to centralize administration of the computing environment, while improving scalability and overall physical resource utilization.

Rationale: Applying virtualization technologies in a cloud environment is a fairly standard practice that allows multiple tenants to share physical resources, while maintaining a reasonable amount of control over access and use of their information. The security perimeter becomes defined by the virtual resources rather than physical ones and allows some additional perimeter controls to be put in place.

5.3.1.13.1.1. Treating Security Risks

Consideration CC-SE5 – Use Cloud-Specific Controls[124]

Cloud clients should consider leveraging the list of cloud-specific controls identified by organizations such as the Cloud Security Alliance and the European Network and Information Security Agency to help ensure that cloud-appropriate safeguards are in place where necessary.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Admin Consideratio

Rationale: Using an industry-specific list of controls as a starting point to mitigate identified risks allows cloud clients to have reasonable assurance that the most appropriate mitigation options are being considered. The Cloud Security Alliance has produced a *Cloud Control Matrix*[125] that contains a list of cloud-appropriate controls and relates those controls to their architectural relevance and *ISO/IEC 27002:2005* clauses.

This consideration is equally applicable to all cloud deployment and service models.

Consideration CC-SE6 – Select Appropriate Deployment/Service Models only where Monitoring Capabilities Exist[126]

Admin Consideratio

[124] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §*6.3.2*

[125] Cloud Security Alliance - *Cloud Control Matrix* Version 3 (https://cloudsecurityalliance.org/research/ccm/)

[126] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §*6.3.4*

Consideration should be given to determining the appropriate use of a cloud deployment and/or service model where auditing and monitoring are not available to cloud clients, such as in Public Clouds. This is one of the key pieces of any privacy or security assurance framework and a key custodial responsibility.

Applicability

	Public	Community	Private
IaaS	H	H	M
PaaS	H	H	M
SaaS	H	H	M

Rationale: Cloud offerings that render auditing and monitoring mechanism opaque to cloud clients (i.e., logs not accessible or not created) may expose Data Custodians and Information Managers to additional business risk if they cannot detect potential breaches and monitor appropriate access to PHI.

This consideration is equally applicable to all cloud service and deployment models.

Consideration CC-SE7 – Reduce Multi-Tenancy Threats[127]

Admin Consideratio

For processing sensitive information, organizations should consider Private or Community Clouds in order to restrict the set of co-tenants.

Applicability

	Public	Community	Private
IaaS	H	M	L
PaaS	H	M	L
SaaS	H	M	L

Rationale: Both Private and Community scenarios mitigate some of the multi-tenancy risks by restricting the number of co-tenants that have access to resources inside the CSP's external firewalls.

In the Community scenario, however, the cloud encompasses more organizations and hence will not restrict the number of co-tenants as much as in the case of a Private Cloud deployment.

[127] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 4-11

The reduction of co-tenant strategy is particularly applicable to those considering the use of Public Clouds, where perhaps moving to a Community or Private Cloud deployment would serve as an effective mechanism for reducing the threat.

Consideration CC-SE8 – Plan for Cloud Service Termination[128]

During the procurement phase of the contract, consideration should be given to planning for the eventual termination of a provider's service. The contract should clarify how assets are to be returned to cloud clients.

Applicability

	Public	Community	Private
IaaS	H	H	L
PaaS	H	H	L
SaaS	H	H	L

Admin Consideratio

Rationale: This is consistent with **Privacy Requirement 2 – Third-Party Agreements**.

Consideration CC-SE9 – Protect Cloud-Client Devices and Systems[129]

Cloud clients should consider protecting devices that will access cloud resources (e.g., a computer running a Web browser) so as to control exposure that might result if a compromised device gains access to those resources.

Applicability

	Public	Community	Private
IaaS	M	M	M
PaaS	M	M	M
SaaS	H	H	H

Admin Consideration

Rationale: If a cloud client visits a malicious Web site and the browser becomes compromised, subsequent access to a SaaS application might compromise the cloud client's data.

As the matrix indicates, this is particularly applicable to SaaS service

[128] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-1

[129] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-3

models; however, the potential exists for compromised cloud client devices to impact any cloud service model.

5.3.1.13.2. *Security Policy*

Consideration CC-SE10 – Evaluate Security Policy Differences

Determine whether, and how well, your organization's security policies fit within a cloud computing environment.

Applicability

	Public	Community	Private
IaaS	H	H	L
PaaS	H	H	L
SaaS	H	H	L

Admin Consideration

Rationale: Organizations interested in leveraging cloud services should first identify differences in security policy details between their current policies and those of the service that they are considering using. For example, the organization's password policy will most likely contain details of password length, strength and frequency of change. A public CSP that provides mail services may not provide any mechanism to enforce those policies but may enforce other policies.

The organization will have to evaluate these differences and then determine whether the organization's policies can be changed or whether a different solution may need to be identified.

This consideration is most appropriate to external CSPs since Private Cloud deployments should have no issues complying with existing policies.

5.3.1.13.3. *Organization of Information Security*

5.3.1.13.3.1. *Internal Organization*

No cloud-specific considerations were identified; however, all of the privacy requirements identified in **Section 4.4.1 – Internal Organization** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.13.3.2. *External Parties*

Consideration CC-SE11 – Identify a Client-Specific Security Perimeter[130,131]

Cloud clients should consider working with their chosen CSP to implement and/or identify a client-specific security perimeter that will allow a custodian (such as a cloud client) to achieve both a measure of control over the use of cloud resources and a means for monitoring access to them.

Applicability

	Public	Community	Private
IaaS	L	M	H
PaaS	**L**	M	H
SaaS	**L**	M	H

Policy & Procedures

Admin Consideration

Rationale: Where possible, having the ability to manage access to protected resources allows the cloud client to increase its visibility into the CSP's operation in order to support their custodial obligations.

From an applicability perspective, smaller CSPs and those where the cloud client has a larger measure of control (e.g. Private or Community Clouds) will have a considerable likelihood of successfully applying this consideration.

Consideration CC-SE12 – Evaluate Service Level Agreements with Respect to Compliance[132,133]

Cloud clients should carefully assess whether the Service Level Agreement (SLA) specifies compliance with appropriate laws and regulations governing the

Policy & Procedures

Admin Consideration

[130] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, § 6.3.2

[131] NIST - *Cloud Computing Synopsis and Recommendations* - SP 800-146, pg. 4-3

[132] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §*6.3.2*

[133] NIST - *Cloud Computing Synopsis and Recommendations* - SP 800-146, §3.4 & §8.4.1

type of information used by a specific cloud service.

Applicability

	Public	Community	Private
IaaS	H	H	M
PaaS	H	H	M
SaaS	H	H	M

Rationale: As data custodians, organizations are required to adhere to any and all custodial obligations within their jurisdiction. In some cases, compliance to local legislation is a policy or regulatory obligation. Organizations should ensure that the SLA with a CSP stipulates that the CSP should respect jurisdictional obligations and possibly those of the data custodian.

Consideration CC-SE13 – Evaluate Cloud Service Provider Against Specific Solution Privacy and Security Requirements[134]

Admin Consideration

As part of their due diligence exercise, cloud clients should first consider articulating their privacy and security requirements for storing and processing PHI in a cloud computing model. This would facilitate assessment and alignment of CSP and cloud client privacy and security requirements.

Applicability

	Public	Community	Private
IaaS	H	H	M
PaaS	M	H	M
SaaS	M	H	M

Rationale: Performing a gap assessment of the CSP's capabilities and requirements against that of the client organization can help to identify where additional effort may be needed to meet the client organization's risk threshold, or identify when that risk threshold cannot be achieved with the CSP being evaluated.

While obtaining the details of a CSP's privacy and security requirements and capabilities would be common in Community and Private deployment models, it may be significantly more difficult for a cloud client to obtain this information from a Public Cloud CSP.

[134] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §*6.3.2*

Consideration CC-SE14 – Ensure Appropriate Limitations on Liability[135]

Admin Consideration

Cloud clients should carefully examine the contractual/service agreement for any disclaimers relating to limitations on liability and ability for loss compensation.

Applicability

	Public	Community	Private
IaaS	H	M	L
PaaS	H	M	L
SaaS	H	M	L

Rationale: A CSP's contractual limitations on liability and insurance may be insufficient in the e-health context. The default service level agreements of Public Clouds specify limited promises that providers make to subscribers and limit the remedies available to subscribers and outline subscriber obligations in obtaining such remedies.

Consideration CC-SE15 – Assess CSP Third-Party Relationships[136]

Admin Consideration

Cloud clients should consider viewing cloud services and security as supply chain security issues. This means examining and assessing the provider's supply chain (i.e., the service provider's relationships and dependencies) to the extent possible.

Applicability

	Public	Community	Private
IaaS	L	M	H
PaaS	L	M	H
SaaS	L	M	H

Rationale: The CSP assessment should account for risks associated with failure of the CSP's suppliers to meet their obligations.

This is generally not possible to evaluate in the case of Public Cloud providers, but becomes more applicable in proportion to the amount

[135] NIST - *Cloud Computing Synopsis and Recommendations* - SP 800-146, pg. 4-14

[136] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 32

of control that the cloud client has over the CSP.

Consideration CC-SE16 – Assess the CSP's Risk-Management Approach[137]

Admin Consideration

Cloud clients should review the risk-management processes and governance of their CSPs to ensure that practices are consistent and aligned with their own business objectives.

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	M	H	H

Rationale: Where possible, an assessment of the CSP's risk-management approach allows cloud clients to determine the best deployment option and specific vendor of cloud services that has instituted risk-management processes that can be aligned and potentially integrated with those of the cloud client.

While Public Cloud CSPs generally may not be willing to provide this type of information, there are efforts underway by groups such as the Cloud Services Alliance that may make this more likely in the near future. Community and Private CSPs should be able to provide this information with minimal issue.

Consideration CC-SE17 – Assess CSP Privacy and Security Governance, Structure and Processes[138]

Admin Consideratio

Cloud clients should consider including a review of specific information security governance structure and processes as well as specific privacy and security controls as part of their due diligence for prospective provider organizations.

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	M	H	H

[137] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 32

[138] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 33

Rationale:

The CSP’s privacy and security governance processes and capabilities should be assessed for sufficiency, maturity and consistency with the cloud client’s privacy and security management processes and requirements. The CSP’s privacy and security controls should be demonstrably risk-based and clearly support these management processes.

The majority of CSPs will be able to provide information for such an assessment; however, the information from Public CSPs will not necessarily be as detailed or complete as the information that can be obtained from a Community or Private CSP, where the cloud client is also an organizational stakeholder.

Consideration CC-SE18 – Ensure Appropriate Privacy and Security Accountability within the CSP Organization[139]

Admin Consideration

Cloud clients should consider ensuring that appropriate accountability is assigned with respect to privacy and security in the CSP's organization.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale:

Privacy Requirement 1 – Accountable Person and **Security Requirement 3 – Information Security Management, Co-ordination and Allocation of Responsibilities** address the need for assigning appropriate accountability for privacy and security respectively within organizations that are health information custodians. This consideration leverages those two requirements to help cloud clients and CSPs align security roles and responsibilities.

Consideration CC-SE19 – Include Incident-Response Processes in Service Level Agreements[140]

[139] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 86

[140] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 101

Admin Consideration

As part of a Service Level Agreement, cloud clients should ensure that adequate incident-response processes (including roles and responsibilities) and metrics are identified.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: Ensuring adequate processes are in place for dealing with privacy and security incidents is a common custodial obligation.

Consideration CC-SE20 – Perform Cloud Solution Assessment[141]

Admin Consideration

Consideration should be given to using a cloud-specific assessment tool in order to evaluate the degree to which a particular CSP meets and demonstrates compliance with the cloud client's privacy and security requirements.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: Used in conjunction with **Consideration CC-SE3 – Determine Client Privacy and Security Requirements**, the use of a rigorous assessment tool enables a cloud client organization to easily identify whether, or which of, their privacy and security requirements will be met by the CSP.

Consideration CC-SE21 – Assess Cloud Service Provider[142]

Admin Consideration

A cloud client should consider:

a) Determining whether the capabilities for defining the necessary privacy and security controls exist within a particular CSP (see

[141] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §6.3.3

[142] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-1

Consideration CC-SE20 – Perform cloud solution assessment);

b) Determining whether those controls are being implemented properly; and

c) Ensuring that the controls put in place by the CSP are documented.[143]

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	M	H	H

Rationale: A thorough assessment of the capabilities and maturity of a CSP organization is necessary to identify gaps in privacy and security controls and provides a level of assurance that the CSP organization is capable of effectively managing the controls they do have.

While generally difficult to achieve in great detail with Public CSPs, the majority of commercial CSPs have independently verified certifications or audit reports that are made available to clients. There is also work being drafted by the Cloud Security Alliance's CloudTrust™ group that, if adopted, could be used to provide ongoing assessment capabilities of CSPs by cloud clients.

This is a highly desirable consideration since ensuring that any third party with which a custodian shares PHI has equivalent protections in place is a custodial obligation. See **Privacy Requirement 2 – Third-Party Agreements** and **Security Requirement 5 – Assessing Threats and Risks from Third Parties**.

[143] This may be accomplished via some form of third-party assessment and/or certification, as well as directly by the cloud client

Consideration CC-SE22 – Evaluate Certifications and Audit Statements[144]

Admin Consideration

A cloud client should consider scrutinizing any certifications (e.g. ISO 27001) or audit statements (e.g. SAS 70) available from the cloud provider for their scope of coverage and applicability.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: This consideration serves to 'level the playing field' with respect to certifications. Usually, the scope of any evaluation or audit is under the control of the organization that commissioned it, and in most cases that will be the CSP. Since they have the ability to exclude control objectives and related controls, comparing CSP organizations on the basis of whether they have a particular certification or audit statement may not provide sufficient information for a fair comparison.

Consideration CC-SE23 – Evaluate CSP Authentication Level of Assurance[145]

Admin Consideration

As part of due diligence exercises, cloud clients should consider whether the provider offers the use of appropriately robust authentication tokens or other forms of advanced authentication.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: In order to ensure control over their information resources in a cloud computing context, clients need reasonable assurance that they have exclusive access to the management functions of their

[144] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-1

[145] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-3

information resources. Authentication mechanisms that provide greater assurance for proving identity can mitigate risks associated with exploits such as account hijacking. This is related to **Security Requirement 1 –Threat and Risk Assessment**, and **Security Requirement 55 – Assigning Identifiers to Users.**

Interoperability Note: Cloud clients should consider the interoperability aspects of the CSP's authentication mechanisms. The use of industry-standard authentication techniques or tokens may permit the federation or reuse of system user credentials, thereby addressing adoption concerns. See **Consideration CC-SE62 – Use Standards-Based Authentication Mechanisms**.

Consideration CC-SE24 – Evaluate CSP Authentication and Authorization Capabilities[146]

Admin Consideration

Cloud clients should have visibility into the following capabilities of a provider:

1. Authentication and access-control mechanisms that the provider infrastructure supports;
2. Tools that are available for cloud clients to provision authentication information; and
3. Tools to input and maintain authorizations for cloud client users and applications without the intervention of the provider.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: Having an understanding of the capabilities that are available to clients that provide authentication and authorization enables the client organization to leverage those capabilities to meet their security requirements where applicable.

[146] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-3

Consideration CC-SE25 – Engage Appropriate Cloud Client Areas during SLA Negotiations[147]

Admin Consideration

In addition to input from their Legal department, cloud clients should consider engaging their Privacy and Information Security departments during the establishment of service level agreements and contractual obligations. This will help ensure that privacy and security requirements are contractually enforceable.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: This consideration helps ensure that a complete set of security requirements is brought forward at the appropriate time and that the implications of trade-offs made with privacy and security requirements is made clear.

Consideration CC-SE26 – Evaluate CSP Risk-Management Documents[148]

Admin Consideration

Cloud clients should consider requesting access to a CSP's risk-management documents (e.g. PIA, TRA or their summaries) as part of their due diligence process in order to confirm that the CSP security architecture and configuration of individual security controls documentation exists.

Applicability

	Public	Community	Private
IaaS	L	H	H
PaaS	L	H	H
SaaS	L	H	H

Rationale: This consideration serves to provide the cloud client with insight into a CSP's privacy and security processes. See **Consideration CC-PR2 – Ensure Appropriate CSP PIA and TRA Handling**.

[147] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 33

[148] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 69

Consideration CC-SE27 – Evaluate CSP Business Continuity Planning[149]

Admin Consideration

Cloud clients should ensure that the CSP has appropriate business continuity (BC) planning and disaster recovery (DR) processes, including relevant certifications (e.g., based on ISO and ITIL standards), audit reports and test protocols.

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	M	H	H

Rationale: This information allows clients to effectively incorporate cloud activities into their own Business Continuity/Disaster Recovery plans. Decisions regarding BC/DR capabilities and responsibilities should be defined and included in contractual agreements.

This consideration may have less applicability to Public Cloud providers, who may not be willing to share detailed information with prospective cloud clients.

Consideration CC-SE28 – Evaluate CSP Event and Incident-Management Processes and Data[150]

Admin Consideration

Consideration should be given, where required, to understanding how the CSP defines ‘events of interest’ versus privacy and/or security incidents, and what events/incidents, and how, the CSP reports to the cloud client. Event information that is supplied using an open standard can facilitate the processing of these reports by the cloud client.

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	M	H	H

[149] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 86

[150] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 100

Rationale: While this is currently unlikely to be supported by Public CSPs, this information it is critical in understanding whether and how the client's privacy and security incident protocols will need to be amended to support a cloud deployment. Without this information, it may be difficult for a cloud client to meet its custodial responsibilities with respect to PHI.

Consideration CC-SE29 – Evaluate SaaS Application Partitioning

Admin Consideration

If multi-tenancy features are not supported in a SaaS service model, consideration should be given to the additional risk associated with a single application and data image that supports multiple clients, rather than dedicated instances for each client.

Applicability

	Public	Community	Private
IaaS	L	L	L
PaaS	M	M	M
SaaS	H	H	H

Rationale: Successful deployment of the single application/data image depends on careful engineering of the application since the application may be processing data belonging to multiple clients at a single time.

This consideration is most applicable to SaaS service models, but has some applicability to PaaS models as well, where the platform may have been designed for multi-tenancy.

Consideration CC-SE30 – Evaluate IaaS Co-Tenant Risks[151]

Consideration should be given to evaluating whether an IaaS CSP has mechanisms in place to protect infrastructure images from risks associated with:

- Other virtual machines on the same physical host;
- The physical host; and
- Internal CSP network vulnerabilities.

Typical detection and prevention mechanisms include Virtual Firewalls, Virtual Intrusion Detection or Prevention Systems (IDS/IPS) and Virtual Private Networks.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	L	L	L
SaaS	L	L	L

Tech Consideration

Rationale: Cloud clients must be protected from potential eavesdropping or tampering on the part of other, possibly malicious, cloud clients. Cloud clients must be isolated from one another, except to the extent that they choose to interact.

This consideration is only applicable to IaaS deployments since this is the only deployment model where a cloud client can evaluate the CSP's controls of this type and put additional technical controls in place to mitigate residual risk.

[151] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 7-7 & 7-8

Consideration CC-SE31 – Conduct an Onsite Visit[152]

Admin Consideration

Cloud clients should consider an onsite visit to the CSP's facility or datacentre, which will allow for an on-the-spot assessment and help the client gain a clear understanding of the different security measures that have been put in place.

Applicability

	Public	Community	Private
IaaS	L	M	H
PaaS	L	M	H
SaaS	L	M	H

Rationale: While not generally offered by many Public CSPs, a site visit can serve as an important step in the due diligence process and can help to establish the likelihood of whether independent assessments are still valid.

Consideration CC-SE32 – Assess CSP's Availability Goals[153]

Admin Consideration

Cloud clients should consider reviewing the provider's business continuity plan and redundancy architecture to understand if their stated availability goals are supported.

Applicability

	Public	Community	Private
IaaS	H	H	L
PaaS	H	H	L
SaaS	H	H	L

Rationale: As part of due diligence, the cloud client should assess whether the CSP's availability estimate or goals are likely to be met.

[152] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 86

[153] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-1

Consideration CC-SE33 – Assess Critical CSP Operating and Service-Management Processes[154]

Admin Consideration

Cloud clients should consider assuring themselves that a CSP employs established internal operating procedures and service-management techniques for reliable system updates, data transfers and other site modifications.

Applicability

	Public	Community	Private
IaaS	M	H	L
PaaS	M	H	L
SaaS	M	H	L

Rationale: This is consistent with **Security Requirement 23 – Controlling Changes to the EHRi**.

5.3.1.14 Asset Management

5.3.1.15 Responsibility for Assets

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.5.1 – Responsibility for Assets** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.16 Information Classification

Consideration CC-SE34 – Classify 'Cloud-Appropriate' Resources[155]

Admin Consideration

Cloud clients should identify the specific resources (i.e. platforms, applications, data) that are suitable for migrating into and out of clouds. Resources could be:

1. Services, such as e-mail;

2. Data repositories, such as shared documents; or

3. Systems that run in virtualized environments.

Applicability

[154] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-1

[155] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-1

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: Identifying and classifying data and application functions in relation to their suitability for cloud deployment of any kind is a critical first step in utilizing cloud resources effectively. By not performing this analysis, client organizations may expose themselves to unqualified risks.

Consideration CC-SE35 – Establish Policies Regarding Location of Processing and Storage of Information[156]

Admin Consideration

An organization that is concerned with knowing workload (e.g., data processing, manipulation and storagelocation should discuss potential outsourcing configurations prior to implementing any cloud strategy, and should ensure that the outsourcing policies are clearly documented for all the cloud clients.

Applicability

	Public	Community	Private
IaaS	H	M	L
PaaS	H	M	L
SaaS	H	M	L

Rationale: In the Public Cloud context, the client resources (processing, disk storage, etc.) are dynamically assigned from an available pool. The assignment is opaque and can result in data being stored and processed in any location the cloud provider deems appropriate.

In some jurisdictions, privacy law places additional requirements on custodians and information managers before PHI can flow outside of federal, provincial or territorial boundaries.[157]

This consideration is most applicable to Public Cloud deployments,

[156] NIST - *Cloud Computing Synopsis and Recommendations* - SP 800-146, pg. 4-11

[157] Nova Scotia and British Columbia currently have legislation that restricts disclosure of personal information based on location

where the potential for storing and processing of sensitive information in multiple jurisdictions is highest. It may apply to Community deployments as well.

