Electronic Health Record Infostructure (EHRi)
Privacy and Security Conceptual Architecture

Version 1.1

June 2005

Preface

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

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

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

Executive Summary

This document describes a privacy protective and secure conceptual architecture for Infoway's interoperable electronic health record infostructure (EHRi). Further refinement and implementation of this architecture will ensure that the privacy of patient/persons is protected and that the confidentiality, integrity and availability of their personal health information (PHI) is maintained. Familiarity with the privacy and security conceptual architecture is essential to an understanding of the privacy and security services that the EHRi will provide and the impact these services will have on future Infoway-funded infostructure projects.

This document is the fifth instalment in a series on privacy and security, published by Infoway in 2004-5. Section 1 describes the purpose, objective, scope of the document and the overall assumptions behind the architecture. Throughout the document, assumptions are highlighted and numbered for ease of reference. Changes in the assumptions over time may require a review of the conceptual architecture. The methodology employed in designing the architecture is described in section 1.5. This involved the creation of several preliminary project documents that were used to underpin the architectural analysis. These include:

a) a legislative scan of existing privacy legislation and regulation in Canada relevant to the practice of healthcare,

b) a use case analysis of all the classes of user who will interact with the EHRi and its related systems and how they will make use of each EHRi component,

c) an analysis of the privacy and security requirements for the handling of personal health information (PHI) that used the ten principles of the CSA Model Code as an organisational framework for the privacy requirements and the ISO standard *Code of Practice for Information Security* (ISO/IEC 17799) as an organisational framework for the security requirements.

d) a privacy and security standards analysis that considered the available standards for privacy and security and their potential applicability to the EHRi.

Additional sources of information such as the *ACIET pan-Canadian Privacy and Confidentiality Framework*[1] were also considered when constructing the architecture and are also listed.

Terms used throughout the document are defined in section 1.6 and abbreviations in section 1.7.

Section 2 describes the background, purpose, and objectives of Infoway's privacy and security project and explains why a conceptual architecture is needed. Certain architectural principles have been adhered to and these are listed in section 2.5.

The work herein builds upon the previous document in the series that specified the privacy and security requirements for the EHRi (item c in the list above). Section 3 provides an overview of these requirements. These requirements reflect legislative obligations as expressed in jurisdictional data protection laws and regulations, established privacy and security best practices, and the privacy and security needs identified in common healthcare situations and identified during the use case analysis. The privacy requirements have been organised according to the ten privacy principles of the Canadian Standards Association's *Model Code for the Protection of Personal Information*. The security requirements rely for their organisational framework on the eleven security control areas of ISO/IEC 17799-1:2005 *Code of Practice for Information Security Management*.

Section 4 provides an overview of the conceptual architecture and introduces ten P&S services that together will satisfy all the P&S requirements discussed in the previous section. The architecture is based on a vision of a desired future state of how the EHRi should operate in years to come. This future

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

state has certain key characteristics that are briefly described and also comes with a set of assumptions that must first be met. These too are explicitly listed.

Section 5 lists the information assets that must be protected, identifies the aspects of confidentiality, data integrity, system availability, and auditability requirements that must be met, and presents how these assets are classified for the purposes of security. For the purpose of classifying PHI in terms of its confidentiality, this document advocates a uniform classification for PHI (i.e., all PHI will be classified as uniformly confidential). The availability requirements for EHRi information asset are also listed.