Consideration CC-SE36 – Use Data Classifications to Inform Cloud Decisions[158]

Admin Consideration

The characteristics of the cloud deployment and service model selected should be considered carefully in relation to any health information classification scheme.

Applicability

	Public	Community	Private
IaaS	L	H	H
PaaS	L	H	H
SaaS	L	H	H

Rationale: This is a basic consideration that supports the appropriate use of cloud resources in the e-health context.

Consideration CC-SE37 – Separate Data with Differing Sensitivities[159]

When data of differing levels of sensitivity is to be processed in a cloud, cloud clients should consider requiring protective mechanisms for separating sensitive and non-sensitive data at the CSP's site.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

[158] European Network and Information Security Agency (ENISA): *Benefits, risks and recommendations for information security*, pg. 70

[159] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-2

Rationale: One example of such a mechanism would be to use multiple distinct clouds concurrently to provide different levels of protection for sensitive and non-sensitive data.

5.3.1.17 Human Resources

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.6 – Human Resources Security** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.18 Physical and Environmental Security

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.7 – Physical and Environmental Security** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.19 Communications and Operations Management

No cloud-specific considerations were identified; however, all of the security requirements identified in Section 4.8 – Access Control still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.20 Operational Procedures and Responsibilities

Consideration CC-SE38 – Ensure Cloud Client and CSP Segregation of Duties[160]

Cloud clients should consider attempting to ensure that processes are in place to compartmentalize the job responsibilities of the CSP's administrators and separate them from the responsibilities of the cloud client's administrators.

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	M	H	H

Admin Consideration

Rationale: The insider security threat is a well-known issue for most organizations and extends to the cloud provider's staff as well. Therefore, cloud clients should make sure that the cloud provider's policies, procedures and controls to protect against malicious insiders are adequate.

[160] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-1

Consideration CC-SE39 – Create or Update Change-Management Procedures[161]

Cloud clients and providers should agree on a set of procedures the cloud client needs to perform covering: how to take an application offline (whether a software patch is going to be installed by the provider or cloud client); the testing that must be performed to ensure the application continues to perform as intended; and how to bring the application back online. Plans for system maintenance should be expressed in the service agreement.

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	M	H	H

Admin Consideration

Rationale: This is consistent with **Security Requirement 23 – Controlling Changes to the EHRi**.

5.3.1.21 Third-Party Service Delivery Management

Consideration CC-SE40 – Implement collaborative governance structures and processes[162]

Collaborative governance structures and processes between cloud clients and CSPs should be identified as necessary as part of the design and development of service delivery as well as service risk assessment and risk management protocols. These should then be incorporated into service agreements.

Applicability

	Public	Community	Private
IaaS	L	H	H
PaaS	L	H	H
SaaS	L	H	H

Admin Consideration

Rationale: As stated in the discussion for **Privacy Requirement 1 – Accountable Person**, custodians have an obligation to ensure comparable levels of protection for sensitive information that may be stored or processed in a cloud environment. Given the sometimes-

[161] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-2

[162] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 33

opaque nature of some cloud operations, a collaborative governance structure allows custodians to ensure that those obligations can be met.

This consideration has been identified as more applicable to Community and Private cloud deployments since Public CSPs are generally not in a position to participate in joint or collaborative governance structures.

5.3.1.22 System Planning and Acceptance

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.8.3 – System Planning And Acceptance** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.23 Protection against Mobile and Malicious Code

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.8.4 – Protection against Malicious and Mobile Code** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.24 Back-up

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.8.5 - Backup** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.25 Network security management

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.8.6 – Network Security Management** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.26 *Media Handling*

Consideration CC-SE41 – Encrypt PHI at Rest[163]

Admin Consideration

Consideration should be given to encrypting PHI at rest in any multi-tenant environment. In the event that PHI is stored in a Public Cloud, the applicability of this consideration in a SaaS environment will be high.

PbD Feature

Applicability

	Public	Community	Private
IaaS	H	H	M
PaaS	H	H	M
SaaS	L	H	M

Rationale: Encryption of data at rest can be an effective mitigation strategy against some of the risks of unauthorized access that are inherent in a multi-tenant, resource-pooling environment, as well as those that arise as a result of using a third-party service provider. (See **CC-SE56 – Prevent Data Leakage in Hybrid Deployment Models** and **CC-SE55 – Manage Cryptographic Keys**).

This consideration supports the Privacy by Design principle of Proactive, not Reactive[164] by recognizing and mitigating the increased risk of unauthorized disclosure in a multi-tenant environment.

Encryption of data at rest may not an option in a publicly deployed, SasS offering. Unless this is an option, organizations should look to other mitigation strategies for sensitive information in a Public CSP SaaS offering. A cloud client organization may want to consider leveraging Private or Community deployment models.

Consideration CC-SE42 – Ensure Secure Deletion of Data[165]

Admin Consideration

Consideration should be given to having a CSP identify a mechanism for reliably deleting data upon request. The availability of this mechanism and its reliability should be included in a service agreement and be consistent

[163] See Security Requirement 35 - Protecting data storage

[164] See http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

[165] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 5-9

with the cloud client's data retention, backup, business continuity and data deletion policies.

Applicability

	Public	Community	Private
IaaS	H	H	M
PaaS	H	H	M
SaaS	H	H	M

Rationale: Ensuring the secure deletion of sensitive information is a basic custodial responsibility.

This requirement is especially applicable in a multi-tenant environment, where resources are dynamically assigned as required.

5.3.1.27 Exchange of Information

Consideration CC-SE43 – Plan for Data Migration

Admin Consideration

Cloud clients should consider developing a plan for migration of data to and from the Cloud and for interacting with the data once it is resident in the Cloud.

Applicability

	Public	Community	Private
IaaS	L	H	H
PaaS	L	H	H
SaaS	L	H	H

Rationale: This consideration supports secure handling of sensitive information in transit, in use and at rest in the Cloud, as well as business continuity efforts.

5.3.1.28 Electronic Commerce Services

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.8.9 – Electronic Commerce Services** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.29 Monitoring

Consideration CC-SE44 – Leverage CSP Monitoring Mechanisms[166]

Cloud clients should consider requesting access to any additional monitoring mechanisms that are deployed at a provider's site. Consideration should also be given to evaluating the level transparency of controls and effectiveness of the controls made available by the provider.

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	M	H	H

Admin Consideration

Rationale: While not currently available with many Public CSPs, there are mechanisms proposed by the Cloud Service Alliance (CSA) that would allow a cloud client to mitigate the risk associated with the opaque nature of the cloud environment and potentially meet custodial obligations[167].

The intent of this consideration is to provide the cloud client with adequate monitoring mechanisms, which may be difficult with some Public Cloud CSPs.

Consideration CC-SE45 – Monitor Cloud Activities[168]

When PHI is used in a cloud deployment model, cloud clients should request that the CSP allow visibility into the operating services that affect a specific cloud client's data or operations on that data, including monitoring of the system's welfare.

Applicability

	Public	Community	Private
IaaS	L	H	H
PaaS	L	H	H
SaaS	L	H	H

Admin Consideration

[166] NIST - *Cloud Computing Synopsis and Recommendations* - SP 800-146, §3.4 & §8.4.1

[167] An example mechanism in draft form is the CloudAudit™ specification from the CSA (https://cloudsecurityalliance.org/research/cloudaudit) - accessed 2012-11-02

[168] *NIST Could Computing Synopsis and Recommendations* – SP 800-146, pg. 9-3

Rationale: While generally not expected from Public CSPs, having the ability to monitor access to, and operations on, PHI supports custodial obligations and could be accommodated with Community and Private Cloud deployments.

Consideration CC-SE46 – Consolidate Access Logs

When required, cloud clients should understand how access logs (application and/or system level) would be extracted and/or integrated into an organization logging service for a holistic picture of access.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	M	H	H

Tech Consideration

Rationale: Especially important as more services are distributed, the ability to account for access to PI or PHI is a fundamental privacy principle as well as a legal requirement in some jurisdictions.

It may be difficult to obtain log information in a way that allows for consolidation from a Public SaaS solution. As a result, this consideration may be less applicable to the Public SaaS scenario. The custodial obligation remains, however, and as a result, cloud clients may wish to look at other options should a SaaS CSP not be willing or able to provide access information in a manner that can be consolidated with other access information that the cloud client collects.

5.3.1.30 Access Control

No cloud-specific considerations were identified; however, all of the security requirements identified in 4.8 Access Control still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.31 Business Requirement for Access Control

Consideration CC-SE47 – Evaluate CSP-Provided Security Policy Management Capabilities[169]

Implementers should consider whether the CSP offers authorization-

Tech Consideration

[169] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 153

management Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs). If so, cloud clients should evaluate whether the PEPs and PDPs can be efficiently configured to allow clients to control authorization policies and ensure interoperability of security capabilities across internal and CSP services.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	L	L	L

Rationale: Support for client-controlled authorization policy tools and services allow clients a further measure of transparency into the CSP’s environment.

The use of standards in this area (e.g. OASIS XACML) provides the opportunity for a cloud client to integrate cloud services with enterprise authorization policies.

This consideration is generally not applicable to SaaS service models since cloud clients generally have no visibility into security policy decision or enforcement mechanisms.

5.3.1.32 User Access Management

Consideration CC-SE48 – Evaluate CSP-Provided Security Policy Management and Maintenance tools[170]

Admin Consideration

Cloud clients should identify CSPs that provide tools that support the intuitive authoring and maintenance of security policies and provide an integrated application development environment covering the full system lifecycle, with an orientation towards facilitating security accreditation.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

[170] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-5

Rationale: Tools that provide access to, and maintenance of, client security policies by the client increase transparency and provide cloud clients with additional controls that facilitate meeting their privacy and security requirements.

Consideration CC-SE49 – Evaluate PaaS Security Interoperability[171]

Admin Consideration

Consideration should be given to evaluating whether a PaaS application can be integrated with existing enterprise/organizational security frameworks such as Identity and Access Management (IAM) solutions.

Applicability

	Public	Community	Private
IaaS	L	L	L
PaaS	H	H	H
SaaS	L	L	L

Rationale: The ability to integrate with a cloud client's IAM solution allows existing identity credentials and authorization policies to be used and enforced in the cloud context. This also facilitates adoption by limiting the number of system user credentials required.

5.3.1.33 User responsibilities

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section4 8 3 User Responsiblities** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

[171] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 6-5

5.3.1.34 Network access control

Consideration CC-SE50 – Use Mutually Authenticated Communications Channels[172]

Tech Consideration

Implementers should consider the use of mutually authenticated communications channels between cloud services and client devices as a critical element in reducing the risk associated with certain attacks.

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	L	L	L

Rationale: The use of mutual authentication (e.g. SSL/TLS) is useful for avoiding risks associated with man-in-the-middle attacks and is especially useful in cloud environments to ensure both clients and servers are communicating with known, trusted counterparts.

5.3.1.35 Operating System Access Control

Consideration CC-SE51 – Restrict Administrative Access to Cloud Resources[173]

Tech Consideration

When using cloud computing resources, organizations should provide only a limited set of trained and trusted users (from the cloud client organization) with administrative access to those resources.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: Limiting access to these resources is consistent with **Security Requirement 24 – Segregating Duties** and **Security Requirement 58 – Granting Access to Users by Role**.

[172] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 155

[173] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 7-8

5.3.1.36 Application and Information Access Control

Consideration CC-SE52 – Use Multi-Tenant-Aware PaaS Application Development Frameworks[174]

Admin Consideration

If available, consideration should be given to those PaaS systems that provide application development frameworks that include architecture and tools for mitigating security vulnerabilities and supporting multi-tenancy where necessary.

Applicability

	Public	Community	Private
IaaS	L	L	L
PaaS	H	H	H
SaaS	L	L	L

Rationale: PaaS offerings that allow the cloud client to self-manage and maintain their own access-control policies independent of other tenants provide increased transparency and allow the client to maintain control of specific safeguards.

Cloud-specific, privacy-protective data architectures should be used to enhance the chosen security architectural framework in order to address cloud-specific issues and threats.

Consideration CC-SE53 – Assess SaaS Application Support for Privacy and Security[175]

Admin Consideration

Consideration should be given to those SaaS offerings that provide applications that include architectural support and tools for mitigating security vulnerabilities and support multi-tenancy where necessary (e.g. Security-as-a-Service).

Applicability

	Public	Community	Private
IaaS	L	L	L
PaaS	L	L	L
SaaS	H	H	H

[174] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 6-5

[175] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 9-1

Rationale: SaaS applications that are specifically written to run in a multi-tenant environment, including Security-as-a-Service, can provide additional measures of control compared to traditional applications simply moved to an SaaS model.

5.3.1.37 Mobile Computing and Teleworking

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.8.8 Mobile Computing Telework** still apply. In addition, **Section 5.3.2 - Mobile Devices** deals specifically with privacy and security considerations for organizations introducing or using mobile devices in their environment. Please refer to those sections for security requirements and considerations as they may apply to cloud computing.

5.3.1.38 Information Systems Acquisition, Development and Maintenance

5.3.1.39 Security Requirements for Information Systems

Consideration CC-SE54 – Design Cloud Applications for Multi-tTenancy[176]

Tech Consideration

Where appropriate, organizations should consider designing or acquiring the use of cloud-candidate applications that embed multi-tenancy concepts and provide controls that allow the organization, and potentially other cloud clients, some measure of transparency and control over access and authorization policies.

PbD Feature

Applicability

	Public	Community	Private
IaaS	M	H	H
PaaS	M	H	H
SaaS	L	H	H

Rationale: Multi-tenancy is one of the core characteristics of the cloud computing model; however, this characteristic increases the risk of unauthorized access and usage. Ensuring that multi-tenancy concepts are designed into the application allows for the potential for cloud clients to control access to sensitive information via the application. See **Consideration CC-SE52 – Use Multi-Tenant**

[176] Canada Health Infoway – *ETG Cloud Computing Technology Profile*, §6.3.6

Aware PaaS Application Development Frameworks.

5.3.1.40 Correct Processing in Applications

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.10.2 – Correct Processing of Information** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.41 Cryptographic Controls

Consideration CC-SE55 – Manage Cryptographic Keys[177]

In a multi-tenancy cloud context where encryption of PHI-at-rest is used, clients should consider managing their own cryptographic keys or use a trusted, specialized cryptographic service.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	L	H	H

Tech Consideration

Rationale: By maintaining control over private keys that are used to protect sensitive information and establish the integrity of messages, clients are able to increase their scope of control over the access and use of information stored or processed within a cloud service.

This consideration is applicable to all deployment and service models, with the exception of the Public SaaS deployment. Since the Public Cloud CSP controls the entire processing stack, it will be difficult for a cloud client to specify whether or how cryptographic controls are used.

5.3.1.42 Security of System Files

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.10.4 – Security of System Files** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

[177] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 134

5.3.1.43 Security in Development and Support Processes

Consideration CC-SE56 – Prevent Data Leakage in Hybrid Deployment Models[178]

Tech Consideration

If a cloud client wishes to use cloud computing for non-sensitive computing, while retaining the security advantages of on-premise resources for sensitive computing, care must be taken to store sensitive data in encrypted form or identify other privacy and/or security controls.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: In any hybrid multi-deployment model scenario where data with different security classifications exists, there is a risk of unintended data leakage from one system or application to another. Encrypting PHI-at-rest is one mechanism to reduce the risk of data leakage.

5.3.1.44 Technical Vulnerability Management

Consideration CC-SE57 – Request Use of Content-Discovery Tools[179]

Tech Consideration

Cloud clients should consider requesting the ability to use content-discovery tools to scan cloud storage and identify exposed sensitive data, or having the provider perform this on their behalf.

Applicability

	Public	Community	Private
IaaS	L	H	H
PaaS	L	H	H
SaaS	L	H	H

Rationale: While not likely supported by Public Cloud providers, the use of these kinds of tools can help to identify unintended exposure of sensitive information.

[178] *NIST - Cloud Computing Synopsis and Recommendations* – SP 800-146, pg. 8-8

[179] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 57

5.3.1.45 Information Security Incident Management

5.3.1.46 Reporting Information Security Events and Weaknesses

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.11.1 – Reporting Incidents and Weaknesses** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.47 Management of Information Security Incidents and Improvements

See **CC-SE19 – Include Incident Response Processes in Service Level Agreements** and **CC-SE28 – Evaluate CSP Event and Incident Management Processes and Data**.

5.3.1.48 Business Continuity Management

Consideration CC-SE58 – Mitigate Against the Risk of CSP Business Failure[180]

Admin Consideration

Consideration should be given to mitigation strategies that offset the risk of a CSP failing, such as:

1. Employing redundant clouds;
2. Monitoring the business health of providers; and
3. Employing hybrid clouds.

Applicability

	Public	Community	Private
IaaS	H	M	L
PaaS	H	M	L
SaaS	H	M	L

Rationale: With public or outsourced cloud computing, cloud clients depend on near-real-time provisioning of services by providers.

Since business shutdown is normal in any marketplace, this dependence is a risk to cloud clients with time-critical computing needs. This consideration is especially relevant to Public CSPs.

[180] NIST - *Cloud Computing Synopsis and Recommendations - SP 800-146*, pg. 8-4

5.3.1.49 Compliance

5.3.1.50 Compliance with Legal Requirements

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.13.1 – Compliance with Legal Requirements** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

5.3.1.51 Compliance with Security Policies and Standards, and Technical Compliance

5.3.1.52

Consideration CC-SE59 – Control Processing and Storage Locations[181]

Cloud clients should determine whether mechanisms to control the physical location of any deployed resources are provided by the CSP, and if they exist, how effective the controls are.

Applicability

	Public	Community	Private
IaaS	H	M	L
PaaS	H	M	L
SaaS	H	M	L

Admin Consideration

Rationale: Once an organization has established its policies with respect to the physical location of information resources, they then need to evaluate the capabilities of the CSP to limit or control the location where the cloud client's storage and processing will take place. In a Public Cloud, cloud clients may not be in a position to verify or request location restrictions.

This consideration is most applicable to Public Cloud deployments, where the potential for storage and processing of sensitive information in multiple jurisdictions is highest, but can apply to certain Community deployments as well.

5.3.1.53 Information Systems Audit Considerations

No cloud-specific considerations were identified; however, all of the security requirements identified in **Section 4.13.3 – Information Systems Audit Considerations** still apply. Please refer to that section for security requirements as they may apply to cloud computing.

[181] NIST - *Cloud Computing Synopsis and Recommendations* - SP 800-146, pg. 4-14

5.3.1.54 Interoperability Considerations

This section deals primarily with considerations that have interoperability impact on the privacy and security area of concern.

Consideration CC-SE60 – Evaluate the Use of Dedicated Identity Management Services

Consideration should be given to how identities will be managed in a hybrid-cloud environment. Cloud clients should consider using dedicated identity management services to facilitate interoperability for authentication and data-sharing purposes between applications and/or clouds rather than using the individual identities in each cloud service or application.

PbD Feature

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Admin Consideration

Tech Consideration

Rationale: CSPs that provide standards-based interfaces for identity management allow clients to use a single-identity strategy for their organization (or security domain). Lack of this type of standards support introduces complexity, overhead and additional risk into the organization's identity management processes.

Consideration CC-SE61 – Assess the Use of a Federated Identity Management (FIdM) Scheme

Cloud clients should consider the many aspects of implementing federation across deployment models and the federation of identities.

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Admin Consideration

Tech Consideration

Rationale: CSPs that support FIdM standards allow cloud clients to establish controls that can interoperate with existing systems, other cloud services and service providers.

Consideration CC-SE62 – Use Standards-Based Authentication Mechanisms[182]

Tech Consideration

Data and applications in the cloud reside on systems the user does not own and likely has limited control over. An important item to consider for interoperable security is the use of interoperable standards for authentication (e.g. SAML, WS-Security).

Applicability

	Public	Community	Private
IaaS	H	H	H
PaaS	H	H	H
SaaS	H	H	H

Rationale: CSPs that support these standards allow cloud clients to establish controls that can be interoperable with existing systems, as well as with other cloud services and service providers.

5.3.1.55 Mapping Considerations to Privacy Principles and Security Clauses.

The issues and considerations identified in the previous material span a number of privacy and security areas. The table below identifies, for each consideration, any appropriate CSA Model Code privacy principle and/or ISO 27002 security clause that it relates to in order to assist the reader to map considerations to any particular privacy or security area.

Table 1. Cloud Computing: Considerations Mapped to Privacy Principles and ISO Security Clauses

Consideration	CSA Model Code/Privacy by Design Principle	ISO 27002 Section
CC-SE11 – Identify a Client-Specific Security Perimeter	1(3) – Accountability 7(1) – Safeguards	6.2 – External parties
CC-SE12 – Evaluate Service Level Agreements with Respect to Compliance	1(3) – Accountability	6.2 – External parties 15.1 – Compliance with legal requirements
CC-SE44 – Leverage CSP Monitoring Mechanisms	7(1) – Safeguards	10.10 – Monitoring

[182] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)*, pg. 67

Consideration	CSA Model Code/Privacy by Design Principle	ISO 27002 Section
CC-SE5 – Use Cloud-Specific Controls	7(1) – Safeguards	4.2 – Treating security risks
CC-SE13 – Evaluate Cloud Service Provider Privacy and Security Requirements	7(1) – Safeguards	10.1 – Security requirements of information systems
CC-SE6 – Select Appropriate Deployment and Service Models where no Monitoring Exists	N/A	4.2 – Treating security risks
CC-SE14 – Ensure Appropriate Limitations on Liability	7(1) – Safeguards	6.2 – External parties
CC-SE35 – Establish Policies Regarding Location of Processing and Storage of Information	7(1) – Safeguards	7.2 – Information classification
CC-SE59 – Control Processing and Storage Locations	7(1) – Safeguards	7.2 – Information classification
CC-SE56 – Prevent Data Leakage in Hybrid Deployment Models	7(1) – Safeguards	12.5 – Security in development and support processes
CC-SE45 – Monitor Cloud Activities	7(1) – Safeguards	10.10 – Monitoring
CC-SE15 – Assess CSP third party relationships	7(1) – Safeguards	6.2 – External parties
CC-SE16 – Assess CSP Risk-Management Approach	7(1) – Safeguards	6.2 – External parties
CC-SE17 – Assess CSP Privacy and Security Governance, Structure, and Processes	7(1) – Safeguards	6.2 – External parties
CC-SE40 – Implement Collaborative Governance Structures and Processes	1(3) – Accountability	6.2 – External parties 10.2 – Third-party service delivery management
CC-SE1 – Establish Cloud Client Risk Tolerance	1(3) – Accountability	ISO 27001: §5.1 – Management Commitment ISO 27005: §7.2 – Basic Criteria
CC-SE18 – Ensure Appropriate Privacy and Security Accountability within the CSP Organization	1(3) – Accountability	6.2 – External parties
CC-SE19 – Include Incident Response Processes in Service Level Agreements	7(1) – Safeguards	6.2 – External parties 13 – Information security incident management

Consideration	CSA Model Code/Privacy by Design Principle	ISO 27002 Section
CC-SE55 – Manage Cryptographic Keys	7(1) – Safeguards	12.3 – Cryptographic controls
CC-PR3 – Use Privacy-Enhanced Identifiers	5 – Limiting Use, Disclosure and Retention 7(1) – Safeguards PbD-1 – Proactive not Reactive PbD-3 – Privacy Embedded into Design	N/A
CC-SE2 – Assess Data Confidentiality	1(3) – Accountability 5 – Limiting Use, Disclosure and Retention 7(1) – Safeguards PbD-1 – Proactive not Reactive PbD-2 – Privacy as the Default	4.1 – Assessing security risks 6.2 – External parties
CC-SE41 – Encrypt PHI at rest	7(1) – Safeguards	10.7 – Media handling
CC-SE3 – Determine Client Privacy and Security Requirements	7(1) – Safeguards	4.1 – Assessing security risks
CC-SE20 – Perform Cloud Solution Assessment	7(1) – Safeguards	6.2 – External parties
CC-SE42 – Ensure Secure Deletion of Data	5(3) – Limiting Use, Disclosure and Retention 7(5) - Safeguards	10.7 – Media handling
CC-SE52 – Use Multi-Tenant-Aware PaaS Application Development Frameworks	7(1) – Safeguards	11.5 – Operating system access control 11.6 – Application and information access control 12.2 – Correct processing in applications
CC-SE53 – Assess SaaS Applications Support for Privacy and Security		11.6 – Application and information access control 12.2 – Correct processing in applications

Consideration	CSA Model Code/Privacy by Design Principle	ISO 27002 Section
CC-SE21 – Assess Cloud Service Provider		6.2 – External parties
CC-SE34 – Classify 'Cloud-Appropriate' Resources	7(1) - Safeguards	7.2 – Information classification
CC-SE22 – Evaluate Certifications and Audit Statements	7(1) – Safeguards	4.1 – Assessing security risks 6.2 – External parties
CC-SE38 – Ensure Cloud Client and CSP Segregation of Duties	7(1) – Safeguards	10.1 – Operational procedures and responsibilities
CC-SE23 – Evaluate CSP Authentication Level of Assurance	7(1) – Safeguards	4.1 – Assessing security risks 11.4 – Network access control
CC-SE24 – Evaluate CSP Authentication and Authorization Capabilities	7(1) – Safeguards	4.1 – Assessing security risks 11.2 – Privilege management 11.4 – Network access control
CC-SE48 – Evaluate CSP-Provided Security Policy Management and Maintenance Tools	N/A	11.1 – Access control policy
CC-SE25 – Engage Appropriate Cloud Client Areas during SLA Negotiations	1(3) - Accountability	6.2 – External parties
CC-PR1 – Assess Compliance Impact	1 – Accountability	4.1 – Assessing security risks 15.5 – Compliance with security policies and standards, and technical compliance

Consideration	CSA Model Code/Privacy by Design Principle	ISO 27002 Section
CC-SE26 – Evaluate CSP Risk-Management Documents	7(1) – Safeguards	6.2 – External parties
CC-SE27 – Evaluate CSP Business Continuity Planning	7(1) – Safeguards	6.2 – External parties 14.1 – Information security aspects of business continuity management
CC-SE28 – Evaluate CSP Event and Incident-Management Processes and Data	1 - Accountability	6.2 – External parties 13.2 – Management of information security incidents and improvements
CC-PR2 – Ensure Appropriate CSP PIA and TRA Handling	1 – Accountability PbD-3 – Privacy Embedded into Design	4.1 – Assessing security risks 6.2 – External parties 15.1 - Compliance
CC-SE43 – Plan for Data Migration	7 – Safeguards	7.2 – Information classification 10.8 – Exchange of information
CC-SE36 – Use Data Classifications to Inform Cloud Decisions	7 – Safeguards	7.2 – Information classification
CC-SE54 – Design Cloud Applications for Multi-Tenancy	7 – Safeguards	12.1 – Information security requirements 12.5 – Development and support processes
CC-SE4 – Assess Appropriate Use of Virtualisation Technologies	N/A	6.2 – External parties
CC-SE7 – Reduce Multi-Tenancy Threats	7 – Safeguards	4.2 – Treating security risks 6.2 – External parties

Consideration	CSA Model Code/Privacy by Design Principle	ISO 27002 Section
CC-SE29 – Evaluate SaaS Application Partitioning	7 - Safeguards	4.1 – Assessing security risks 6.2 – External parties
CC-SE49 – Evaluate PaaS Security Interoperability		11.2 – User access management
CC-SE30 – Evaluate IaaS Co-Tenant Risks	7 - Safeguards	4.1 – Assessing security risks 6.2 – External parties
CC-SE47 – Evaluate CSP-Provided Security Policy-Management Capabilities	N/A	11.1 – Access control policy
CC-SE50 – Use Mutually-Authenticated Communications Channels	7 – Safeguards	11.4 – Network access control
CC-SE51 – Restrict Administrative Access to Cloud Resources	7 – Safeguards	11.5 – Operating system access controls
CC-SE31 – Conduct an Onite Visit	7 – Safeguards	4.1 – Assessing security risks 6.2 – External parties
CC-SE37 – Separate Data with Differing Sensitivities	7 – Safeguards	7.2 – Information classification
CC-SE60 – Evaluate the Use of Dedicated Identity Management Services	N/A	N/A
CC-SE61 – Assess the Use of a Federated Identity Management (FIdM) Scheme	PbD-3 – Privacy Embedded into Design	N/A
CC-SE62 – Use Standards-Based Authentication Mechanisms	PbD-3 – Privacy Embedded into Design	N/A
CC-SE46 – Consolidate Access Logs	1 - Accountability PbD-7 – Respect for User Privacy	10.10 – Monitoring
CC-SE58 – Mitigate against Risk of CSP Business Failure	N/A	4.1 – Assessing security risks 14.1 – Information security aspects of business continuity management

Consideration	CSA Model Code/Privacy by Design Principle	ISO 27002 Section
CC-SE8 – Plan for Cloud Service Termination	N/A	4.1 – Assessing security risks 14.1 – Information security aspects of business continuity management
CC-SE32 – Assess CSP`s Availability Goals	N/A	4.1 – Assessing security risks 14.1 – Information security aspects of business continuity management
CC-SE33 – Assess Critical CSP Operating and Service-Management Processes	7 - Safeguards	4.1 – Assessing security risks 10.1 – Operational procedures and responsibilities
CC-SE39 – Create or Update Operating Procedures	7 – Safeguards	10.1 – Operational procedures and responsibilities
CC-SE9 – Protect Cloud Client Devices and Systems	7 - Safeguards	4.2 – Treating security risks
CC-SE10 – Evaluate Security Policy Differences		5.1 – Information security policy
CC-SE57 – Request Use of Content-Discovery Tools	7 – Safeguards	12.6 – Technical vulnerability management

5.3.2 Mobile Devices

Mobile devices – laptops, tablets, smartphones and Personal Digital Assistants (PDAs) – are a fact of life in many health care settings. The Cisco® Visual Networking Index[183] estimates that 29% of all devices connected to the Internet in Canada will be mobile by the year 2016 and that mobile data traffic will grow at a compound annual rate of 83% between 2011 and 2016.

These mobile devices provide a number of mechanisms for users to conveniently collect, access and disclose PHI. The devices are used in a variety of settings by providers with a variety of applications. In addition, these devices are increasingly being used by patients for a broad range of functions related to their health, from gathering

[183] The Cisco® Visual Networking Index (http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html) is an ongoing initiative to track and forecast the impact of visual networking applications on global networks. The version referenced in this document was last updated 2012-02-12 and was accessed on 2012-10-08

information on a particular health issue, to scheduling appointments with providers, to capturing health measurement data.

For the purposes of this section, a mobile device is considered to have the following characteristics:[184]

- Capable of being easily carried in one hand (i.e. a small form factor);
- The device has some computational capability and can run at least one application;
- The device is able to perform some of its basic functions without being physically tethered to either a power source or a network (i.e. it is 'mobile');
- The device has some ability to store information locally; and
- The device has some ability to communicate wirelessly with other systems.

Many mobile devices in common use today have capabilities that far exceed those listed above. Many are able to record high-quality audio and video, run a wide variety and rapidly increasing number of applications, determine their current location, retrieve and transmit information over high-speed networks using at least one type of wireless networking and store large amounts information internally and on small, removable storage media.

The portability of these devices means that they can be used to provide benefits anywhere the user is. This same portability means that traditional mechanisms used to physically secure stationary devices within the organization's boundaries cannot be used.

Until recently, organizations have used traditional approaches to the acquisition and management of mobile devices – the devices are controlled by the organization and provided to users with a limited set of functions. More recently, using employee-owned devices to store and access corporate information has been seen to provide more utility for the user and may offer potential cost savings to the organization. This "Bring Your Own Device" (BYOD) strategy results in a user's personal applications and information residing on the same device as the organization's sanctioned applications and information.

The effective management of a wide variety of consumer-class devices that allow the user the freedom to do what they like with their devices while maintaining adequate privacy and security controls over information that the organization is responsible for can be a significant challenge. Mobile Device Management (MDM) solutions have been developed to help organizations with this challenge, and Gartner Group, while classifying this market as nascent, has identified more than 100 vendors[185] in this space, with rapid growth being seen.

[184] NIST SP800-124 Rev 1 (Draft) - *Guidelines for Managing and Securing Mobile Devices in the Enterprise* – July, 2012

[185] Gartner press release: http://www.gartner.com/it/page.jsp?id=2010217, accessed 2012-12-04

5.3.2.1 Issues

The previous section outlined some of the benefits of adopting mobile devices within organizations. This adoption does, however, raise some issues and areas of concern, which this section identifies.[186]

Policies and Procedures

The introduction of mobile computing into an organization requires that privacy and security policies and procedures be created or updated to reflect an environment where confidential information is accessed via, or stored on, mobile devices.

In this context, confidential information encompasses information that either the mobile device user or the organization wishes to remain confidential. The term encompasses any combination of personal information, personal health information and business confidential information.

Users having physical control of a device that contains, or has access to, confidential information presents privacy and security vulnerabilities that are normally mitigated by a series of physical and technical controls, largely administered directly by operations or security staff.

Users need to have a reasonable understanding of the privacy and security risks associated with the devices under their control. Education should be provided so that users will understand how their actions can increase or decrease those risks and what practices are appropriate for organization-controlled devices, applications or information.

Device and Application Management

Whether using organization-owned or user-owned (BYOD) devices, the introduction of mobile technologies requires device and application management strategies, processes and procedures that will ensure that the mobile devices that can access and store information under the organization's control have adequate safeguards.

Gartner defines a Mobile Device Management solution as one that:

> *"includes software that provides the following functions: software distribution, policy management, inventory management, security management and service management for smartphones and media tablets. MDM functionality is similar to that of PC configuration life cycle management (PCCLM) tools; however, mobile-platform-specific requirements are often part of MDM suites."*[187]

All-encompassing MDM solutions include management of device firmware, application deployment and remote data erase capabilities. A newer class of management tool – Mobile Application Management solutions – focuses on application provisioning, versioning and security management alone.

[186] Readers are encouraged to review the HIMSS® Mobile Security Toolkit at http://www.himss.org/files/HIMSSorg/content/files/PrivacySecurity/MS01_MS_Toolkit_Intro_Final.pdf for additional information on privacy and security issues and recommendations

[187] Gartner IT Glossary - http://www.gartner.com/it-glossary/mobile-device-management-mdm - accessed 2013-02-12

Physical Control

One of the more obvious issues with respect to mobile computing is that the use of the device can take place in locations that are outside an organization's control. As a result, the organization is unable to use the physical controls that are normally used to protect non-mobile devices from loss, theft or tampering. Once lost or stolen, confidential information may be at risk of being exposed to unauthorized users if an organization does not institute an appropriate mitigation strategy that is focussed on mobile issues and capabilities.

User Identity and Authentication

A great many mobile devices have few or no identity and access control mechanisms activated by default; however, the requirement to identify a user with some level of assurance prior to allowing access to corporate applications and/or confidential information is no different on a mobile device than with any other access path.

Many organizations are deploying mobile devices for use within a department (e.g. a hospital ward) and the device is shared by multiple individuals over the course of a day. This deployment model can present challenges to certain devices that do not have multi-user design concepts embedded into the operating system. In those cases, multiple levels of user authentication may need to be used in order to uniquely identify the individual using a shared device at any given time. This issue is equally (if not more) applicable to user-owned devices accessing organizational resources.

The interoperability of mobile identities within applications running on a mobile device and with organizational and/or federated identities is not a default capability. Strategies need to be identified and implemented in order to enable such interoperability.

Access Control

The lack of default access controls in many mobile devices creates the potential for unauthorized access to the device owner's personal information as well as confidential, organization-controlled information. While most mobile devices have access-control capabilities, either as part of the operating system or as an add-on application, these capabilities need to be evaluated and integrated into the organization's overall access-control strategy in order to be effective.

Location Privacy

Many mobile devices have onboard Global Position System (GPS) capabilities that can pin-point the device's (and therefore the user's) location to within a few metres. This information can be collected by on-device applications and transmitted, knowingly or unknowingly, to a central service to build up a profile of a person's whereabouts.

Bring Your Own Device (BYOD)

The use of user-owned mobile devices to access and store confidential corporate information introduces an additional set of privacy and security issues over and above those associated with organization-owned devices. Specifically, issues relating to untrusted applications and untrusted devices are key areas warranting focus.

Application Trustworthiness

Mobile operating system and device vendors provide online, electronic 'storefronts', giving users the ability to download, install and run their choice of hundreds of thousands of applications on their mobile devices.

While certain storefronts publish and enforce guidelines related to the development of applications, these guidelines are not standardized among vendors. Regardless of a particular vendor's application development guidelines, or enforcement thereof, an organization's privacy and security policies for the handling and protection of confidential information are unlikely to be met based solely on compliance with any storefront's guidelines.

Unlike organization-owned devices, users can determine what applications are downloaded and installed on the devices that they own. In order to have a successful BYOD environment, organizations must work together with the users to protect organization-controlled confidential information, at the same time allowing users the greatest flexibility to configure user-owned devices to suit their needs.

As with stationary devices, malicious applications have been produced and made available that compromise the security of the mobile device and its information. This is particularly significant when dealing with user devices that have been 'jail broken' or 'rooted', where the operating system and/or controls put in place by the system vendor have been overwritten by the user (see Device Trustworthiness below).

Device Trustworthiness

Each mobile device model and operating system release supports a set of privacy and security controls that must be evaluated from the organization's perspective to determine whether the device can be configured appropriately to access and store confidential information. User-owned devices may have various software components, including the vendor-supplied operating system, that can be replaced with less-secure alternatives. In keeping with their privacy and security policies, any organization contemplating a BYOD strategy will need to determine how to effectively manage the configuration profile (i.e., application and operating system configurations) of a wide variety of devices.

Prior to any evaluation of user-owned devices, the organization should be able to explain the scope of the examination and the limits that will be placed on collection, use and disclosure of personal information that is contained on a user-owned device.

Network Security

Mobile devices have the capability to communicate wirelessly over a number of different network technologies, the most common ones of which are currently cellular, Wi-Fi and Bluetooth. Each of these technologies has different vulnerabilities that should be understood and appropriate mitigation strategies employed in order to ensure the privacy and security of information that is exchanged over these networks.

In many cases, the considerations for overcoming untrusted wireless networks is similar to that employed to safeguard communications over any public or untrusted network.

5.3.2.2 Considerations

This section identifies the specific considerations that should be taken into account when an organization is planning to deploy, or is deploying, mobile devices. The considerations are organized in the same order as the issues discussed in the previous section.

Policies and Procedures

Consideration MC1 – Determine Business Criteria for Use of Mobile Devices

Organizations should review their business mandate and operations to determine if the adoption of mobile devices and BYOD arrangements are appropriate and feasible.

Admin Consideration

Rationale: The benefits associated with the use of mobile devices to store and/or access confidential information should be weighed against the increase in costs to mitigate the increased risks to privacy and security.

Consideration MC2 – Evaluate and Augment Policies, Procedures and User Training

Organizations should augment their privacy and security policies, procedures and training to include specific role-based training related to mobile devices and BYOD arrangements, if required.

Admin Consideration

Rationale: A custodian has a responsibility to take reasonable steps to protect against the loss, theft or unauthorized use or disclosure of PHI.[188] When the use of mobile devices is expected or required as part of a person's role, specific privacy and security training on the mobile devices in use is appropriate.[189]

The user of a mobile device has full physical control over that device when not on the organization's premises, a responsibility with

[188] Alberta *Health Information Act - 2000,* S.8(6), Ontario *Personal Health Information Protection Act – 2004, S.12(1)*

[189] CSA Model Code, Principle 7 – Safeguards - *http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code/article/safeguards*

obligations that may not normally be part of the user's role. Providing detailed privacy and security training and continued follow-up helps to improve the user's understanding of the risks as well as the individual's obligations with respect to the confidential information stored on, or accessed by, that device.

Consideration MC3 – Create and / or Update Privacy and Security Policies

Organizations should evaluate whether they need to create and/or update policies to reflect their privacy and security requirements in respect of mobile devices. Consideration should be given to addressing topics such as:

a) What classification(s) of confidential information are acceptable on a mobile device;

b) What protections (e.g. encryption) are required in order to store confidential information on mobile devices;

c) Acceptable use of organization-owned and user-owned mobile devices, including:

   a. user obligations with respect to incident management; and

   b. attributes of mobile applications that are not acceptable.

d) The requirements or criteria for supporting a mobile device;

e) What information will be collected from the individual using the mobile device, and the purpose for that collection;

f) What obligations the individual and the organization have when devices are relinquished or staff terminated; and

g) What the frequency and extent of automatic review of default settings is for any device that is being, or has been, on-boarded.

Organizations considering BYOD arrangements should also review:

h) What user obligations will be required with respect to security of their devices; and

i) What the organization's rights are regarding collection, use, disclosure and retention of device identity data and the auditing of device use.

Admin Consideration

Rationale: See **Privacy Requirement #3 – Privacy Policy**, and **Security Requirement #2 – Security Policy**. Policy updates should be taken into account when looking at **Consideration MC2 – User Training**.

Consideration MC4 – Update Operational Processes and Procedures

Organizations should identify and apply any updates that may be required to their operational processes and procedures in order to support the introduction of mobile devices. Examples of the procedures that may be affected include:

a) Malware protection;

b) Operating system and application patch management;

c) Secure handling and disposal of mobile media; and

d) Data backup.

Admin Consideration

Rationale: Introducing new devices and technology into any organization may require updated or additional processes or procedures to ensure that the organization's obligations with respect to the protection of sensitive information are being met.

Device Management

Consideration MC5 – Evaluate and Deploy a Mobile Device Management System

Organizations should evaluate whether the acquisition and deployment of a Mobile Device Management (MDM) and/or a Mobile Application Management (MAM) solution would benefit them in helping to ensure compliance with mobile-specific privacy and security policies.

Tech Consideration

Rationale: The use of MDM/MAM solutions can help to ensure that privacy and security policies are being adhered to without a significant investment in human resources that might be required to perform the same functions manually. The same solutions can be leveraged to provide functions such as inventory control, location tracking, remote application installation and remote data erase.

Consideration MC6 – Scan to Ensure Compliance

Organizations should consider solutions that have the ability to periodically scan corporate- and user-owned devices to ensure policy compliance.

Tech Consideration

Rationale: A solution such as this helps the organization ensure compliance and provides the potential to identify where user training has not been effective.

Consideration MC7 – Remove Privacy-Reducing Applications

Organizations should remove applications that they consider to be insecure or privacy-invasive prior to deploying organization-owned mobile devices.

Admin Consideration

Rationale: Many mobile devices are pre-populated by the vendor with multiple applications, some of which may introduce new privacy or security risks. Prior to issuing these devices to users, the organization should remove those applications from the devices.

See **Consideration MC14 - Evaluation and Maintenance of Approved and Restricted Applications**.

Consideration MC8 – Track Access to PHI on Mobile Devices

Organizations should consider mechanisms that will allow them to track and report access to PHI contained on the mobile devices.

Tech Consideration

Rationale: The ability to track and report on access to PHI is a custodial responsibility that enables the organization to respect information-access report requests from patients and to review access patterns to ensure legislative and policy compliance.

The mechanisms can include tracking built into the device operating system or the application used to perform the access. When accessing PHI remotely, the expectation is that the remote application will be able to provide an equivalent mechanism.

See **Privacy Requirement 18 – Logging Access, Modification and Disclosure**, **Security Requirement 41 – Logging Access to PHI in POS Systems** and **Security Requirement 46 – Reporting Every Access To A Patient/Person's EHR**.

Consideration MC9 – Consolidate Access Logs

Organizations should consider mechanisms to facilitate the consolidation of access logging information collected from mobile devices with that collected from more traditional applications and endpoints.

Tech Consideration

Rationale: The ability to account for all accesses to PHI is a custodial responsibility.

Location-Based Information

Consideration MC10 – Establish the Purpose for any Collection of Location Information

Where mobile devices have the capability to determine and record their location, organizations should consider the appropriate purpose(s) for which the collection of location information is warranted.

Admin Consideration

Rationale: See **Privacy Requirement 4 – Privacy Impact Assessments**

Consideration MC11 – Limit Collection of Location Information

Where mobile devices have the capability to determine and record their location, organizations should consider collecting only the minimum amount of information required to satisfy the legitimate purpose(s) for the collection.

Admin Consideration

Rationale: See **Privacy Requirement 6 - Limitation of Collection to Identified Purposes**. For example, the collection might be turned off during non-working hours or only collected when the location is owned or controlled by the organization.

Bring Your Own Device (BYOD)

Consideration MC12 – Establish Processes for Maintaining an Approved Device List

Organizations may want to consider establishing processes to evaluate BYOD devices and maintain a list of approved devices for users to review.