Section 6 identifies ten P&S services that are critical to the protection of PHI in the EHRi. These services are part of a larger suite of data protection tools that all users of PHI in an EHRi environment must adopt, including various data protection policies and procedures, privacy and security training for EHRi users, as well as potential accreditation or certification of EHRi users and the organisations they represent in order to ensure that they have met their responsibilities for protecting PHI in the EHRi. Infoway recognises that the successful protection of PHI in the EHRi depends on an optimal mix of both policy *and* technology instruments. It is the responsibility of the EHRi to protect the privacy of the data that healthcare custodians entrust to its care. Taken together, the ten P&S services described constitute a necessary and sufficient set of technology instruments for providing this protection: they act as a filter to ensure the privacy and security of PHI stored within the EHRi. Because the document provides a P&S *conceptual* architecture, these services do not prescribe specific technologies, vendor products or operating system environments. Infoway recognises, however, that EHRi users will eventually adopt specific privacy and security technologies to support the implementation of the P&S services identified in this document. The ten services are:

1. a **User Identity Management Service** that includes service components to address the need to accurately identify users of the system,
2. a **User Authentication Service** – a transactional service that builds upon identity management to establish the validity of the claimed identity of a user logging into the system and thereby providing protection against fraudulent transactions,
3. an **Access Control Service** that provides access control methodologies as part of a unified privilege management service for EHRI users,
4. a **Consent Directives Management Service** that translates privacy requirements arising from sources such as legislation, policies, and individuals' specific consent directives, and applies these requirements in an EHR environment,
5. an **Identity Protection Service** that will improve privacy protection by facilitating the separate storage of personal information that uniquely identifies individuals (e.g. name, address, health card number, etc.) from health information relating to their care and treatment; as well as allowing approved researchers access to anonymised longitudinal data by providing pseudonymously identifier PHI,
6. an **Anonymisation Service** that takes PHI representing an identifiable individual and then removes all personal identifiers prior to aggregating the data into data sets of completely anonymised data for use in research and statistical analysis,
7. an **Encryption Service** that maintains data confidentiality and integrity using cryptography,
8. a **Digital Signature Service** that allows a health care professional to sign a digital document such as an e-prescription in much the same way that they would apply a signature to paper, and with the assurance that that the signature cannot be forged and neither the document nor the signature can be altered without rendering the signature invalid,
9. a **Secure Audit Service** to record significant privacy and security-related events in an event log. Component services include event logging and log analysis, and
10. **General Security Services** common to most large IT infrastructures, such as scanning for viruses, secure backup and restoration of data, secure data archiving, and secure data destruction.

Each of the ten P&S services is described and a rationale given for why it is needed (section 7). For many of the services, alternative approaches are described – including the advantages and disadvantages of each – and a recommendation is made as to which approaches should be pursued. Policy enforcement for each service is discussed; i.e., how jurisdictional policies related to the service can be effectively operationalised and continuously maintained. A process flow is provided for each service describing, at a conceptual level, how the service will operate. The service's availability requirements are described; i.e., how critical the service is to the ongoing operation of the EHRi. Interactions among the services are also described. Requisites are listed for the successful implementation of each service. Each service is broken down into service components and the reader is referred to the appropriate sections of Appendix A where each service component is described in detail.

Section 7.2.2 explains who the users of the EHRi will be. While it is expected that most EHRi users will be healthcare providers, explicit support is provided in the architecture for patients/persons who wish to directly access and securely access portions of their EHR.

Certain other EHRi services will also have an impact on privacy and security and these general services are described in section 8. They include:

- policy management service,
- session management service,
- EHR services,
- provider registry and user registry services,
- notification services,
- messaging services, and
- mapping services.

Each of these general EHRi services will have an impact on privacy and security and that impact on privacy and security is examined. Where P&S services depend on these more general services, the dependencies are listed.

As the EHRi will be deployed over many years, it will pass through interim states of deployment and development. These interim states are discussed in section 9 (albeit only in outline).

Privacy and security related issues have a significant impact on governance of the EHRi and these impacts are discussed in section 10. While some basic questions are addressed (e.g.: why the EHRi requires governance), many others remain outstanding. What are the rules for cross-border data exchange? What are the minimum criteria for effective inter-jurisdictional data sharing agreements? How is custodianship addressed and custodial responsibility maintained when data flows from one jurisdiction to another? How are disputes fairly and efficiently resolved? Such questions will require much discussion and a clear framework is needed within which to answer them. Jurisdictional stakeholders have clearly articulated their desire to see such questions answered and such a governance framework established. While governance itself is outside the scope of Infoway's mandate, there remains a possible future role for Infoway in facilitating further inter-jurisdictional discussions on governance, especially as such discussions relate to privacy, security, and the EHRi.