Admin Consideration

Rationale: Each mobile device and configuration will have a unique set of vulnerabilities that should be evaluated against the organization's criteria for acceptable devices. Publishing the list of approved devices gives users additional information that can be leveraged when they are choosing devices for themselves, potentially making the BYOD program more effective.

Consideration MC13 – Provide 'App Store' or Application Curation Functionality

Organizations may want to consider establishing one or more 'App Stores', where approved applications (in-house or third-party) may be downloaded and installed by users.

Tech Consideration

Rationale: An organization-managed set of approved applications helps to encourage the use of applications that specifically meet the organization's requirements for privacy and security.

Consideration MC14 – Evaluate and Maintain Lists of Approved and Restricted Applications

Organizations may want to consider evaluating applications and maintaining a user-accessible list of approved and restricted applications.

Tech Consideration

Rationale: By evaluating applications, the organization has an opportunity to determine how well an application meets its privacy and security requirements. Maintaining lists of applications that have been approved or rejected allows users to be better informed about the choices they make when considering publicly available applications for their mobile devices.

MDM solutions may offer the capability to restrict access to applications that can access confidential information if a rejected application has been installed on a device.

User Identity and Authentication

Consideration MC15 – Require the Use of Multiple Authentication Factors

Where mobile devices will be used to access confidential information, organizations should consider requiring users to provide multiple authentication factors when authenticating to the application that provides access to that information.[190]

Tech Consideration

Rationale: Organizations may find that the use of a password alone to ensure a user identity will be insufficient to access confidential information (See **Security Requirement 70 - Robustly Authenticating Users**). This is especially true when access is attempted from a mobile device, since a lost or stolen device can be subjected to numerous password attacks. Requiring an additional authentication factor helps to ensure that the claimed identity is legitimate. Examples of additional factors include: a one-time password from a security token (smart card), a Near-Field Communications (NFC) token or a voice print.

The minimum level of assurance requirement for mobile devices may be no different than accesses from more traditional endpoints. However, each mobile device may have differing support for the mechanisms implemented to meet those requirements. As a result, an organization that supports multiple devices may also need to support multiple combinations of authentication factors in order to robustly identify a user of a mobile device.

Many mobile devices provide four-digit Personal Identification Numbers (PINs) or pattern matching applications that result in less-robust authentication to the device. In keeping with their existing security policies, organizations will need to identify and select those authentication mechanisms that maintain an adequate level of

[190] *HIPAA Security Guidance* – U.S. Dept. of Health and Human Services, 2006-12-28, pg. 4-5

assurance for the classification of information that is being accessed.

Consideration MC16 – Integrate Mobile Devices into Identity-Management Infrastructure

Consideration should be given to integrating mobile devices into an interoperable identity infrastructure to allow the binding of an individual to a single identifier (single sign-on) regardless of endpoint device.[191]

Policy & Procedures
Admin Consideration

Rationale: Establishing the identity of the user with a reasonable level of assurance is a prerequisite to effective access control. Since most organizations already have well-defined identity-management solutions and practices, integration with those environments reduces complexity, implementation cost and the requirement for users to remember multiple identities. Please refer to **Section 5.3.4 – Federated Identity Management** for more information.

Consideration MC17 – Uniquely Identify the Individual Using a Mobile Device

Establish approved mechanisms that will allow the organization to uniquely identify the user of a shared mobile device, prior to granting access to confidential information.

Tech Consideration

Rationale: Native support for multiple identities on the majority of smartphones and tablets is only just beginning to be available. Organizations will have to determine what mechanisms are available for their target devices, recognizing that there is a trade-off between identity assurance and ease-of-use.

Organizations will need to ensure that they can reliably determine the identity of the person accessing confidential information via a mobile device. This may be accomplished by the user directly entering their credentials and/or some other means, such as bringing a proximity device (e.g. NFC, RFID) close to the mobile device.

[191] *The Roadmap for PbD in Mobile Communications* – Ontario Office of the Information and Privacy Commission, pg. 9

Access Control

Consideration MC18 – Configure Available On-Device Controls

Organizations should establish the set of technical security controls that need to be active on mobile devices that will have access to confidential information, and ensure that those controls are configured appropriately on each device prior to allowing access to the organization's networks and data.

Tech Consideration

Rationale:

While most modern mobile devices have the option of enabling multiple security controls, those controls are generally disabled by default. As part of the commissioning process for both organization-owned and user-owned devices, those security controls that the organization has adopted need to be configured.

Examples of controls that may be supported by a mobile device include:

- Passwords that adhere to the organization's password policy;
- Auto-lock after a period of inactivity;
- Remote wipe of all, or a portion of, the device contents; and
- Remote device locator.

Consideration MC19 – Protect PHI Stored on Mobile Devices

Organizations should use strong encryption techniques to protect PHI stored on mobile devices or restrict the use of mobile devices to providing only 'thin-client' capabilities to centralize applications for the collection or access of PHI.[192,193]

Tech Consideration

Rationale:

The Ontario Privacy Commissioner has issued orders that make the encryption of PHI on mobile devices a requirement in that jurisdiction. See also **Security Requirement 35 - Protecting Data Storage**.

[192] *The Roadmap for PbD in Mobile Communications* – Ontario Office of the Information and Privacy Commission, pg. 8

[193] Ontario Information and Privacy Commissioner of Ontario, *Order HO-004, March, 2007*

Consideration MC20 – Protect PHI on Lost or Stolen Mobile Devices

Organizations should use remote-erase mechanisms to minimize the impact of a lost or stolen device or on a device where access needs to be terminated.

Tech Consideration

Rationale: This technical control allows an organization to extend its reach in order to reduce the risk of unauthorized disclosure of PHI once a mobile device containing, or having access to, PHI has been reported lost or stolen.

See **Security Requirement 84 – Management of Incidents and Improvements**.

Consideration MC21 – Establish and Enforce Session Timeouts

When designing or acquiring mobile applications intended to access or store PHI, organizations should ensure that the application has the ability to enforce a mandatory session timeout when left unattended.

Tech Consideration

Rationale: While most organizations have an existing policy regarding session timeout for desktop applications, mobile devices may require different values. Each organization will need to determine an appropriate session timeout value based on the trade-off between the risk of unauthorized disclosure as a result of session timeout being too long, and the usefulness of the function if the timeout is too short. A value of 15 minutes, while not necessarily recommended, appears to be a common timeout value used by many organizations.

Will also depend on device/application capabilities. See **Security Requirement 71 – Restricting Access to Unattended Workstations**.

Network Security

Consideration MC22 – Ensure Communications Channel Encryption

Organizations should ensure that all mobile communications channels that transmit or receive confidential information are encrypted.

Tech Consideration

Rationale: Regardless of the communications technology employed, any channel used to communicate PHI should be encrypted using strong encryption algorithms and robust technologies.

See **Security Requirement 30 – Encrypting PHI During Transmission** and **Security Requirement 74 – Protecting Wireless Networks**.

Consideration MC23 – Disable Unused On-Device Network Services

Organizations should ensure that unused network services are turned off on mobile devices. Mechanisms to accomplish this include:

- User training;
- On-device applications that can monitor and control on-device networks; and
- Deployment of a Mobile Device Management solution to enable target timeout periods to be controlled.

Admin Consideration Tech Consideration

Rationale: Leaving networks open and active while not being used increases the number of paths that an attacker can use to extract information or gain access to the mobile device.

Consideration MC24 – Include Privacy and Security in Wireless Carrier Evaluations

When choosing a wireless carrier to provide services for mobile devices, organizations should evaluate the privacy and security policies and practices of the provider as part of the overall business evaluation.

Admin Consideration

Rationale: Since wireless carriers have the ability to push operating system software updates to the device and read information from the devices, they effectively have administrative capabilities for those devices. Organizations need to understand the privacy and security policies and practices of their carriers to ensure they meet the organization's requirements.

Agreements between the organization and the wireless carrier should reflect the organization's needs. See **Privacy Requirement 2 – Third-Party Agreements**, **Security Requirement 5 – Assessing Threats and Risks from Third Parties** and **Security Requirement 6 – Addressing Security in Third-Party Agreements**.

5.3.3 Remote Patient Monitoring

Remote Patient Monitoring (RPM) involves the application of technology to enable the monitoring and reporting of a patient's health data in the home or other non-clinical settings. The benefits of these programs include improved patient quality-of-life and better outcomes.[194]

This section includes those processes and technologies (i.e. devices and applications) that are prescribed and may be owned by a Health Care Delivery Organization (HDO) or third-party solutions that enable the collection and/or transmission of health information collected in non-clinical, patient-controlled settings to a central point for consolidation. The consolidation point is designated or controlled by the HDO.

In some cases, RPM devices may be considered 'medical devices'. Regulatory agencies in Canada and the U.S. have issued guidance based on medical device definitions, the intended purpose of products and the risks associated with the potential for the device or system to cause harm. The Food and Drug Administration (FDA) issued the *"Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff"* on September 25, 2013. This guidance explains the agency's oversight of mobile medical apps as devices and their focus on only the apps that present a greater risk to patients if they do not work as intended. Included are apps that cause smartphones or other mobile platforms to impact the functionality or performance of traditional medical devices. Specific considerations with regard to medical device licensing are outside the scope of this section.

The devices and applications mentioned above present a unique set of challenges, but are addressed as part of these considerations. Readers are also encouraged to refer to the mobile applications-related considerations in **Section 5.3.2 - Mobile Devices** of this document when evaluating RPM applications that run on mobile devices.

[194] Praxia, Gartner, *Telehealth Benefits and Adoption – Connecting People and Providers Across Canada*, Canada Health Infoway, May 30, 2011

This section addresses medical devices, as defined in the *Food and Drug Act,* as well as consumer devices and applications. There are considerations identified that address these two different categories of devices and applications.

Specifically excluded is a discussion of Telehealth, which integrates a number of technologies and approaches to provide a virtual clinical environment for both the health care delivery organization and the patient and is discussed separately in this document.

Technology

The components that make up the overall technology involved in enabling remote home health monitoring are:

- A sensor device – a device that collects physical or environmental data and communicates that data to …
- A monitoring application – an application running on a device located in the home that collects the sensor data (and optionally performs some local processing, including displaying information to the patient or caregiver) and forwards the data to …
- A central data-collection point – a centralized data-collection and management system (that the HDO has control over, either directly or via agreement) that collects the information sent by a monitoring application.

The sensor device and monitoring application may reside on a single physical device or may be separate (e.g., an activity-sensor linked with a mobile device application).

In the whitepaper on Remote Patient Monitoring[195], the Ontario Privacy Commissioner identified that transmission of data collected by remote monitoring devices can occur in one of two modes:

- Event-based – data is transmitted only when a specific event occurs, such as when a motion sensor is triggered or when a series of conditions in a network of sensors has been met (e.g., a motion sensor is triggered between the hours of 11:00 p.m. and 6:00 a.m.). The data that is transmitted may contain only the fact that the event occurred or it may contain additional information that more fully describes the event; or
- Continuous – data is analyzed and transmitted continuously. Usually these devices are worn by the patient or implanted. Examples include heart rate and blood pressure monitors.

[195] Cavoukian, A., *Remote Home Health Care Technologies: How to Ensure Privacy? Build it in: Privacy by Design*, Office of the Information and Privacy Commissioner of Ontario, November, 2009

5.3.3.3 Issues

Accountability[196]

In instances where RPM has been deployed, the HDO maintains its custodial responsibilities; however, the collection of PHI is no longer necessarily direct or in the HDO's sole control. As a result, accountability may be shared between the HDO and the patient and/or caregiver (e.g. family member).

In many cases, remote monitoring devices are operated by the patient or a caregiver rather than by a health care provider, resulting in the potential for increased risk of operator-introduced error. In these instances, questions arise as to whether there is shared responsibility and liability for the correct operation of the device and/or the integrity of the data collected and what each party's responsibilities are.

The HDO that is prescribing one or more remote monitoring devices has an obligation to ensure that adequate training is provided and understood before a patient or caregiver can be reasonably expected to shoulder any responsibility or liability.

The deployment, maintenance and lifecycle management of remote monitoring devices and applications are not necessarily performed by health care providers, and are outsourced much of the time. Nevertheless, the HDO still maintains an obligation to provide appropriate privacy and security training and to hold organizations, whether internal or third-party, to the same standard of patient confidentiality as the health care delivery organization.

Consent

Regardless of the mechanism used for the collection of PHI, an individual's wishes with respect to the handling of their PHI will most likely not be altered. Organizations are encouraged to ensure that devices and applications involved in RPM have functionality that enables them to interoperate with consent mechanisms established within in the EHR Infostructure (EHRi).

Some remote devices, especially continuously recording and embedded devices, may be so unobtrusive that the individual may not fully realize the extent of the health information that is being collected. Other devices may be capable of recording personal information of other household members. These people may need to be informed of that possibility and have their consent obtained.

[196] Tran K, Polisena J, Coyle D, Coyle K, Kluge E-H W, Cimon K, McGill S, Noorani H, Palmer K, Scott R. *Home telehealth for chronic disease management [Technology report number 113]*. Ottawa: Canadian Agency for Drugs and Technologies in Health, 2008, §7.2.1

Origin of Health Data

Knowing where and how health data is collected may be an important aspect of how a health care provider makes decisions regarding a patient's care plan. Without knowing the origin of health data, a provider will very likely assume that the information was collected directly from the patient by another health care provider. Understanding the origin of an observation gives a provider an opportunity to evaluate whether any additional risk to data integrity has been introduced via the collection source and mechanism, and whether or how to mitigate those risks.

5.3.3.4 Remote Monitoring Considerations

Accountability

Consideration RM-1 – Consider Defining and Communicating Patient and Organization Responsibilities

Organizations that deploy remote monitoring devices and/or applications will likely want to formally define and communicate the responsibilities and liabilities they are willing to accept and those they expect patients to accept. This may take the form of a formal agreement between the HDO and the patient.

Admin Consideration

Rationale: While organizations should ensure that the risk of patient-generated data-collection errors associated with any specific prescribed device or application is minimized (See **Consideration RM-2 – Consider Establishing Criteria during Device and Application Selection that will Tend to Reduce the Risk of Patient-Introduced Errors after Deployment**), there may be cases where those errors do occur. Patient-generated data integrity issues may be the result of such things as improper device calibration, improper environmental or patient conditions or other household members using the device.[197]

Where health data collection is outside of a direct provider-patient interaction, the current models of liability may not be wholly applicable and organizations may want to determine whether agreements may be needed to ensure that the HDO, any third party involved and patients all understand and agree to the risks involved.

[197] Tran K, Polisena J, Coyle D, Coyle K, Kluge E-H W, Cimon K, McGill S, Noorani H, Palmer K, Scott R. *Home telehealth for chronic disease management [Technology report number 113]*. Ottawa: Canadian Agency for Drugs and Technologies in Health, 2008, §7.2.1e, pg. 39

Consideration RM-2 – Consider Establishing Criteria during Device and Application Selection that will Tend to Reduce the Risk of Patient-Introduced Errors after Deployment

Organizations prescribing remote monitoring devices and/or applications should evaluate those devices and/or applications in part based on the likelihood of data errors being introduced as a result of user (patient and/or caregiver) error or misuse.

Admin Consideration

Rationale: This is directly related to **Consideration RM-1 – Consider Defining and Communicating Patient and Organization Responsibilities** and **Consideration RM-3 – Consider how to Ensure Comprehensive Privacy and Security Training Awareness is Provided for Individuals Prescribing, Deploying and Using Remote Patient Monitoring Technologies**. Minimizing the risk of erroneous data being collected as a result of operator error or misuse is an important criterion that should be included in any evaluation of remote home monitoring devices and/or applications.

One potential criterion to support this could be based on Health Canada device approval. Both Health Canada and the U.S. Food and Drug Administration (FDA) mandate mitigation of data integrity issues for certain classes of devices.

Consideration RM-3 – Consider how to Ensure Comprehensive Privacy and Security Training Awareness is Provided for Individuals Prescribing, Deploying and Using Remote Patient Monitoring Technologies

Organizations should evaluate the need to create or extend privacy and security training programs to include remote monitoring devices and applications and target staff, patients, caregivers and any third-party organizations that are involved in the deployment or lifecycle management of the devices and/or applications.[198]

Policy & Procedures

Admin Consideration

Rationale: An HDO's existing privacy and security training programs are normally focused on staff and information contained within the organization's boundaries. Remote home monitoring devices and applications may be new to many prescribers, patients or support personnel and appropriate use is not necessarily obvious.

Patient and caregiver awareness should address: proper use of the device and application; an explanation of the patient's responsibilities; and mechanisms to maintain privacy and security of personal information. Additional awareness topics related to privacy and security could include material that explains how to obtain any necessary support for the device or application, including how to report a lost or stolen device and what to do if the patient or caregiver believes the device or application has been tampered with.

[198] Tran K, Polisena J, Coyle D, Coyle K, Kluge E-H W, Cimon K, McGill S, Noorani H, Palmer K, Scott R. *Home telehealth for chronic disease management [Technology report number 113]*. Ottawa: Canadian Agency for Drugs and Technologies in Health, 2008, §7.2.1f, pg. 39

Consideration RM-4 – Consider Defining Roles, Responsibilities and Liabilities for all Participants Involved in RPM Deployment and Operation

When establishing an RPM program, organizations should identify all the participants (e.g., device manufacturer/supplier, RPM application provider, aggregator application provider, support provider, patient, household member, etc.) as well as their roles, responsibilities and liabilities.

Admin Consideration

Rationale: This is related to **Consideration RM-1-Consider defining and communicating patient and organization responsibilities – Consider Defining and Communicating Patient and Organization Responsibilities** and **Consideration RM-3 – Consider how to Ensure Comprehensive Privacy and Security Training Awareness is Provided for Individuals Prescribing, Deploying and Using Remote Patient Monitoring Technologies**. Identification of all participants allows the HDO to include them in the HDO's risk-assessment exercise.

Consideration RM-5 – Consider Embedding Confidentiality Requirements in Agreements

Organizations should ensure that all persons involved in the deployment, delivery or management of home remote monitoring solutions are bound by the same obligation of patient confidentiality.[199]

Admin Consideration

Rationale: The custodian maintains accountability for the protection of identifiable health and personal information, regardless of the role that an individual within the custodian's organization has or the organization they may sub-contract certain roles to. Employment agreements and service contracts should include clauses that make the obligation to protect PHI clear.

[199] Tran K, Polisena J, Coyle D, Coyle K, Kluge E-H W, Cimon K, McGill S, Noorani H, Palmer K, Scott R. *Home telehealth for chronic disease management [Technology report number 113]*. Ottawa: Canadian Agency for Drugs and Technologies in Health, 2008, §7.2.1g, pg. 40

Consideration RM-6 – Consider whether Agreement to Participate is Required

Organizations should determine whether obtaining agreements to participate from patients and possibly household members is required as a prerequisite to the deployment of an RPM device. The 'clinicalization' of the patient's home should be part of that determination.[200]

Admin Consideration

Rationale: An individual's awareness of being monitored may have negative impact on the health outcome desired and/or interpersonal relationships since the stress of 'being watched' may override any benefit of monitoring.

Identifying Purposes

No RPM considerations were identified; however, all of the privacy requirements identified in **Section 3.2 – Identifying Purposes for Collection, Use and Disclosure of PHI** still apply. Please refer to that section for privacy requirements as they may apply to remote health care monitoring.

Consent

Consideration RM-7 – Consider whether it is Appropriate for the RPM Device/Application to Support Privacy Preferences

Organizations should consider whether the ability of the device and/or application to support privacy preferences of individuals should be used as part of the selection criteria when evaluating remote health care monitoring devices and applications.

Admin Consideration

Rationale: Devices and applications that support privacy preferences can reduce the administrative effort required for custodians to comply with patients' wishes in respect of the PHI collected via RPM devices and applications.

Related considerations are **Consideration RM-12 – Evaluating Local Data Storage/Retention Risks** and **Consideration RM-13**

[200] Tran K, Polisena J, Coyle D, Coyle K, Kluge E-H W, Cimon K, McGill S, Noorani H, Palmer K, Scott R. *Home telehealth for chronic disease management [Technology report number 113]*. Ottawa: Canadian Agency for Drugs and Technologies in Health, 2008, §7.2.1c, pg. 38

– Limiting or Eliminating Transmission of PHI.

Consideration RM-8 – Consider Evaluating Device / Application Privacy Interoperability with EHRi Consent Mechanisms

Organizations should ensure device or application privacy preferences are interoperable with mechanisms that have been established in the EHRi.

PbD Feature

Admin Consideration

Rationale: If at all possible, monitoring devices and applications should be configured to adhere to an individual's privacy preferences as expressed in the jurisdictional EHRi. This will prevent potentially conflicting instructions and will effectively allow the individual's privacy preferences to be their default setting. The integration of Privacy by Design (PbD) principles as defined by the Ontario Information and Privacy Commissioner is considered a best practice.

Limiting Collection

No remote monitoring considerations were identified; however, all of the privacy requirements identified in Section 3.4 - Limiting Collection of PHI still apply. Please refer to that section for privacy requirements as they may apply to remote health care monitoring.

Limiting Use, Disclosure and Retention

Consideration RM-9 – Consider Mechanisms for On-Device and In-Application Retention and Secure Removal of Health Information

Organizations should evaluate the need for and mechanisms to ensure that health information residing on devices and in local applications is retained only as long as necessary and is subsequently removed securely, without requiring patient intervention.

Technology Consideration

Rationale: Health information retained on sensors and in local application stores presents a greater risk of unauthorized disclosure than information actively managed within an HDO's security perimeter. Once the information is no longer required in the monitoring locale (e.g., when the device is returned to the HDO), it should be securely removed from the device or application's data store.

Accuracy

Consideration RM-10 – Consider Mechanisms to Identify the Origin of Data

Organizations should evaluate whether and how to identify the origin of data for health information collected via a remote monitoring device, and link origin metadata with the health information.

Admin Consideration Technology Consideration

Rationale: There may be additional risks associated with data collected via remote home monitoring devices. This consideration allows providers making decisions based on data to take the source of the data into consideration.

Safeguards

Consideration RM-11 – Consider Including Device and Application Certification as Part of Selection Criteria

In selecting sensors and applications for remote health care monitoring, organizations should consider what certification(s) may be appropriate and desirable as part of their evaluation criteria.

Admin Consideration

Rationale: Certification from organizations such as Health Canada may be required or desired, depending on the intended use of the RPM device and/or application. The U.S. Food and Drug Administration has issued guidance on the types of devices and applications that they intend to regulate, using a risk-based approach. Organizations may want to review this guidance to help determine whether the risk associated with a class of device and/or application requires any further certification.

Regardless of certification criteria, organizations may want to consider developing a minimum set of security and privacy criteria for any devices selected for use in RPM.

Consideration RM-12 – Consider Evaluating Local Data Storage / Retention Risks

In selecting sensors and applications for remote health care monitoring, organizations should consider the benefits and risks associated with retaining PHI locally after transmission to a central collection point.

Admin Consideration

Rationale: Depending on the health attributes being monitored, it may be beneficial to retain health information on a device or application for the individual or their caregiver to monitor. However, the benefits of doing so should be weighed against any unmitigated risk to privacy that may result from the retention.

This consideration and **Consideration RM-10 - Mechanisms to Identify the Origin of Data** should be addressed together.

Consideration RM-13 – Consider Limiting or Eliminating Transmission of PHI

Health information transmitted from remote devices/applications to a central point should be completely and robustly de-identified.[201]

PbD Feature

Admin Consideration

Rationale: In many cases, only sensor readings and some unique, non-identifying attributes, such as the device identifier or unique application-generated identifier,[202] need be transmitted. Once it is at the central collection point and protected by the HDO's security controls, the data can be re-identified or associated with the identity of the individual.

Where the identity of the individual must be associated with health data at the point of collection, the dataset to be communicated should be robustly de-identified prior to transmission to the central collection point. The integration of Privacy by Design (PbD) principles as defined by the Ontario Information and Privacy

[201] Cavoukian, A., *Remote Home Health Care Technologies: How to Ensure Privacy? Build it in: Privacy by Design*, Office of the Information and Privacy Commissioner of Ontario, November, 2009, pg. 12

[202] Also referred to as a Persistent Anonymous Identifier (PAI)

Commissioner is considered a best practice.

Consideration RM-14 – Consider whether a Requirement Exists for Device/Application Support Organizations to aAccess Patient Identities

Organizations should attempt to eliminate any requirement for a device/application support organization, whether internal or external, to need personally identifiable information in order to provide support for an in-service device or application.

PbD Feature

Admin Consideration

Rationale: Registering and validating unique device and/or application instance identifiers for support purposes may be all that is required to ensure that the device is eligible for support (i.e., is a valid, HDO-supplied device and is covered for maintenance). Organizations should identify specific reasons why device/application support would require personally identifiable information for support purposes (See **Consideration RM-13 – Limiting or Eliminating Transmission of PHI**). The integration of Privacy by Design (PbD) principles as defined by the Ontario Information and Privacy Commissioner is considered a best practice.

Consideration RM-15 – Consider Establishing Lifecycle Management Processes for RPM Devices/Applications

Organizations should understand the entire lifecycle of the device and/or application and establish privacy-protection and secure lifecycle management processes in order to adequately protect health data held in the device or application.

Admin Consideration

Rationale: Each phase of the lifecycle should be examined to understand the potential privacy or security risk associated with the business process, and steps should be taken to mitigate those risks.

Openness

No remote monitoring considerations were identified; however, all of the privacy requirements identified in **Section 3.8 – Openness about Practices Concerning the Management of Personal Health Information** still apply. Please refer to that section for privacy requirements as they may apply to remote health care monitoring.

Individual Access

No remote monitoring considerations were identified; however, all of the privacy requirements identified in **Section 3.9 – Individual Access to Personal Health Information** still apply. Please refer to that section for privacy requirements as they may apply to remote health care monitoring.

Challenging Compliance

No remote monitoring considerations were identified; however, all of the privacy requirements identified in **Section 3.10 – Challenging Compliance** still apply. Please refer to that section for privacy requirements as they may apply to remote health care monitoring.

5.3.4 Federated Identity Management

This section includes an introduction to Federated Identity Management (FIdM) concepts and makes the case for FIdM in the Canadian health care environment. It identifies governance, policy and technology considerations that organizations or jurisdictions may want to take into account when establishing and operating an FIdM model. This topic is intended to have applicability to the issuance of digital identities to clinicians as well as consumers within the digital health ecosystem. The aspects of authentication and authorization as they relate to FIdM are also within scope of this section.

The technology used in FIdM is fairly well documented as it is used in many industries. Our research has highlighted the lack of guidance with regard to the administrative and governance aspects of FIdM in the health care sector. In order to provide the greatest value to readers, this section focuses on the administrative and governance aspects of implementing an FIdM solution.

The discussion includes business-specific identifiers (e.g. provider ID, client ID or PHN) only insofar as their relationship to establishing identity credentials. As each jurisdiction within Canada has implemented provider and client registries, any discussion of the management or operation of those identifiers or registries is not expected to add significant value and is deemed out of scope for this document.

The following are also considered out of scope for this topic since they are not directly related to a federation of digital identities:

- Identity Management Models that include the issuance of a single identity and credential; and
- Single-Sign-On technology solutions.

5.3.4.1 FIdM Definitions

Understanding FIdM requires basic knowledge of commonly used terms such as “entity”, “digital identifier”, “identifying information”, “identity service provider” and “relying party”. The following section provides the reader with a subset of the definitions used throughout this section of the document. It is highly recommended that the reader consult the Glossary at the end of this document for additional definitions of interest. The following definitions are based on the International Telecommunications Union (ITU-T x.1252). Please see the referenced document for a comprehensive set of definitions.

Assertion: A statement made by an entity without accompanying evidence of its validity.

(Entity) Authentication: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

> NOTE – Use of the term “authentication” in an identity management context is taken to mean entity authentication.

Credential: A set of data presented as evidence of a claimed identity and/or entitlements.

Digital Identity: A digital representation of the information known about a specific individual, group or organization.

Entity: Something that has separate and distinct existence and that can be identified in context.

> NOTE – An entity can be a physical person, an animal, a judicial/legal person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities.

Federation: An association of users, service providers and identity service providers. A *federation*, in this context, is a “group of organizations that trusts certain kinds of information from any member of the group to be valid.”[203]

Identification: The process of recognizing an entity by contextual characteristics.

Identifier: One or more attributes used to identify an entity within a context.

Identity: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management purposes, the term identity is understood as contextual identity or subset of attributes (i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts).

> NOTE – Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical

[203] A. Bhargav-Spantzel, A. C. Squicciarini, E. Bertino, *Establishing and Protecting Digital Identity in Federation Systems,* DIM '05 Proceedings of the 2005 workshop on Digital identity management – pg. 11-19, Association of Computing Machinery, 2005

issue and eludes any description and practical usage because the number of all possible attributes is indefinite.

Identity Management: Refers to the policies, processes and techniques involved in managing the lifecycle of digital identities and their associated attributes which are known in a particular security domain.

Trust: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately within a specified context.

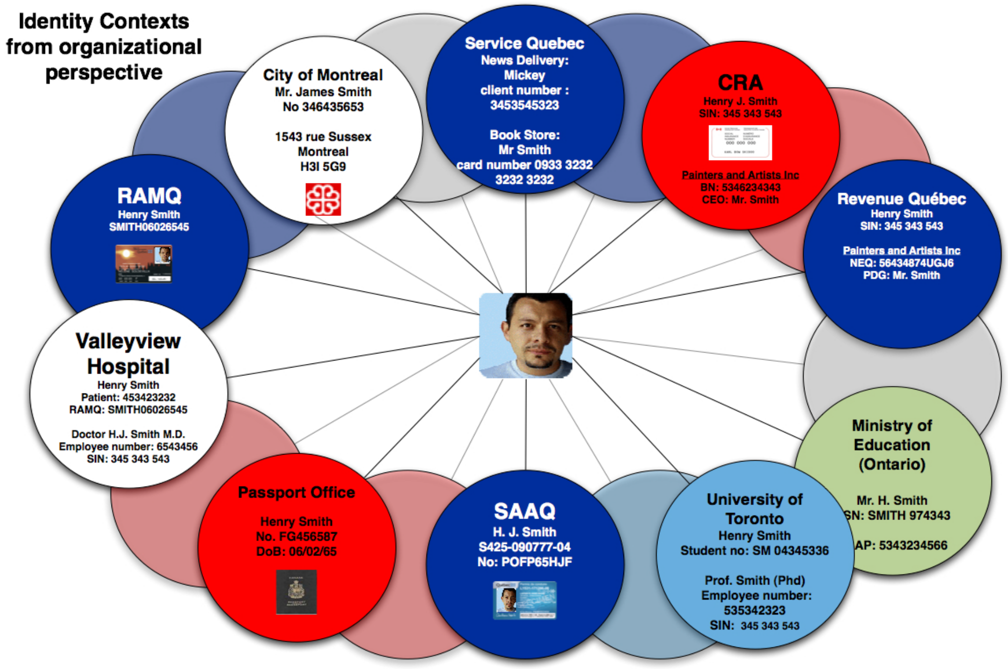
5.3.4.2 Digital identities

The following section is intended to be a brief introduction to the topic of identities and digital identities. It is generally recognized that individuals may have several identities in different contexts, such as a clinician, patient, consumer or employee. There are differing views in the IdM and authentication field as to whether a person should have one identity and multiple roles, or multiple and different identities depending on the context.

This is relevant when a person can have multiple digital identities, as is the case with many HDOs supporting several clinical and administrative applications. There is general consensus for the need to separate a person’s identity from a variety of potential contexts or roles. In addition to various identities, the level of assurance associated with the issuance and management of digital identities may vary based on the sensitivity of the information or information resources accessed. Different information and different processes may be required to identify and authenticate a person in different contexts (e.g., information necessary to identify or authenticate a social media user may not be sufficient or suitable to identify or authenticate a patient accessing their PHI via a Consumer Health Solution portal).

The following figure and text are extracted from the document entitled “*A Pan Canadian Strategy for Identity Management and Authentication*”. They provide an excellent summary of the concept of multiple identities and credentials.

> “This figure illustrates identity context from an organizational perspective in terms of the different ways one person may be known across contexts.”
>
> “It illustrates the different identities one person may legitimately have. In this example, Dr. Smith is identified one way by government institutions (e.g. his legal name, date of birth and Social Insurance Number) and another way in his professional life by the hospital he works for and by his patients. In his personal life, Dr. Smith is not known to his friends and family by his legal first name, Henry, but is instead known by variations of his middle name (James, Jim, Jimmy) or by a nickname. Dr. Smith also uses a number of pseudonymous identities on the Internet to conduct non-identified transactions.



The Identity Management Challenge

Health care organizations rely on multiple computer applications and mobile device apps to support their clinical and business processes. As traditional information systems did not have a requirement to share information or be interoperable, each system evolved with its own specific identity management capability whereby each system user has a unique digital identity and credentials (e.g. login ID and password) – potentially, one set of credentials for each clinical system, another for the organization's e-mail system and more still for each administrative system used, such as billing or scheduling. Therefore, each system has a separate IdM solution providing its own digital identity and credential issuance and management processes. The integration of mobile computing into the HDO with a multitude of mobile applications further compounds the problem. As clinicians adopt mobile health solutions and provide care from various locations outside an organization's boundaries, the challenge of managing a multiplicity of digital identities increases.

Having separate digital identities and credentials for each application results in increased privacy and security risks in addition to negatively affecting adoption of these systems. It becomes more difficult for users to remember the username and password for each of the applications they require access to and tends to encourage such behaviour as creating trivial passwords that are easy to guess, writing the credentials down and leaving them where they may be accessible by unauthorized persons or creating a 'do-it-yourself' SSO by reusing the same passwords for multiple digital identities.

Increased digital identity and credential administrative resources and errors are to be expected as an organization adds more applications to its portfolio. In a worst case scenario, an organization would have a separate IdM solution for each portfolio of applications, each with its own set of identity proofing, digital identity and credential-issuing processes and mechanisms. The integration of mobile computing may further compound the problem with a multitude of mobile applications. In the traditional organizational model, the owner of each application might establish a process that involves a centralized authority for the registration of users.

As clinicians become more mobile and provide care from various locations at differing HDOs, the identity challenge is further compounded. The need for clinicians to access relevant PHI when necessary from any location infers seamless access to that PHI. In order to meet new health care challenges, new clinical services and functionalities (e.g. remote patient monitoring, mobile devices) are being deployed, making traditional IdM models untenable. As regional and jurisdictional health care applications are conceived and implemented, the issue of establishing and maintaining identity information must be addressed. FIdM will most likely be driven by the seamless integration requirements of greenfield[204] health care solutions.

There is often confusion between the concepts of FIdM and SSO technologies, which the following paragraphs are intended to clarify. Please note that SSO technologies are outside of the scope of this section.

SSO technologies allow an IT system user to use one digital identity to access several e-health applications even though each application still requires a unique digital identity and credential. SSO technology maps the provided digital identity to several digital identities and credentials required by each application. This is typically viable within a single organization. To some degree, SSO technologies mitigate the irritants associated with users having to deal with multiple credentials for multiple applications within an organization. IT system users are only required to manage and remember one set of credentials. The solutions generally automate the process of scripting a system user's logon to individual systems and/or applications, saving time and user password fatigue. SSO solutions may also provide a centralized location for IT administrative and/or security staff to manage password compliance and reporting.

SSO technologies do not completely solve the identity challenge. SSO technologies only solve the multiple-password-and-digital-identity irritant for IT system users. They do not eliminate the redundant digital identity and credential administrative tasks. An IT system user still has several digital identities and credentials that must be managed and synchronized. SSO technologies typically do not provide a common set of authentication, identity issuance and management assurance levels since there is often no underlying trust framework. Therefore, SSO technologies typically do not allow systems across organizations to recognize an SSO-technology-managed digital ID and authentication scheme. This capability is a key feature of an FIdM model.

The Federated Identity Management (FIdM) Approach

Wikipedia defines FIdM as:

> "...having a common set of policies, practices and protocols in place to manage the identity and trust of IT users and devices across organizations. FIdM allows users to reuse electronic identities, saves administrators redundant work in maintaining user accounts and provides a consistent, trustworthy infrastructure component."

FIdM permits the portability of digital identities and credentials across the digital health ecosystem. From an identity and authentication perspective, clinicians from one organization can seamlessly access PHI, information services and clinical capabilities across HDOs, within or across jurisdictions, without the need for, or cost of, redundant user administration. FIdM can increase security and lower risk by enabling an organization to identify

[204] Greenfield solutions are entirely new e-health applications or services deployed within a jurisdiction

and authenticate a user once and then use that identity information across multiple systems, including other HDO or jurisdictional systems.

For example, a clinician would be able to register and enrol at one HDO. The HDO would perform the identity-proofing function in accordance with the FIdM Framework guidelines, which would include a validation with the appropriate jurisdictional licensing bodies and provider registries. The clinician would be assigned a digital identity and associated credentials to be used during the authentication process. The management of the clinician's identities and credentials would be performed by the issuing organization. A digital identity credential maps to one and only one entity; however, an entity may have more than one credential, just as it occurs in their personal life. Depending on the implementation, entities may be able to choose from multiple credentials within a single context depending on the activities that they wish to perform.

The clinician would be able to access applications, information services and clinical tools that are part of the federation with a single identity and credential. Additionally, if the clinician wished to access a home-care application or e-prescribing service offered by a cloud service via their mobile device, they would be able to do so using the same digital identity and credentials, provided this service is a member of the federation. This cloud service and home-care application would each be considered a Relying Party (RP).

FIdM is an enabler for the seamless integration of new capabilities and functionality in the digital health ecosystem by permitting the reuse of existing trusted identities and credentials for new applications and services.

The concept of federated identities and FIdM are also applicable to consumers wishing to access consumer health solutions and Personal Health Records (PHRs) that may be offered by an HDO. Consumers can access HDO portals from home computers and may also use HDO-developed mobile applications to access the same PHI and other services, such as e-visits. The use of federated identities and credentials applicable to both types of applications is a key adoption enabler.

5.3.4.4 Issues

While FIdM technologies and related standards are well understood, many of the implementation challenges are related to the complex nature of the digital health ecosystem. In order to realize the potential of FIdM, the following categories of issues should be given consideration by digital health solution strategists, decision-makers and enterprise privacy/security solution architects.

Governance

The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly and without the need for completely redundant user administration. Therefore, FIdM permits the portability of identity information across the digital health ecosystem, but requires trusted relationships between member organizations within the federation.

FIdM requires there to be a common set of standards, policies, practices and protocols in place to manage the identity and trust of IT users and devices across organizations. A governance authority is typically charged with establishing and maintaining such standards, policies, practices and protocols in addition to monitoring compliance. A governance structure must have the authority on behalf of member organizations to adopt or establish open industry standards and/or openly published specifications such that federation members can achieve interoperability and trust.

Trust, Security Models and FIdM Frameworks

Trust, Security Models and FIdM Frameworks defines a common set of capabilities that permit the establishment of trust relationships between parties involved in FIdM services.

Frameworks and models are standardized approaches that articulate the requirements, policies, mechanisms and procedures that allow one member organization to trust another's identity assertions. They define the different trust roles involved in assuring identity claims and issuing and accepting credentials. Trust models and FIdM frameworks should include standardized templates, language for trust agreements and processes on defining liability, decision making, auditing and compliance.

The creation of a formal security model is part of a process used to support the IT security of a business solution. A security model is derived from a security policy and subsequently informs the development of IT security requirements, specifications, design criteria and security solution development. It also serves as a basis for demonstrating compliance and conformity to security objectives. A security model for an FIdM solution will describe the expected behavior of the security components of the FIdM solution and, when implemented by member organizations, assist in establishing trust.

Privacy Protection

FIdM may have important implications for privacy. An FIdM solution may be privacy-invasive or enhancing depending on how the system is designed, implemented and operated. The creation of an identifier and its attributes to be used in an authentication system that creates transactional records and reveals an individual's online activities may have implications for privacy. In the context of consumer federated identities used in Consumer Health Solutions, there may be concerns over profiling and tracking when used in digital health solutions. If designed correctly, FIdM can improve privacy compliance by allowing the user to control what information is shared or by limiting the amount of information shared. The use of standard privacy risk-assessment tools, such as Privacy Impact Assessments, to understand how privacy can be impacted by various FIdM processes and technology solutions is critical. The integration of Privacy by Design principles as defined by the Ontario Information and Privacy Commissioner is considered a best practice.[205] An assessment of the applicability of each design principle is strongly recommended. Privacy of FIdM solutions should include the protection of personally identifiable information used to establish and manage an entity's identity. This includes data elements such as name, address and profession.

[205] http://www.ipc.on.ca/images/Resources/privacybydesign.pdf

Interoperability

In order for FIdM to permit the portability of identities and credentials across the digital health ecosystem, interoperability across member organizations is a fundamental requirement. Interoperability must be achieved at various levels, including processes, policies and technologies. Federations must agree on the use of identity federation standards that allow for semantic and syntactic interoperability, common authentication protocols and interoperability of FIdM services and solutions.

Governance

Consideration ID-1 – Consider Establishing an Effective Governance Structure that takes into Account Relevant Stakeholders

Organizations should establish an effective governance structure that includes all relevant stakeholders, including consumers where applicable.

Admin Consideration

Rationale: Consideration should be given to determining the organization(s) that would have the authority to set policies and processes with regard to the FIdM framework and operational aspects of the federation. The development of strategies to address potential structural and administrative barriers should be included in the governance structure. The establishment of an FIdM governance structure is critical to a successful implementation and adoption. The role of the governance structure would be to establish and maintain the roles and responsibilities of its members, standards, policies, practices and protocols.

The definition of a governance structure should include the ability to address structural and administrative barriers associated with using FIdM within the digital health ecosystem. Potential examples include:

- The limitations of digital health solutions to support new processes or authentication techniques;
- The various identity-proofing processes used by various HDOs across a Regional Health Authority; and
- Varying laws and regulations within or across jurisdictions.

The governance structure should also consider the definition and adoption of a common set of principles by which the federation will be governed. An example is the use of Privacy by Design principles.

The following is a set of FIdM principles identified by "*The Pan Canadian Strategy for Identity Management and Authentication*" that should be considered:[206]

Principle 1: Justifiable and Proportionate
Principle 2: Client Choice, Consent and Control
Principle 3: Limited Information for a Limited Use
Principle 4: Client-focused, Consistent Experience
Principle 5: Diversity of Identity Contexts and Systems
Principle 6: Trusted and Secure Environment
Principle 7: Transparency and Accountability
Principle 8: Enduring Solution

Consideration ID-2 – Consider whether Cross-Jurisdictional Sharing of Identity Information is Required

In the event that PHI is shared across jurisdictions, the FIdM governance authorities should determine whether sharing of identity data is also required.

Admin Consideration

Rationale: Depending on business requirements, PHI may be shared across jurisdictions. The security and trust models may require that authentication assertions also be shared between jurisdictions before sharing PHI. Should authentication assertions be required, federation governance authorities should determine if the sharing of identity information is required and under what conditions. This may be of particular importance when considering consumers accessing Personal Health Records via Consumer Health Solution portals. The assessment of potential legislative barriers should also be included.

Consideration ID-3 – Organizations should Consider Assessing any Potential Legislative Barriers to the Use of FIdM in the Digital Health Ecosystem

The assessment of potential legislative barriers with regard to the sharing of

Admin Consideration

[206] Inter-Jurisdictional Identity Management and Authentication Task Force, July, 2007, A Pan- Canadian Strategy for Identity Management and Authentication

personal information for the purpose of verifying and updating identification information between authoritative and relying parties should be assessed and, if required, addressed.

Rationale: Governance authorities should identify and address potential legislative barriers with regard to the collection and sharing of identity information or issuance of digital identities. Legislative frameworks may have certain restrictions with regard to the issuance of digital identities or sharing of identity information. The roles of Identity Service Providers and Relying Parties should be taken into account. The assessment should include the authority to act as an Identity Service Provider for both clinicians and consumers.

Consideration ID-4 – Consider Including Provisions for the Auditing of Member Organization Processes as Part of Federation Agreements

Federation agreements should include a provision for the auditing of a member organization's enrolment/registration process and resulting data. Results should be made available to the appropriate federation governance bodies.

Admin Consideration

Rationale: Member identity-proofing and associated processes should be auditable. Members should be able to investigate potential incidents upon request of other members within the federation. This capability is critical in determining potential liabilities and demonstrating compliance to federation standards and guidelines. Independent third parties should also be considered for attestation of compliance to minimum requirements.

Consideration ID-5 – Consider Developing Policies and Mechanisms that Require Regular Validation of Source Identity Information

The governance entity should develop policies that require member organizations to regularly validate source identity information used in the entity registration process.