A brief description is given in section 11 of another document in the P&S series that discusses privacy and security related technical standards.

Canada Health Infoway / Inforoute Santé du Canada

CONTENTS

LIST OF FIGURES AND ILLUSTRATIONS

1 Introduction

1.1 Purpose

This document describes the conceptual architecture needed to ensure that the privacy and security (P&S) requirements for an interoperable EHRi are met.[2] It is the basis for Infoway's funding of P&S architectural solutions. The conceptual architecture (CA) includes a description of IT services that will become core components of Infoway's electronic health record infostructure (EHRi). The document will also allow key stakeholders to validate the architecture and the P&S services that it defines.

1.2 Objective

This report has several objectives:

1. build upon the work on P&S CA already defined in the *EHRS Blueprint, and in the Electronic Health Record Privacy and Security Requirements;*
2. define concepts of trusted connections for interconnection to the EHRi;
3. delineate the EHRi information assets that must be protected and the level of security that must be met;
4. explain the P&S architectural challenges that must be met by the design of the EHRi;
5. specify the design principles that will be applied to the P&S conceptual architecture;
6. identify, describe and analyse specific privacy and security services for the EHRi based on Infoway's P&S use case analysis[3], its privacy and security requirements, and an analysis of jurisdictional privacy legislation and attendant obligations;
7. provide a cross-jurisdictional view of those services in support of an interoperable EHR; and
8. serve as a reference document for the Canadian health care IT community.

1.3 Scope

The scope of this work includes all of the following:

1. a delineation of the EHRi information assets that must be protected and the sensitivity of each asset in terms of confidentiality, integrity and availability;
2. an analysis and recommendation of all the P&S security services that are needed to construct a secure and privacy protective interoperable EHR. Services include those needed by the EHRi itself and those that specify connection points with outside services such as Point of Service (POS) Systems and users of the EHRi (healthcare providers, healthcare support staff, etc.)
3. examples of process flow for the major architectural components;
4. examples of anticipated interim states that the implementation is likely to pass through before the fully elaborated architectural vision is finally achieved throughout the EHRi and its interconnected systems.
5. All of the following will be described in detail:
    a. **User Identification:** establishing a valid and unique identity for each EHRi user;

[2] The P&S requirements for the EHRi are detailed in *Electronic Health Record (EHR) Privacy and Security Requirements*. See References section at the end of this document.
[3] The P&S use case analysis can be found in *Electronic Health Record (EHR) Privacy and Security Use Case Analysis.* See References section at the end of this document.

b. **Authentication:** validating the identity of EHRi users or devices upon each system access, transaction or message

c. **Access control (privilege management and user authorisation)**: protecting the confidentiality and integrity of EHRi information assets by preventing unauthorised access and use.

d. **Identity protection and pseudonymisation:** mechanisms for separating, to the greatest extent possible, personal information that uniquely identifies patient/persons[4] from health information relating to treatment, diagnosis, etc.

e. **Anonymisation:** ensuring that aggregated data is available for research and public health surveillance that protects the privacy of patients/persons to the greatest extent possible.

f. **Confidentiality:** ensuring information is not made available or disclosed to unauthorised individuals, entities or processes.

g. **System and data integrity:** ensuring that the contents of each EHR, transaction or message has not been altered or destroyed in an unauthorised manner.

h. **Availability**: ensuring that information assets are always available in a timely and reliable manner when needed by authorised EHRi users and devices.

i. **Audit and Control:** establishing accountability for transaction processing by creating a permanent record of transaction and message history.

This document makes no recommendations on specific technologies, vendors, or products.

Data quality is vital to a trustworthy EHR, the definition data quality service will be incorporated into subsequent versions of the Infoway EHRS Blueprint and is therefore out of scope for this document.