Admin Consideration

Tech Consideration

Rationale: Certain data elements of identity information change over time, such as name and address. As this information is often part of the identity-proofing process, federations should give consideration to the policies and mechanisms to be implemented to ensure the accuracy of identity information. This may include regular validation of jurisdictional regulated professional repositories.

Trust Models, IDM Frameworks and Security Models

Consideration ID-6 –Consider Defining an FIdM Framework

An FIdM framework provides a comprehensive overview of an FIdM solution. The FIdM framework should be adopted by all member organizations.

Admin Consideration

Rationale: The development of FIdM frameworks will facilitate the establishment of trust models and assurance levels used by member organizations. The frameworks define a structured approach for the design, development, implementation and operation of all aspects of an FIdM. A framework will provide the foundation for the development of specific aspects of an FIdM solution, including detailed privacy, security and operational requirements, mechanisms and procedures. A framework will greatly facilitate interoperability between members of the federation since it will establish common requirements and capabilities.

The following components should be considered when defining a framework. For more details on each of the components, please consult the following documents: *ITU-T Y.2720*[207] and the *"Pan*

[207] ITU-T Y.2720 (01/2009) Series Y Global Information Infrastructure, Internet Protocol aspects and next-generation networks – Security NGN Identity Management Framework

Canadian Strategy for Identity Management and Authentication".[208]

1. Identity lifecycle management

   Identity lifecycle management includes the functions and processes required as part of enrolment, issuance and management of identity data and credentials.

2. Identity management operation, administration, maintenance and provisioning functions

   Relates to all functions and capabilities required to support the daily operations of an FIdM, including performance monitoring, security management and diagnostics.

3. FIdM identity functions

   Includes all functions that support identity-federation services (e.g. identity issuance, revocation, authentication assertions).

4. FIdM user and subscriber functions

   Functions and capabilities that allow the control and management of identity information by end users and subscribers. Includes delegation and consent functions.

5. FIdM performance, reliability and scalability

   Sets out requirements, service level agreements and procedures for performance and reliability of FIdM solutions.

6. FIdM security

   Functions and procedures for the security protection of FIdM systems.

7. FIdM legal and regulatory rules

   The set of laws, legislation, regulations and authorities

[208] Inter-jurisdictional Identity Management and Authentication Task Force, July, 2007, A Pan Canadian Strategy for Identity Management and Authentication

that govern identity management and authentication within respective jurisdictions.

For additional examples of FIdM framework components, readers are encouraged to consult the *"Pan Canadian Strategy for Identity Management and Authentication"*.

Consideration ID-7 – Consider Developing Guidelines for Identity-Proofing of Entities

The FIdM framework should include standards, policies, practices and protocols for identifying entities, including dependents, designates and delegates. It should include the minimum set of identity information necessary for enrolment of an entity, what information is recorded and how this information is to be protected. Also, the type of evidence required for verifying a relationship between the client and the dependent, designate or delegate should be considered.

Admin Consideration

Rationale: In order for member organizations to trust the authentication assertions of federation participants, common processes and policies with regard to identifying entities should be established. The scope of entities should include IT resources (e.g. servers), all care providers and staff, and consumers. The guidelines should consider delegation of authority within a clinical practice, whereby a regulated health care professional may delegate legal authority to a non-regulated health care professional (e.g. practice administrator or medical secretary).

Guidelines on acceptable registration channels, verification processes, evidence of identity and authentication factors would flow from this component.

Consideration ID-8 – Consider Addressing the Issues of Liability and Distribution of Risk as Part of the Federation Agreement

Federation agreements should include provisions that stipulate a member organization's liabilities and the overall distribution of risk that may arise from the mis-identification or incorrect authentication of an entity.

Admin Consideration

Rationale: The member organization’s risks and liabilities should be clarified as part of prudent business practices. This will facilitate adoption of federated identities across the digital health ecosystem.

Consideration ID-9 – The FIdM Framework should Consider Entity Identity Contexts

Entities (persons and organizations) may have different identities based on a given context. Therefore the FIdM framework should provide guidance on how to identify individuals, organizations and HDOs in varying contexts. FIdM solutions should support this capability.

Admin Consideration

Rationale: An entity’s identifier may change based on a given context, such as a clinician becoming a patient and using a CHS, which would require a context-specific identity. Entities may also have different identity attributes based on a given context. There are two categories of identity attributes:

- Tombstone attributes (date of birth)
- Transient attributes (name, address, profession)

The FIdM framework should take into consideration how it will manage the different contexts an entity will face and how the various identities will be managed in these contexts.

Consideration ID-10 – Consider Compliance with Common Procedures and Policies

Member organizations should be required to comply with a common set of procedures and policies as part of an overarching trust model.

Admin Consideration

Rationale: It is most likely that organizations currently issuing identity credentials have different processes to perform functions like identity-proofing and authentication. Some may vary within the same HDO. An example is the use of varying identity documents and identity-proofing processes. The use of common processes with regard to standardized identity attributes used to verify identities, along with a common trust and assurance model, will facilitate a uniform level of assurance and trust to be used by relying parties. This will facilitate trust between member organizations when relying on identity credentials.

Consideration ID-11 – Consider Development of a Formal FIdM Trust Model

Trust models define the requirements, policies and guidelines that permit the establishment of trust relationships among parties involved in FIdM services.

Admin Consideration

Rationale: The clear articulation of requirements, policies, mechanisms and procedures that allow one member organization to trust another's identity assertions is fundamental to the adoption of federated identities. Participants in the federation must trust a wide range of processes, mechanisms and policies used in issuing and managing identities, credentials and authentication assertions. A trust model defines the different trust roles involved in assuring identity claims and issuing and accepting credentials. It should include standardized templates, language for trust agreements and processes on defining liability, decision making, auditing and compliance.

Consideration ID-12 – Consider the Determination of Acceptable Source Documents and Verification Processes as Part of Federation Agreements and Frameworks

An FIdM framework and associated agreements should define acceptable source documents and verification processes to be used by member organizations.

Admin Consideration

Rationale: Trust between member organizations will in part be based on the level of assurance associated with the identity-proofing process. This process requires the validation of identity source documents and information. It is generally recognized that most issuing entities not part of a federation have varying processes and procedures for performing identity-proofing. The FIdM framework should establish common policies and procedures that specify the acceptable source documents to be considered as part of identity-proofing.

Security Models

Consideration ID-13 – Consider Development of a Minimum Set of Guidelines, Policies and Procedures for Authentication Assurance

Authentication assurance is the process of establishing confidence in the identities and claims presented to an information system. Identities and claims may have varying levels of assurance based on issuance processes, procedures and type of credentials used.

Admin Consideration

Rationale: The use of common policies and guidelines for the establishment of acceptable authentication levels is crucial to FIdM adoption and trust. Acceptable levels of authentication assurance allow the relying party to determine the level of confidence that an entity is that which is claimed. As an example, user IDs and passwords provide a lower level of confidence than biometrics. In other words, each replying party must trust the authentication assertions of member organizations based on a common set of requirements, guidelines and processes. Therefore, the establishment of authentication assurance levels should also take into account the robustness of authentication mechanisms and protocols specified in these policies and guidelines. Consideration should also be given to mechanisms that will communicate the level of authentication assurances to member organizations in order that they may make decisions about access to information resources based on the level of authentication assurance.

Consideration ID-14 – Consider Establishing Authentication Protocols for Use Among Member Organizations

Admin Consideration

Tech Consideration

Rationale: The use of common authentication protocols is necessary to meet levels of assurance and interoperability among member organizations. There are a multitude of standardized authentication protocols used, each providing various levels of assurance. Federation governance authorities must define the acceptable authentication protocols based on the required assurance levels and technical and operational concerns. Consultation with member organizations is recommended since clinical solutions may require adaptation to specified protocols.

Consideration ID-15 – Consider the Definition of Minimum Requirements and Specifications for Audit and Logging Capabilities to be Used by Member Organizations

Member organizations should consider use of common logging and auditing functions to facilitate trust relationships and to meet accountability obligations.

Admin Consideration

Rationale: A trustworthy FIdM ecosystem relies on the ability of its members to demonstrate accountability to the overall FIdM framework. Security logs play an important role in auditing and investigation of potential incidents and compliance. They also enable adherence to accountability requirements, protecting and appropriately using personal information, and providing notification to the appropriate systems or entities (e.g. identity owners).

Potential logging and auditing guidelines can include:

- Logging and auditing of IDM events such as access to identity information, unauthorized access attempts and changes to IDM information;
- Common data schemas for logging of FIdM-related activities to allow the sharing and linking of logs in order to facilitate incident investigations across the digital health ecosystem; and
- Harmonized capability of auditing tools to facilitate detection of non-compliance to applicable policies.

Consideration ID-16 – Consider Evaluating the Costs and Benefits of Various Auditing Infrastructures (centralized / distributed, federated / non-federated)

Organizations should assess the best approach to the various auditing and logging approaches in an FIdM ecosystem.

Admin Consideration

Tech Consideration

Rationale: In order for member organizations to meet their required accountability to the overall FIdM framework and trust model, an efficient logging and auditing capability must be deployed. Several architectural models can be considered, each with its advantages and challenges specific to each member organization. The core capability of using logging files to investigate potential incidents in a timely manner across the digital health ecosystem must be facilitated by the chosen auditing infrastructure model.

Privacy Protection

Consideration ID-17 – The FIdM Framework should Include the Definition of Privacy Requirements

The governance authority should analyze legislation that governs the privacy of personal information to identify privacy requirements for the FIdM framework. These requirements may include aspects of consent, notification, limits on use and authority to collect identifying information.

Admin Consideration

Rationale: The definition of privacy requirements is essential to the deployment of a privacy-protective FIdM solution for all federation participants. Privacy requirements should take into consideration the legislative obligations of applicable jurisdictions. Examples of privacy components to be considered include:

- Notification of use to individuals;
- Consent, for limiting collection, use and disclosure of identity

information; and

- Entity control of identity information, and accuracy, access and accountability.

The establishment of privacy requirements should lead to the development of privacy policies and guidelines for the FIdM solution.

Consideration ID-18 – Consider Implementing User-Centric Identity-Management Models and Technology

User-centric identity-management models allow users to control the transfer of their identity credentials from one digital health service to another.

Admin Consideration Tech Consideration

Rationale: User-centric identity-management models and technology provide enhanced privacy protection due to the ability of users to control the transfer of their identity credentials from one digital health service to another. The integration of user-centric identity-management models will allow entities to control the sharing of identity information. While this may be of lessor importance for clinicians, it is a critical privacy feature for consumers and patients.

Consideration ID-19 – Consider Allowing Entities the Ability to Exercise Control over the Identity Information Used in an FIdM Model

This capability speaks directly to how a user can control the personal information that an organization or federation maintains about them. Organizations and federations should identify what information they hold regarding subscribers/users and to what extent they can, or are willing to, provide user control over that information.

Admin Consideration Tech Consideration

Rationale:

This consideration supports basic privacy principles that allow an individual to exercise some control over their personal information. Organizations operating an FIdM solution should be fully transparent with entities with regard to what information is collected and what level of control an entity has over their personal information.

An example of ‘level of control’ would be to permit an individual to determine which personal information they are willing to share (e.g. e-mail address).

Consideration ID-20 – FIdM Solution Designers should Consider the Use of Meaningless But Unique Numbers (MBUNs) or Persistent Anonymous Identifiers (PAIs) as the Consumer Entity Identifier

The use of MBUNs/PAIs or a similar concept should be considered when defining requirements and designing an FIdM solution.

PbD Feature

Admin Consideration

Tech Consideration

Rationale:

The use of MBUNs/PAIs is one of the most important PbD features in an FIdM ecosystem.

Identity is socially constructed and contextual as we move across contexts. An entity’s identity differs when accessing social media versus a consumer health solution, for example. Therefore it is less of a privacy issue if an entity’s contexts cannot be re-constructed via a linkage of an individual’s various identities.

The linking of identifiers only at the time of usage by Relying Parties to specific contexts is the basic feature of MBUNs and PAIs.

Consideration ID-21 – Consider how the Collection of Personal Information for the Purpose of Identity Management will be Done in a Privacy-Protective, Secure Manner

The issuance and management of identities and credentials requires the collection of personal information. This information should be collected and stored in a privacy-protective and secure manner.

Admin Consideration

Tech Consideration

Rationale: While traditionally considered less sensitive than PHI, identifying information in the context of federated identities allows for the potential sharing of identifying information between member organizations. This sensitive information should be protected from unauthorized access that could lead to identity theft. The enrolment and registration processes for the issuance of identities and credentials should include the confidentiality of this information.

As a basic privacy principle, personal information should not be retained indefinitely. Therefore, consideration of the retention period for personal information should also be addressed as part of this activity.

Interoperability

Consideration ID-22 – Consider Establishing a Common Set of Terms or Lexicon for Use within the Federation

A common terminology and lexicon used by the federation is required to support interoperability and compliance among member organizations.

Admin Consideration

Rationale: The use of common terminology among member organizations will facilitate a common understanding of requirements and interpretation of policies and procedures. Common terminology will also assist in establishing adequate conformance and compliance to federation standards and guidelines. Where possible, industry-standard terminology should be leveraged.

Consideration ID-23 – Consider Adopting Interoperable Identity Credential Standards

Federation partners should adopt identity credential standards appropriate to the federation's requirements.

Policy & Procedures

Admin Consideration

Rationale: Organizations participating in an identity federation need to be able to understand and process credentials that are provided by federation partners. The interoperability of identity credentials is based on standards and protocols.

The evaluation and selection of well-established standards for this purpose reduces the cost and implementation time for each partner. Examples of IdM standards that facilitate interoperability are: *SAML V2, oAuth and OpenId*. The choice of an IdM interoperability protocol should be based on a risk assessment of the level(s) of assurance provided by the protocol.

Interoperability will be dependent on the use of standards that allow for semantic and syntactic interoperability of FIdM services and solutions.

5.3.5 Inter-Jurisdictional Health Information Sharing

The communication of health information over Canadian jurisdictional boundaries for the provision of care and secondary uses has been a reality for a number of years in every Canadian jurisdiction. For 2005-2006, approximately 2.3 million health care services were billed as a result of encounters with patients from other jurisdictions[209].

There are many instances where information is shared across boundaries, including out-of-province care delivery, federally administered programs, public health and many more.

Rather than attempt to encompass all scenarios that may involve the disclosure of PHI from one jurisdiction to another, the scope of the discussion that follows has been limited to:

[209] Canada Health Infoway, *Trans-jurisdictional Flows of EHR Data in Canada, v.2*, July, 2009, http://www2.infoway-inforoute.ca/Documents/Trans-Jurisdictional_Flows_of_EHR_Data_in_Canada_v2.pdf, pg. 14

- Transaction-based information sharing for events such as out-of-jurisdiction emergency care or a referral to a centre of excellence;[210]
- Discrete requests for specific or pre-arranged datasets; and
- The pre-authorized transfer of PHI for secondary uses such as public health.

Specifically excluded from this discussion are situations that involve the wholesale extraction and transfer of an individual's record from the EHRi as might be requested when an individual moves from one jurisdiction to another. Also excluded from this discussion is inter-jurisdictional access to health information by an individual via a Consumer Health Solution or Personal Health Record.

This topic leverages principles outlined in *Infoway's Common Understandings*[211] paper, which the reader is encouraged to consult, and includes foundational aspects[212] that explore:

- Support for privacy-protective disclosures of PHI between jurisdictions and the need to have legislation and/or policies that clearly authorize those disclosures;
- The need for governance structures in each jurisdiction to include privacy and information governance components that allow other jurisdictions to feel confident that any PHI disclosed to another jurisdiction will be handled and protected appropriately;
- The need for both the disclosing and collecting parties to meet their respective legislative and policy obligations;
- Each jurisdiction's need to meet its legislative requirements, while striving for pan-Canadian interoperability; and
- The recognition that once PHI has been disclosed to an organization in another jurisdiction, the PHI becomes subject to the collecting organization's jurisdictional information-handling, legislation and policies.

[210] Additional examples can be found in: Treasury Board Secretariat - CIO Branch/Canada Health Infoway - Emerging Technology Group, *Inter-jurisdictional Health Information Sharing - Whitepaper*, Sept, 2012

[211] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common understandings of the Pan-Canadian Health Information Privacy Group – Version 2.0,* July 31, 2012

[212] The foundational aspects identified here are not the complete set identified in the Common Understandings paper

5.3.5.1 Issues

Trust Models

The *Treasury Board of Canada* whitepaper[213] states:

> "Trustworthy inter-jurisdictional health information sharing is as essential as the information that will be shared. The foundations for trustworthy inter-jurisdictional sharing must be based on a common trust model framework which includes the managing of identities, access to health information and protecting the privacy of Canadians' Personal Health Information (PHI). For sharing to occur, the functioning system must be seen to be trustworthy by all stakeholders thereby encouraging adoption, meaningful use and participation."

Trust model frameworks normally include governance and policy areas, such as accreditation and/or certification requirements, risk and change management processes, policies and auditing, as well as technical components that include identity management, authentication and access control.

Governance

Accountability for the governance of inter-jurisdictional disclosures of PHI is discussed in the *Common Understandings* paper[214], while the Treasury Board whitepaper[215] identifies some of the governance issues.

Governance includes establishing authorities, roles and responsibilities as well as identifying authorities for such things as setting privacy and security standards between two or more jurisdictions within the context of inter-jurisdictional data sharing and establishing data sharing agreements that define the mechanisms for information sharing and the rights, obligations and remedies that each party has in regard to sharing.

Patient Identity Management

The ability to associate or bind an individual's identity with their personal information is a key requirement for patient safety as well as for maintaining a privacy-protective environment that includes an individual's measure of control over their PHI. At this point, every jurisdiction has implemented some form of Client Registry that enables the association to take place within the jurisdiction; however, as patient information flows between jurisdictions, issues associated with maintaining that binding between jurisdictions arise. Mapping patient identifiers between jurisdictions and Client Registry interoperability are two of the areas that may need to be addressed.

[213] Treasury Board Secretariat - CIO Branch/Canada Health Infoway - Emerging Technlogy Group, *Inter-jurisdictional Health Information Sharing - Whitepaper*, Sept, 2012, §6.4 – pg. 27

[214] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common understandings of the Pan-Canadian Health Information Privacy Group – Version 2.0,* July 31, 2012, §3 - pg. 64-65

[215] Treasury Board Secretariat - CIO Branch / Canada Health Infoway - Emerging Technology Group, *Inter-jurisdictional Health Information Sharing - Whitepaper*, Sept, 2012, §6.3 – pg. 24-26

Provider Identity Management

In any jurisdictional EHRi or system connecting to a jurisdictional EHRi, the positive identification of every provider accessing PHI is a requirement (See **Security Requirement 53 – Registering Users** and **Security Requirement 54 – Assigning Identifiers to Users**. How those identities are managed and communicated between jurisdictions will be a question that is impacted by the trust model established between partner jurisdictions. Will the provider be required to be authenticated directly to another jurisdiction or will the assertion that their home jurisdiction has authenticated them suffice?

Audit and Logging and Incident Investigation

Auditing, monitoring and logging of user activity involving PHI in Clinical Information Systems (CISs) supports accountability and helps to ensure these systems are compliant with the organization's privacy requirements.

Mechanisms to establish and maintain an audit log 'chain of trust' need to be identified when PHI is communicated across jurisdictional boundaries to ensure that audit records can be linked and shared across jurisdictions. The ability to perform this linkage is key to supporting breach protocols.[216]

Consent

No issues or considerations were identified in this work that have not been discussed in the *Common Understanding* paper,[217] which the reader is encouraged to review.

[216] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common understandings of the Pan-Canadian Health Information Privacy Group – Version 2.0,* July 31, 2012, pg. 34

[217] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common understandings of the Pan-Canadian Health Information Privacy Group – Version 2.0,* July 31, 2012

5.3.5.2 Inter-Jurisdictional Health Information Sharing Considerations

Governance

Consideration DS-1 – Consider Identifying Authority, Roles and Responsibilities for Privacy and Security

Jurisdictional partners should assess the need to establish where the authority and responsibility lie for establishing privacy and security policies and procedures that will guide the handling of PHI transactions between jurisdictions.

Admin Consideration

Rationale: Identification and agreement of roles and responsibilities ensures that accountability is maintained and privacy and security issues that are specific to the inter-jurisdictional transfer of PHI are addressed.

Consideration DS-2 – Consider Establishing Privacy and Security Interoperability Standards

Privacy and security interoperability standards may need to be established in order to enable the privacy-protective disclosure and collection of PHI from partnering organizations in other jurisdictions.

Admin Consideration

Rationale: In order for privacy-protective inter-jurisdictional data-sharing to be realized in electronic mode, privacy and security interoperability standards must be agreed to and implemented by all parties. Examples of such standards include the pan-Canadian Transport Level Interoperability specification and OASIS SAML.

Without privacy and security interoperability mechanisms in place, privacy-protective transfer of PHI will be a challenge due to inconsistencies between or among the parties involved.

In the absence of standards, numerous point-to-point connections and/or integration engines may be required, increasing implementation and operating costs and increasing security risks.

See also **Security Requirement 30 – Encrypting PHI during Transmission.**

Consideration DS-3 – Consider Establishing Data-Sharing Agreements for the Privacy-Protective Disclosure of PHI between Jurisdictions

Organizations involved in disclosing PHI to, and collecting PHI from, other jurisdictions should consider establishing data-sharing agreements that identify such things as:[218,219]

- Applicable law(s);
- Allocation of liability and risk;
- Privacy and security obligations;
- Permitted purposes;
- Duty to respond;
- Future use of data received;
- Duties of each party;
- Security and privacy breach protocols;
- Dispute mechanism(s);
- Retention and disposal of data; and
- Procedures for correction of data.

Admin Consideration

Rationale: The establishment of a data-sharing agreement is a mechanism to set out the legal obligations, understandings, dispute mechanisms and penalties that enable organizations to disclose PHI to organizations in other jurisdictions while maintaining their custodial obligations.

[218] This is by no means an exhaustive list of items to be considered

[219] Treasury Board Secretariat - CIO Branch / Canada Health Infoway - Emerging Technology Group, *Inter-jurisdictional Health Information Sharing - Whitepaper*, Sept, 2012, pg. 30

Identity Management

Consideration DS-4 – Consider how Patient Identities will be Managed[220]

Organizations should address whether and how patient identities will be resolved when transfers of PHI take place across jurisdictional boundaries.

Policy & Procedures

Admin Consideration

Rationale: Just as the process of accurately identifying patients is vital to patient safety and privacy, the need to identify and resolve any issues that may impact both sending and receiving jurisdictions' ability to identify patients is equally critical.

The majority of jurisdictions has implemented Client Registries using the pan-Canadian messaging standards; however, specific functionalities may differ because of jurisdictional extensions to those standards, and the particular version of a standard implemented may impact the overall interoperability of the solutions.

Organizations that are involved in inter-jurisdictional data-sharing may need to address what obligations each party has with respect to ensuring that identities, personal information (PI), and PHI that is received from another jurisdiction are correctly associated, and whether and how the management of identifiers will be coordinated between jurisdictions.

[220] Treasury Board Secretariat - CIO Branch/Canada Health Infoway - Emerging Technology Group, *Inter-jurisdictional Health Information Sharing - Whitepaper*, Sept, 2012, pg. 27-28

Consideration DS-5 – Consider how Provider Identities will be Managed[221]

Organizations should address whether and how provider identities will be resolved in transfers of PHI across jurisdictional boundaries.

Admin Consideration

Rationale: The trust model established will impact this consideration directly. In some cases, both the disclosing and requesting provider identities may be required to be directly identifiable by both parties. With other models, an identifier from a trusted assigning authority may be all that is required.

Auditing, Logging and Incident Management

Consideration DS-6 – Consider how Audit Trails will be Linked

Organizations should address how audit records associated with a given inter-jurisdictional transaction can be linked between interacting systems in order to provide a complete record of the transaction.

Admin Consideration

Tech Consideration

Rationale: The audit trail is required to provide accountability of user actions and is a legislative requirement in some jurisdictions. Without the ability to link audit records associated with a given transaction across jurisdictions, activities such as breach investigation and patient-access reporting is made much more difficult.[222]

This consideration may have both business process and technical aspects that should be addressed.

Consideration DS-7 – Consider the Alignment of Incident-Management Protocols

Organizations should review their privacy and security incident-management protocols to determine if any adjustment is required in order to align and coordinate with partners in other jurisdictions.

[221] Treasury Board Secretariat - CIO Branch/Canada Health Infoway - Emerging Technology Group, *Inter-jurisdictional Health Information Sharing - Whitepaper*, Sept, 2012, pg. 228

[222] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common understandings of the Pan-Canadian Health Information Privacy Group – Version 2.0,* July 31, 2012, pg. 45

Rationale: Inter-jurisdictional sharing of PHI will require the coordination of incident-management protocols, procedures and overall capabilities. This gives data custodians the ability to maintain accountability with regard to their obligations.

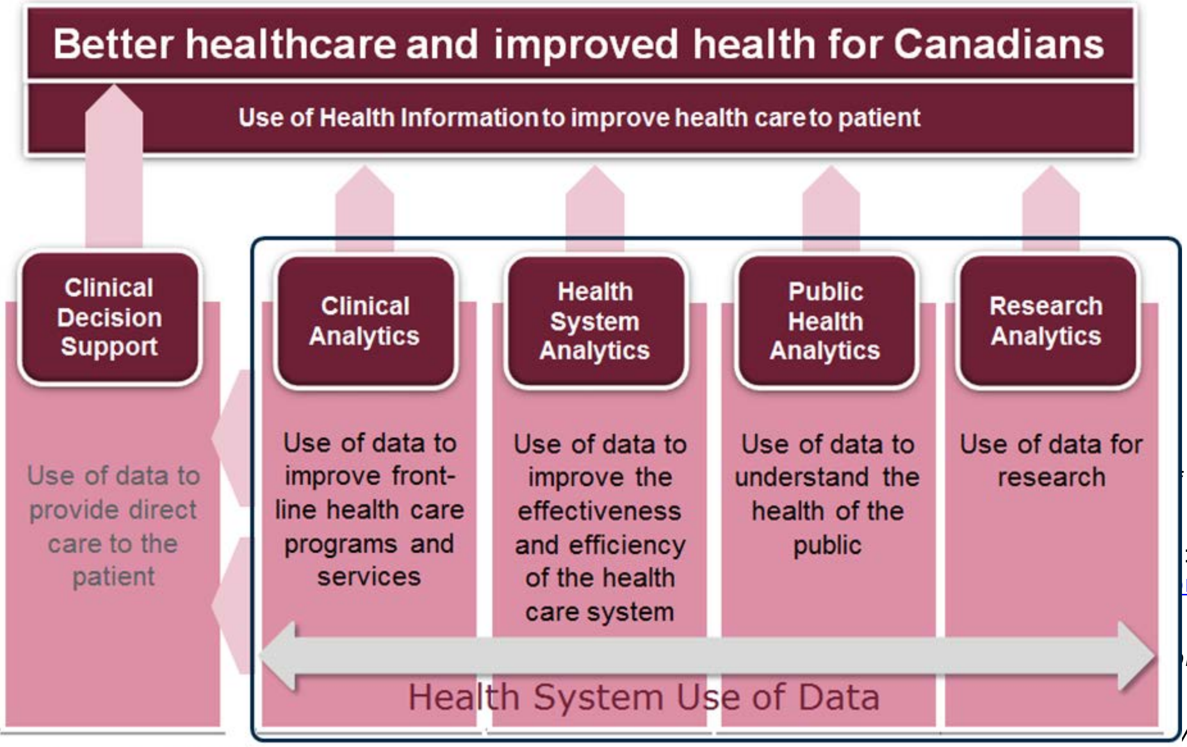
Consent

No inter-jurisdictional considerations within the identified scope were found that have not been addressed in the *Infoway Common Understandings* paper.[223]

5.3.6 Secondary Use

Secondary Use refers to the "utilization of health information for any purpose other than the provision of direct care and treatment"[224]. The concept has also been called 'Health System Use' (HSU)[225]. Secondary Use applications primarily use data collected for the provision of care to support such activities as clinical analytics, health system monitoring, quality improvement, public health and health research[226]. These applications include, but are not limited to: data warehousing, data mart, analytics and decision support software.

Figure 6 illustrates categories of information processing for secondary use as outlined in *Infoway's* Health Analytics in Canada presentation[227] .


Better healthcare and improved health for Canadians
Use of Health Information to improve health care to patient
Clinical Decision Support
Use of data to provide direct care to the patient
Clinical Analytics
Use of data to improve front-line health care programs and services
Health System Analytics
Use of data to improve the effectiveness and efficiency of the health care system
Public Health Analytics
Use of data to understand the health of the public
Research Analytics
Use of data for research
Health System Use of Data

Note: Health care data is also used to support other uses of data required as permitted by law, such as ensuring food safety and complying with regulatory and medical certification requirements.

Figure 6. Health System Use Categories of Analytics – source: Canada Health Infoway, Health Analytics in Canada presentation, *May 2013*

[223] Ca *the Pan-Canadian*
Health

[224] Ca *f the Pan-Canadian*
Health

[225] Ca : https://www.infoway-
inforo r-health-system-use-of-
data-i

[226] Ca *nalities – Win/Win,*
March

[227] Ca */-in and Creating Value*
from t

Figure 6 refers to different types of analytics (clinical analytics, health system analytics, etc.) The term *analytics* includes activities associated with accessing and analyzing data, such as data warehousing, business intelligence and big data analytics. Secondary use is enabled by the ever-growing digitization of health data and processed by analytics ranging from small data sets to large, from structured data to free text processed by natural language processors.

Gartner defines a "Data Warehouse" (DW) as "a storage architecture designed to hold data extracted from transaction systems, operational data stores and external sources. The warehouse then combines that data in an aggregate, summary form suitable for enterprise-wide data analysis and reporting for predefined business needs."[228]

Gartner also defines "Business Intelligence" (BI) as "an umbrella term that includes the applications, infrastructure and tools, and best practices that enable access to and analysis of information to improve and optimize decisions and performance."[229]

Canada Health Infoway uses the term "Big Data Analytics" to mean functions that "handle open ended "how and why" type questions, whereas BI tools are designed to query specific "what and where" and process mostly structured data to find patterns. DW systems process mostly structured and mostly aggregated data."[230]

The goal of Secondary Use is to apply all of these techniques (and more) where appropriate to provide improved insight and decision-making in clinical programs and services, the overall health system, public health and health research.

5.3.6.1 Issues

A discussion of issues and principles for Secondary Use in Canada is also outlined in *Infoway's Privacy and EHR Information Flows in Canada – Common Understandings of the Pan-Canadian Health Information Privacy Group, Version 2.0*, available at https://www.infoway-inforoute.ca/index.php/resources/reports/privacy/doc_download/626-privacy-and-ehr-information-flows-in-canada-version-2-0.

De-identification

Since some of the downstream use of health data does not require identifiable information, sending that data with direct or indirect identifiers removed or in aggregate form alleviates much of the risk of a privacy

[228] http://www.gartner.com/it-glossary/data-warehouse. Accessed 2013-09-10

[229] http://www.gartner.com/it-glossary/business-intelligence-bi. Accessed 2013-09-10

[230] Canada Health Infoway, *Big Data Analytics in Health – White Paper (Full Report)*, April, 2013, https://www.infoway-inforoute.ca/index.php/resources/technical-documents/emerging-technology/doc_download/1419-big-data-analytics-in-health-white-paper-full-report

breach from secondary-use activities[231]. Other secondary uses do require the ability to link records from the same patient or to re-identify individuals based on a certain event or result (e.g. public health). In these cases, some form of re-identification of the record must be possible. When re-identification is possible, additional security measures should be considered, including procedures that dictate no data aggregation with other sources of data, limiting disclosure or the encryption of re-identified data while in static storage.

HSU relies heavily on robust de-identification techniques[232] in order to provide a balance between patient privacy and utility of health data for multiple uses.

Data elements used for secondary purposes should be kept to a minimum to limit the risk of re-identification and impact of inappropriate disclosure. An analysis of requested data elements should be performed to ensure they are necessary to achieve the proposed objective of the secondary use.

Studies have shown that while de-identification done poorly can, and has, resulted in privacy breaches, robust de-identification techniques implemented properly[233] provide an effective mechanism for protecting patient privacy.[234]

Notice

The majority of health privacy legislation in Canada provides for information collected during the provision of care to be used and disclosed for other authorized purposes.

As the capabilities of analytics progress, there may be perfectly valid uses that arise that were not contemplated when the information was collected, or when it was de-identified and transferred to a larger health data pool. Providing patients with adequate notice of future potential uses at the point of collection gives them the ability to understand where their information may be accessed and is key to engendering patient trust in secondary-use processes.

Big Data Analytics

One of the challenges that Big Data Analytics helps to solve is the evaluation of ‘unstructured data’. Wikipedia defines unstructured data as “data that does not have a pre-defined data model and is not organized in a pre-defined manner”. As the capabilities to interpret very large amounts of data increase, the potential for analysis of unstructured data or linking of previously unlinkable data becomes a risk for the re-identification of de-identified data.

[231] Canada Health Infoway. *Privacy and EHR Information Flows in Canada – Common Understandings of the Pan-Canadian Health Information Privacy Group Version 2.0*, July 31, 2012, pg. 41

[232] For a review of de-identifcation techniques, see Fraser, R. and Willison, D., *Tools for De-Identification of Personal Health Information*, September, 2009, http://www2.infoway-inforoute.ca/Documents/Tools_for_De-identification_EN_FINAL.pdf

[233] K. El Emam, E. Jonker, L. Arbuckle, B. Malin: “*A Systematic Review of Re-identification Attacks on Health Data.*” In PLoS ONE 6:12: e28071. DOI:10.1371/journal.pone.0028071, 2011

[234] Cavoukian A., *Looking Forward: De-identification Developments – New Tools, New Challenges,* Office of the Information and Privacy Commissioner of Ontario, May, 2013, *pg.1* http://www.privacybydesign.ca/content/uploads/2013/05/de-identifcation-developments.pdf

The reader is encouraged to review the *Infoway* Emerging Technology Group's *Big Data Analytics in Health – White Paper (Full Report)* available at https://www.infoway-inforoute.ca/index.php/resources/technical-documents/emerging-technology/doc_download/1419-big-data-analytics-in-health-white-paper-full-report for a full discussion on the benefits and risks of Big Data Analytics.

The reader is also directed to *Looking Forward: De-identification Developments – New Tools, New Challenges,* Office of the Information and Privacy Commissioner of Ontario, May 2013, available at http://www.privacybydesign.ca/content/uploads/2013/05/de-identifcation-developments.pdffor a discussion on some new mechanisms and challenges in de-identification techniques, some of which are directly related to Big Data.

Governance and Accountability

Governance for Secondary Use may include different stakeholders and roles than those established to provide governance of health systems whose focus is provision of care. Governance for Secondary Use may include providing direction for topics such as de-identification and considering the privacy and/or security impacts of emerging techniques (e.g. Big Data Analytics).

The governance model should include an approval body. As mentioned earlier, assessment of data, approval for use of data and guidelines on the protection of the data should be considered in order to ensure the protection of PHI throughout the secondary-use process. Entities may also wish to ensure retention and data deletion details are included in the consent and secondary-use activities.

5.3.6.2 Secondary Use Considerations

De-Identification

Consideration SU-1 – Consider where De-identification and/or Anonymization is Performed

Organizations should determine the practicality of performing robust de-identification or anonymization of PHI as close to the data source as possible.

Admin Consideration

Rationale: While de-identified data always has the potential for re-identification, a robust[235,236], source- or near-source-controlled mechanism to transform PHI into de-identified data and/or anonymized data, may have the potential to reduce system-wide operational costs and may reduce privacy and/or security risks.

Organizations should consider limiting the number of personnel that have access to the identifiable data, including a defined procedure with specified accountable personnel. The procedure may include a segregation of duties, where the collection of de-identified data is separate from the role of re-identification approval.

The use of cryptography for de-identification has shown to be robust and can significantly reduce the risk of unauthorized re-identification when used appropriately. The use of appropriate cryptography can also facilitate the secure re-identification of health information when necessary.

In a 2013 publication, Ontario's Information & Privacy Commissioner states that

> *"De-identification is a valuable tool in that it enables the protection of individual privacy and drastically reduces the risk that personal health information will be used or disclosed for unauthorized or malicious purposes, while also complying with data minimization practices and enabling the information*

[235] Privacy Analytics Whitepaper: *De-identification Maturity Assessment*, http://www.privacyanalytics.ca/wp-content/uploads/2013/07/DMM.pdf

[236] Canadian Institute for Health Information, *'Best Practice' Guidelines for Managing the Disclosure of De-Identified Health Information*, October, 2010

to be used for authorized secondary purposes."[237]

Consideration SU-2 – Consider Selecting Mechanisms for De-identification Based on Re-identification Risks

When selecting a mechanism for de-identification, organizations should first identify the likelihood of information being re-identified and the risk associated with that likelihood.[238]

Admin Consideration

Rationale: While the focus of the *Common Understandings*[239] paper is on trans-jurisdictional flows, three of the understandings related to this consideration are appropriate whenever information is disclosed for secondary use:

- In general, information to be used for secondary use should be disclosed in aggregate or de-identified form (Common Understanding 37);
- organizations and individuals responsible for handling disclosure requests associated with HSU should have current, in-depth knowledge regarding de-identification tools and techniques and have the ability to apply them (Common Understanding 39); and
- De-identification techniques should work hand-in-hand with risk-assessment processes, agreements and safeguards (Common Understanding 40).

This consideration makes the assumption that a robust risk-assessment program is in place (see **Consideration SU-3 – Consider which Risk-Assessment Tools are Appropriate** below).

[237] Cavoukian A., *Looking Forward: De-identification Developments – New Tools, New Challenges,* Office of the Information and Privacy Commissioner of Ontario, May, 2013, *pg.1* http://www.privacybydesign.ca/content/uploads/2013/05/de-identifcation-developments.pdf

[238] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common Understandings of the Pan-Canadian Health Information Privacy Group Version 2.0*, pg. 42, July 31, 2012

Risk Assessment and Mitigation

Consideration SU-3 – Consider which Risk-Assessment Tools are Appropriate

In order to ensure that only authorized and appropriate users have the ability to access PHI or potentially re-identifiable data, organizations should ensure they perform a risk assessment and identify a range of mitigation controls.

Admin Consideration

Rationale: In addition to using robust de-identification techniques, organizations should identify a range of risk-assessment and mitigation techniques[240].

There may be little difference between the obligations, risks or techniques used within the EHRi and those used in an HSU repository that contains de-identified information.

Organizations should consider which mechanisms and approaches are to be used in risk identification. The use of automated tools that will calculate probability of re-identification should be used in the risk-assessment process.

Consideration SU-4 – Consider the Use of Data Flow Mapping Techniques

Where multiple data sources are collected into repositories, data flow mapping techniques that examine flows from multiple data sources into one or more repositories should be used to determine the applicable privacy and security controls to apply and the most appropriate place(s) to apply them.

Tech Consideration

Rationale: Secondary Use information can come from many sources, including, but not limited to:

- Public health;
- Primary Care;
- Specialists;

[240] K. El Emam, "*Risk-based health data de-identification*" In IEEE Security and Privacy, 8(3):64-67, 2010

- Pharmacists;
- Laboratories;
- Diagnostic Imaging Centres;
- Emergency Rooms;
- Hospitals;
- Electronic Medical Record systems in GP clinics;
- Long-Term Care Homes; and
- Community Programs.

Each of these may supply different types/classes of PHI, some more sensitive to an individual than others. Information may flow through, or be consolidated at, a number of points before a particular use is realized. With complex flows of information such as these, it will be important to evaluate privacy and security risks and controls as each new source of information is added (see **Consideration SU-3 – Consider which Risk-Assessment Tools are Appropriate**).

Consideration SU-5 – Consider Evaluating Risks Associated with Analysis of Unstructured Data

Organizations should identify the privacy and security risks associated with processing unstructured data and determine whether additional control measures are required when the analysis of that data is being considered.

Admin Consideration

Rationale: Currently, there is no guarantee that unstructured data will not contain identifiable data (PHI). For example, PHI might be found in narrative form in a notes section of a clinical document or in a scanned report that had been processed by optical character recognition (OCR) software to extract content from it.

For research, a Research Ethics Review of the project may be appropriate, while jurisdictions may rely on existing data stewardship policies and practices.

For Secondary Use other than research, jurisdictions and others who may be involved may need to review and extend rules for using unstructured data if they find existing protocols inadequate for this type of data analysis.

Monitoring and auditing of analysis projects using unstructured data would also provide insight into any additional protective measures that may be required.

Consideration SU-6 – Consider Establishing Mechanisms to Reduce Small-Cell-Size Impacts

Organizations participating in any form of analytics need to consider which mechanisms should be put in place to prevent or reduce the likelihood of users being able to infer the identity of an individual returned from a query as a result of the small size (few observations) of the returned result.[241]

Admin Consideration

[241] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common Understandings of the Pan-Canadian Health Information Privacy Group Version 2.0*, July 31, 2012, pg. 41

Rationale:

When there is only a small number of observations in a summary table or information query result, organizations should consider the minimum number of observations that need to be in a cell of the table to avoid running the risk of providing an unintended pathway to re-identification.[242]

Results that are based on age tend to have few individuals at the extremes, and without some modification to identify age ranges, it may be very easy to identify the health condition of, for example, the 102-year-old man living in a small town since he may be known simply by being the oldest person in town.

Consideration SU-7 – Consider Re-evaluating Security and Privacy Controls Based on Purpose(s) of Use

Identify whether additional technical and/or administrative controls are needed in order to limit access to, or use of, PHI and/or health information; and consider if the controls should vary depending on the requestor's intended use(s) for the data.

Admin Consideration

Tech Consideration

Rationale:

The basic privacy principle of limiting access to the use and disclosure of PHI may take the form of administrative and/or technical controls. In the context of Secondary Use, the orginal purpose for collection and use of PHI may change over time. As purposes for the use of PHI evolve, organizations should re-assess the appropriateness of the original privacy and security controls. This may be done as part of a Privacy Impact Assessment (PIA).

[242] International Organization for Standardization, *Health Informatics – Deployment of a clinical data warehouse,* ISO/TS 29585:2010, §5.7.9

Patient Notice

Consideration SU-8 – Consider the Development of Policies which Balance Patient Privacy and Appropriate Sharing of Information

Ensure that policies are in place to facilitate and encourage the appropriate sharing and use of information for secondary use while maintaining patient privacy.[243]

Admin Consideration

Rationale: The *Common Understandings* paper states:

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

While the quote deals with transjurisdictional requests, the same statement can be made with respect to all requests for disclosure of PHI or de-identified information for secondary-use.

Organizations should consider limiting use, via agreement between releasing and receiving parties on what the information will be used for, how it will be used, manipulated and disclosed, and the retention period. Agreements can include clauses to ensure data is not to be aggregated with any other data, ensuring the level of re-identification does not change.

[243] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common Understandings of the Pan-Canadian Health Information Privacy Group Version 2.0*, July 31, 2012, pg. 43

Consideration SU-9 – Consider Logging Disclosures of PHI and De-identified Information

Organizations should consider enabling logging from their information systems of all disclosures of PHI as well as of data in de-identified form in order to provide an audit trail for patient-access requests or for privacy or security analyses.[244]

Admin Consideration

Rationale: A significant determinant of the success of secondary use programs will be how comfortable patients are with their personal health information being disclosed for purposes not related to their direct care. Being able to provide patients with information that identifies specifically who their information was disclosed to and why it was disclosed will help in continuing to build trust in the system[245].

Where possible, logging disclosures of de-identified (and re-identifiable) data provides a more complete picture to patients of where their information has been sent, and should also give them with confidence that measures were taken to protect that information.

[244] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common Understandings of the Pan-Canadian Health Information Privacy Group Version 2.0*, July 31, 2012, pg. 31, 46 (Common Understandings 25 and 45)

[245] *Ibid*, pg. 31 (Common Understanding 25)

Consideration SU-10 – Consider a Policy Permitting Patient-Access Requests Regarding which Part of their EHR has been De-identified for Secondary-Use

Policies should be developed and made publicly available that specify whether the organization can honour a patient's request for information regarding which part of their record has been de-identified for secondary purposes.[246]

Admin Consideration

Rationale: Organizations will have to determine what their obligations are in this regard as there is always a risk, however small, that de-identified information may be re-identified. A patient should be able to get general information about who has access to the de-identified information and for what purpose.

If an organization determines that it will not provide detailed access information for de-identified data to a patient, it should consider providing notice that identifies the type of secondary uses that patient data in de-identified form may be subject to[247]. See **Consideration SU-11 – Consider Providing Notice that Includes Discussion of Secondary Uses**.

Consideration SU-11 – Consider Providing Notice that Includes Discussion of Secondary Uses

Organizations that collect patient information that will be made available for secondary-use need to ensure that patients have an opportunity to understand how their health information will be used in a privacy-protected way and what their rights are with respect to those uses.[248]

Admin Consideration

Rationale: See also **Consideration SU-10 – Consider a Policy Permitting Patient-Access Requests Regarding which Part of their EHR**

[246] International Organization for Standardization, *Health Informatics – Deployment of a clinical data warehouse,* ISO/TS 29585:2010, §5.7.9

[247] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common Understandings of the Pan-Canadian Health Information Privacy Group, Version 2.0*, July 31, 2012, pg. 44

[248] *Ibid*, pg. 24-25, 45

has been De-identified for Secondary Use.

Notice should include indication of Research Ethics Board approval, and/or consent of the individual, where required, to provide approval for release of data for secondary-use.

Consideration SU-12 – Consider how to Address Familial and/or Household Data-Linking Issues

Organizations need to identify and, if required, address issues related to familial and/or household data linking.

Policy & Procedures

Admin Consideration

Rationale: Having the ability to identify familial and/or household linkages can be a great benefit to certain classes of studies; however, those linkages can render de-identified information easier to re-identify. Organizations will need to determine an appropriate balance between the increased privacy risk and the increased utility of the information.

After assessing legislative and regulatory requirements in their jurisdictions, organizations can make a policy decision around whether, how and from whom to seek consent as it relates to identifiable information when data-linking is desired.

Governance and Accountability

Consideration SU-13 – Consider the Authority, Roles and Responsibilities of all Stakeholders

In planning repositories to be used in supporting secondary-use (e.g. data warehouses or data marts), all stakeholder groups should be identified, their roles determined, authority understood and their involvement sought.[249,250]

Policy & Procedures

Admin Consideration

Rationale: Each stakeholder group may have a different perspective on privacy and security as it relates to repositories intended for secondary-use.

[249] Canadian Institute for Health Information, *Better Information for Improved Health: A Vision for Health System Use of Data in Canada. Ottawa, ON: CIHI, 2013.*, pg. 13-14

[250] Canada Health Infoway, *Inter-Jurisdictional Health Information Sharing White Paper, Sept. 2012, pg 27*

Consumers of health data will no doubt be focussed on access to information, while patients and information providers or custodians may have more of a focus on protecting information. Identification of each of these groups, and their participation in the planning process, helps to ensure a balance between ease-of-access and protection of patient privacy.

Some of the potential stakeholders may be requestors, custodians, information managers, any approving bodies (e.g. ethics board, approval committees), process owners and/or IT service providers.

Consideration SU-14 – Consider the Establishment of Governance Structures for Secondary-Use.

When planning data repositories, organizations should establish governance structures appropriate for secondary-use, secondary-use repositories or requestors of secondary-use data.

Admin Consideration

Rationale: Establishing overall governance for data repositories intended for secondary-use is required in order to meet many custodial obligations.

In many cases, governance structures exist where it may make sense to include Secondary Use in their mandate if it isn't already. This can help ensure that the risks identified and controls that a custodian has in place for the protection of PHI are considered when PHI and de-identified information flows from custodians to secondary-use repositories.

Consideration SU-15 – Consider Developing and Including Guidance on De-identification Approaches as Part of Governance

A governance mechanism should be considered which allows for the determination of where and how PHI is de-identified.[251]

Admin Consideration

Rationale: Common de-identification mechanisms used by all stakeholders will facilitate interoperability and establish a minimum level of robustness. This consideration works in conjunction with **Consideration SU-2 – Consider Selecting Mechanisms for De-identification Based on Re-identification Risks.**

Consideration SU-16 –Ensure Adequate User Privacy Training is Provided

Organizations that provide access to PHI or de-identified data have a responsibility to ensure that users who access that information have been adequately trained to understand appropriate use and handling of that data, including consequences of a privacy breach, as well as the protocol for reporting and managing a breach.[252] In many jurisdictions, health information legislation exists that requires custodians to establish policies to support this.

Admin Consideration

Rationale: This is in keeping with the Accountability principle. Organizations that consume information for secondary-use have a responsibility to provide this training and have protocols in place in order to deal with breaches. The inclusion of de-identified information may introduce complexities in recognition of a breach and the breach protocol.

[251] Canada Health Infoway, *Privacy and EHR Information Flows in Canada – Common Understandings of the Pan-Canadian Health Information Privacy Group, Version 2.0*, July 31, 2012, pg. 46-47

[252] Canadian Institute for Health Information. *Better Information for Improved Health: A Vision for Health System Use of Data in Canada. Ottawa, ON: CIHI, 2013,* pg. 20

Consideration SU-17 – Consider a Review of Privacy Policies in Light of Big Data Analytics

Organizations that supply data for Big Data Analytics may wish to review their privacy policies to ensure a balance between the principles of limiting use and data minimization and the realities and capabilities of new research platforms.

Admin Consideration

Rationale: We are moving into an era of research platforms rather than one-off projects, where data needs and specific research are not defined at the outset. As the features and capabilities available in the analytics market grows, new approaches to analysis and new uses of PHI will arise. Given this new reality, existing policies may need to be reviewed and adjusted regularly to continue to protect patient privacy.

For a more fulsome discussion on Big Data in the Canadian health milieu, see *Infoway's Big Data Analytics in Health – White Paper (Full Report)* available at https://www.infoway-inforoute.ca/index.php/resources/technical-documents/emerging-technology/doc_download/1419-big-data-analytics-in-health-white-paper-full-report.

Appendix A - Summary of Requirements

The following two tables summarize the privacy requirements and security requirements detailed in **Section 3 – Privacy Requirements** and **Section 4 – Security Requirements** above.

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, organizations hosting components of the EHRi, or organizations connecting to the EHRi.

Table 2. Summary of Privacy Requirements

	Requirement Applies to:					
Privacy Requirements	**EHRi**	**PoS Systems Connected to EHRi**	**Organizations Hosting Components of EHRi**	**Organizations 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 6 – Limitation of Collection, Use or Disclosure to Identified Purposes			✓	✓	✓	
Requirement 7 – Obtaining Knowledgeable Consent			✓	✓	✓	
Requirement 8 – Recording Consent in PoS Systems		✓			✓	✓
Requirement 9 – Associating Consent with PHI in PoS Systems		✓			✓	✓
Requirement 10 – Recording Consent in the EHRi	✓				✓	✓
Requirement 11 – Associating Consent Directives with PHI in the EHRi	✓				✓	✓
Requirement 12 – Logging the Application of Consent Directives	✓					✓

	Requirement Applies to:				Administrative Requirement	Technical Requirement
Privacy Requirements	EHRi	PoS Systems Connected to EHRi	Organizations Hosting Components of EHRi	Organizations Connecting to EHRi		
Requirement 13 – Implications of Consent Directives			✓	✓	✓	
Requirement 14 – Recording Identity of Substitute Decision-Makers	✓				✓	✓
Privacy Requirement 15 – No Coerced Consent			✓	✓	✓	
Privacy Requirement 16 –Collecting Information by Fair and Lawful Means			✓	✓	✓	
Privacy Requirement 17 – Limiting Use and Disclosure of Personal Health Information Means to Identified Purposes			✓	✓	✓	
Privacy Requirement 18 – Logging Access, Modification and Disclosure	✓	✓				✓
Privacy Requirement 19 – Notifying Patients/Persons of Inappropriate Access, Use or Disclosure			✓	✓	✓	
Privacy Requirement 20 – Retaining Records	✓	✓	✓	✓	✓	✓
Privacy Requirement 21 – Accuracy			✓	✓	✓	✓
Privacy Requirement 22 – Denoting Patients/Persons at Elevated Risk	✓	✓				
Privacy Requirement 23 – Training Users and Raising Privacy Awareness			✓	✓	✓	
Privacy Requirement 24 – Openness			✓	✓	✓	
Privacy Requirement 25 – Patient/Person Access			✓	✓	✓	
Privacy Requirement 26 – Amending Inaccurate or Incomplete Information			✓	✓	✓	✓
Privacy Requirement 27 – Challenging Compliance			✓	✓	✓	
Privacy Requirement 28 – Complaint Procedures	✓	✓			✓	
Privacy Requirement 29 – Investigation	✓	✓			✓	

Table 3. Summary of Security Requirements

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	PoS Systems Connected to EHRi	Organizations Hosting Components of EHRi	Organizations Connecting to EHRi		
Security Requirement 1 – Threat and Risk Assessment			✓		✓	
Security Requirement 2 – Security Policy			✓	✓	✓	
Security Requirement 3 – Information Security Management, Co-ordination and Allocation of Responsibilities			✓		✓	
Security Requirement 4 – Independent Review of Security Policy Implementation			✓	✓	✓	
Security Requirement 5 – Assessing Threats and Risks from Third Parties			✓		✓	
Security Requirement 6 – Addressing Security in Third-Party Agreements			✓		✓	
Security Requirement 7 – Transmitting PHI			✓	✓	✓	
Security Requirement 8 – Responsibility for Information Assets			✓		✓	
Security Requirement 9 – Classifying PHI			✓	✓	✓	
Security Requirement 10 – Labelling Personal Health Information As Confidential		✓				✓
Security Requirement 11 – Addressing User Responsibilities in Job Descriptions			✓	✓	✓	
Security Requirement 12 – Addressing User Responsibilities in Terms of Employment			✓	✓	✓	
Security Requirement 13 – Verifying the Identity of Users			✓	✓	✓	
Security Requirement 14 – Confidentiality Agreements			✓	✓	✓	
Security Requirement 15 – Training Users and Raising Security Awareness			✓	✓	✓	
Security Requirement 16 – Terminating User Access When Terminating Employment			✓	✓	✓	
Security Requirement 17 – Physically Securing EHRi			✓		✓	✓

	Requirement Applies to:					
Security Requirements	**EHRi**	**PoS Systems Connected to EHRi**	**Organizations Hosting Components of EHRi**	**Organizations Connecting to EHRi**	**Administrative Requirement**	**Technical Requirement**
Systems						
Security Requirement 18 – Protecting EHR Systems from Hazards			✓		✓	✓
Security Requirement 19 – Protecting EHR Systems from Disruptions			✓		✓	✓
Security Requirement 20 – Protecting EHRi Equipment Off-Premises and During Maintenance			✓		✓	
Security Requirement 21 – Disposing of or Reusing EHRi Equipment			✓	✓	✓	✓
Security Requirement 22 – Removing EHRi Equipment, Data or Software			✓		✓	
Security Requirement 23 – Controlling Changes to the EHRi			✓		✓	
Security Requirement 24 – Segregating Duties			✓		✓	
Security Requirement 25 – Separating Development and Testing from Operations			✓		✓	✓
Security Requirement 26 – Maintaining Capacity			✓		✓	✓
Security Requirement 27 – Upgrading the EHRi			✓		✓	✓
Security Requirement 28 – Protecting Against Malware			✓	✓	✓	✓
Security Requirement 29 – Securely Backing Up Data			✓		✓	✓
Security Requirement 30 – Encrypting PHI During Transmission	✓					✓
Security Requirement 31 – Protecting Source and Destination Integrity During Transmission of PHI	✓					✓
Security Requirement 32 – Acknowleging Receipt of Transmitted PHI	✓					✓
Security Requirement 33 – Protecting PHI on Portable Media			✓		✓	✓
Security Requirement 34 – Disposing of Media Containing PHI			✓	✓	✓	✓

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	PoS Systems Connected to EHRi	Organizations Hosting Components of EHRi	Organizations Connecting to EHRi		
Security Requirement 35 – Protecting Data Storage			✓		✓	✓
Security Requirement 36 – Protecting Storage of Unencrypted PHI in the EHRi			✓		✓	
Security Requirement 37 – Logging Transactions in the EHRi	✓					✓
Security Requirement 38 – Preserving the History of PHI in the EHRi	✓					✓
Security Requirement 39 – Preserving the History of PHI in PoS Systems		✓				✓
Security Requirement 40 – Logging EHRi Transmissions of PHI	✓					✓
Security Requirement 41 – Logging Access to PHI in PoS Systems		✓				✓
Security Requirement 42 – Minimum Content of Audit Logs	✓	✓				✓
Security Requirement 43 – Retaining Audit Logs			✓	✓	✓	✓
Security Requirement 44 – Continuously Logging the EHRi	✓					✓
Security Requirement 45 – Detecting Patterns of Misuse	✓					✓
Security Requirement 46 – Reporting Every Access To A Patient/Person's EHR	✓					✓
Security Requirement 47 – Reporting Every Access By A User	✓					✓
Security Requirement 48 – Analyzing EHRi Audit Logs for Patients/Persons at Elevated Risk	✓					✓
Security Requirement 49 – Securing Access to EHRi Audit Logs	✓		✓		✓	✓
Security Requirement 50 – Making EHRi Audit Logs Tamper-Proof	✓					✓
Security Requirement 51 – Regularly Reviewing EHRi Audit Logs	✓				✓	

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	PoS Systems Connected to EHRi	Organizations Hosting Components of EHRi	Organizations Connecting to EHRi		
Security Requirement 52 – Policy for Access Control	✓				✓	
Security Requirement 53 – Registering Users				✓	✓	
Security Requirement 54 – Assigning Identifiers to Users				✓		✓
Security Requirement 55 – Time-Limited User Registration				✓	✓	
Security Requirement 56 – Reviewing User Registration Details				✓	✓	
Security Requirement 57 – Granting Access to Users by Role	✓	✓				✓
Security Requirement 58 – Selecting A Single Role Per Session		✓				✓
Security Requirement 59 – Granting Access to Users in Workgroups	✓	✓				✓
Security Requirement 60 – Timely Revocation of Access Privileges	✓	✓				✓
Security Requirement 61 – Granting Access by Association	✓	✓				✓
Security Requirement 62 – Reporting the Access Privileges of a User	✓				✓	✓
Security Requirement 63 – Acceptable-Use Agreements				✓	✓	
Security Requirement 64 – Authenticating EHRi Network Access			✓			✓
Security Requirement 65 – Controlling Access to EHRi Network Diagnostics and Network Management Services			✓			✓
Security Requirement 66 – Segregating EHRi Network Users, Services and Systems			✓			✓
Security Requirement 67 – Controlling Routing on EHRi Networks			✓			✓
Security Requirement 68 – Controlling Access to EHRi System Utilities			✓			✓
Security Requirement 69 – Restricting Connection Times to	✓					✓

Security Requirements	Requirement Applies to:				Administrative Requirement	Technical Requirement
	EHRi	PoS Systems Connected to EHRi	Organizations Hosting Components of EHRi	Organizations Connecting to EHRi		
EHRi Applications						
Security Requirement 70 – Robustly Authenticating Users	✓	✓				✓
Security Requirement 71 – Restricting Access to Unattended Workstations		✓				✓
Security Requirement 72 – Acceptable Use of Mobile Devices				✓	✓	
Security Requirement 73 – Acceptable Use of Teleworking				✓	✓	
Security Requirement 74 – Protecting Wireless Networks			✓	✓		✓
Security Requirement 75 – Uniquely Identifying Patients/Persons	✓	✓				✓
Security Requirement 76 – Validating Input Data	✓	✓				✓
Security Requirement 77 – Validating Printed Data		✓				✓
Security Requirement 78 – Providing Digital Signatures for Users		✓				✓
Security Requirement 79 – Validating and Preserving Digital Signatures on PHI	✓					✓
Security Requirement 80 – Implementing Software and Upgrades in the EHRi			✓		✓	
Security Requirement 81 – Protecting EHRi Software			✓			✓
Security Requirement 82 – Managing Known Vulnerabilities			✓			✓
Security Requirement 83 – Reporting Security Incidents Involving the EHRi	✓	✓				✓
Security Requirement 84 – Responding to Security Incidents Involving the EHRi			✓			
Security Requirement 85 – Managing Business Continuity			✓			
Security Requirement 86 – Testing Business Continuity Plans			✓			

Appendix B - Glossary and Acronyms

Acronyms

Term	Description
ACL	Anterior Cruciate Ligament
ADT	Admission/Discharge/Transfer
Anonymity	A situation where an entity cannot be identified within a set of entities. NOTE: Anonymity prevents the tracing of entities or their behaviour, such as user location, frequency of a service usage, and so on.
Assertion	A statement made by an entity without accompanying evidence of its validity.
Assurance Level	A level of confidence in the binding between an entity and the presented identity information.
Attribute	Information bound to an entity that specifies a characteristic of the entity.
Authentication (entity)	A process used to achieve sufficient confidence in the binding between the entity and the presented identity. NOTE: Use of the term Authentication in an identity management (IdM) context is taken to mean Entity Authentication.
Authetication Assurance	The degree of confidence reached in the authentication process that the communication partner is the entity that it claims to be or is expected to be. NOTE: Based on the degree of confidence in the binding between the communicating entity and the identity that is presented.
CDM	Chronic Disease Management
CDS(S)	Clinical Decision Support (Clinical Decision Support System)
CHI	Canada Health Infoway
CHS	Consumer Health Solution
CIHI	Canadian Institute for Health Information
CIS	Clinical Information System
COPD	Chronic Obstructive Pulmonary Disease
COTS	Commercial-off-the-Shelf
CPO	Chief Privacy Officer

Term	Description
Credential	A set of data presented as evidence of a claimed identity and/or entitlements.
CSP	Cloud Service Provider
Digital Identity	A digital representation of the information known about a specific individual, group or organization.
DIS	Drug Information System
DOM	Domain Object Model
DUR	Drug Utilization Review
EA	Enterprise Architect
ED	Emergency Department
EHR	Electronic Health Record
EHRi	Electronic Health Record infostructure
EHRS	Electronic Health Record Solution
EMR	Electronic Medical Record
ENISA	European Network and Information Security Agency
Enrollment	The process of indoctrination of an entity into a context. NOTE 1: Enrolment may include verification of the entity's identity and establishment of a contextual identity. NOTE 2: Enrolment is a pre-requisite to registration. In many cases, the latter is used to describe both processes.
Entity	Something that has separate and distinct existence and that can be identified in context. NOTE: An entity can be a physical person, an animal, a judicial person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities.
EO	Electronic Orders
ER	Emergency Room
ETUM	EHRi Trusted User Model
F/P/T	Federal/Provincial/Territorial

Term	Description
Federation	An association of users, service providers and identity service providers. A *federation*, in this context, is a "group of organizations that trusts certain kinds of information from any member of the group to be valid. [253]
GP	General Practitioner
HIAL	Health Information Access Layer
HIS	Health Information System
HIP	Health Information Privacy Forum
HSU	Health System Use of Data
IaaS	Infrastructure-as-a-Service
Identification	The process of recognizing an entity by contextual characteristics.
Identifier	One or more attributes used to identify an entity within a context.
Identity	A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term Identity is understood as contextual identity or subset of attributes (i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts). NOTE: Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.
Identity Assurance	The degree of confidence in the process of identity validation and verification used to establish the identity of the entity to which the credential was issued, and the degree of confidence that the entity that uses the credential is that entity or the entity to which the credential was issued or assigned.
Identity Management	The policies, processes and techniques involved in managing the lifecycle of digital identities and their associated attributes which are known in a particular security domain.
Identity-Proofing	A process which validates and verifies sufficient information to confirm the claimed identity of the entity.
IdSP	Identity Service Provider. An entity that verifies, maintains, manages and may create and assign identity information of other entities.
IT	Information Technology

[253] A. Bhargav-Spantzel, A. C. Squicciarini, E. Bertino, *Establishing and Protecting Digital Identity in Federation Systems,* DIM '05 Proceedings of the 2005 workshop on Digital identity management – pp. 11-19, Association of Computing Machinery, 2005

Term	Description
ITAC	Information Technology Association of Canada
IVR	Interactive Voice Response
iHHQ	Interoperable Health History Questionnaire
LRS	Longitudinal Record Service
NHS	National Health Service
OTUM	Organizational Trusted User Model
P&S	Privacy and Security
PaaS	Platform-as-a-Service
PACS	Picture Archiving and Communications System
PAQC	Patient Access to Quality Care (Canada Health Infoway Investment Program)
PI	Personal Information
PHI	Personal Health Information
PHR	Personal Health Record
PIPEDA	Personal Information Protection and Electronic Documents Act
PoS	Point-of-Service
PPR	Patient-Provider Relationship
Pseudonym	An identifier who's binding to an entity is not known or is known to only a limited extent, within the context in which it is used. NOTE: A pseudonym can be used to avoid or reduce privacy risks associated with the use of identifier bindings which may reveal the identity of the entity.
Registration	A process in which an entity requests and is assigned privileges to use a service or resource. NOTE: Enrolment is a pre-requisite to registration. Enrolment and registration functions may be combined or separate.
RP	Relying Party. **[ITU-T Y.2720]:** An entity that relies on an identity representation or claim by a requesting/asserting entity within some request context.
SaaS	Software-as-a-Service
SCCC	Standards Collaborative Coordinating Committee

Term	Description
SCSC	Standards Collaborative Steering Committee
SCWG	Standards Collaborative Working Group
SHR	Shared Health Record
SLA	Service Level Agreement
SME	Subject Matter Expert
Trust	The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.
Trust Level	A consistent, quantifiable measure of reliance on the character, ability, strength or truth of someone or something.
Trusted Third Party	[ITU-T Y.2702], [ITU-T X.800], and [ITU-T X.810]: In the context of a security policy, a security authority or its agent that is trusted with respect to some security-relevant activities.
User	Any entity that makes use of a resource (e.g. system, equipment, terminal, process, application, corporate network).
User-Centric	An identity management system that provides the user with the ability to control and enforce various privacy and security policies governing the exchange of identity information, including the user's personally identifiable information (PII), between entities.

Acknowledgements

Infoway woud like to thank the following individuals/organizations who participated in the review of this deliverable and provided valuable input into its development:

Patrick Lo	eHealth Ontario
Gerry Fairweather	New Brunswick Department of Health
Jeff Curtis	Sunnybrook Hospital
Anne Lavigne	The Ottawa Hospital
Jason Lin	Ontario Telehealth Network
Christine Underwood	eHealth Saskatchewan
Duncan Weatherstone	University Health Network
Guy Laliberté	Ministère Santé Service Sociaux
Ken March	NewFoundland and Labrador Center Health Information