Network security is a jurisdictional responsibility and will not be discussed further in this document, other than in section 7.12.1 which observes that the P&S architecture does *not* depend upon network security services or protocols to maintain the confidentiality or integrity of PHI traversing any network to which the EHRi is connected.

Server security, vulnerability management, and change management are also jurisdictional responsibilities and while essential for overall security, will not be discussed further in this document.

1.4 Assumptions

Throughout the document, assumptions are highlighted and consecutively numbered for ease of reference. If in the future one or more of these assumptions no longer hold, the impact on the architecture will need careful review and the architecture itself may need revision.

Assumption 1	The whole of the EHRi will be built upon message-based service oriented architecture[5].
Assumption 2	The EHRi will not facilitate the transmission of PHI from POS system to POS system on a strict peer-to-peer basis.
Assumption 3	Health information custodians will be responsible for the security of any PHI downloaded from the EHRi into their POS systems. Once the EHRi has provided the requested information into a local system, the custodian/trustee of that system assumes custodial responsibility for maintaining the privacy and security of the information.

[4] This document follows the convention of the EHRS Blueprint in referring to recipients of healthcare and subjects of healthcare administration as patients/persons. For more information, see section 2.1.9 on page 4 of the EHRS Blueprint.
[5] See the EHRS Blueprint, page 14.

Assumption 4	POS systems connecting to the EHRi must be demonstrably compliant with appropriate published security policies and standards that have been endorsed by jurisdictional authority responsible for the EHRi's operation in a given jurisdiction (see section 10 on Governance of the EHRi).
Assumption 5	Implementations of the EHRi exist within a uniform high trust model. The same may not be true of POS systems connecting to the EHRi.
Assumption 6	Rigorous change management practices and vulnerability management will be in place for networks, hardware and software (e.g., firewalls, patch management).
Assumption 7	Malware security will run on all EHRi servers.
Assumption 8	Not all P&S services described in this document will be operationalised in every jurisdiction's implementation of the EHRi, as some are not currently required by every jurisdiction's legislative obligations. All the EHRi services will be operational in at least some jurisdictions.
Assumption 9	Security services will not support location-based security; i.e., that privacy and security business rules may restrict access to PHI based on role, work group, etc., but not based on access from a specific physical location. Use of wireless services (for example, by ambulance services) makes the concept of physical location in relation to access moot and in any event, protection of privacy depends upon who accessed PHI and what was done with it, not where the access took place. The P&S services will also not have the capacity to attest to or audit the physical location where a service or access request originated.
Assumption 10	The EHRi common services messaging infrastructure will be designed to enable acknowledgement of message receipt.
Assumption 11	To ensure that healthcare providers trust the messaging system that EHRi common services provides, the EHRi common services will relentlessly attempt delivery of messages until receipt is either acknowledged or until the EHRi common services notification service successfully notifies an appropriate entity of message delivery failure.
Assumption 12	The EHRi will only process and store information consent directives, not consent to treatment directives; including consent to participate in clinical trials. As a consequence, the P&S conceptual architecture will not provide functionality to allow patients/persons to record within the EHRi consent directives related to treatment or clinical trials.
Assumption 13	Inter-jurisdictional disclosures of PHI will not take place until all of the consent requirements of the disclosing jurisdiction have been met.
Assumption 14	Every implementation of the EHRi will store PHI under the governance of the implementing jurisdiction(s).

1.5 Methodology

The P&S conceptual architecture builds upon four prior P&S projects:

a) a legislative scan of existing privacy legislation and regulation in Canada relevant to the practice of healthcare. The results of the legislative scan can be found in Appendix A of *Electronic Health Record (EHR)Privacy and Security Requirements, revised February 2005,* available at **www.canadahealthinfoway.ca**

b) a use case analysis carried out over a four month period, culminating in the publication on Infoway's web site of a comprehensive set of EHR P&S use cases. The analysis considered all the classes of user who will interact with the EHRi and its related systems, the various scenarios within which they will use an EHRi, and the individual uses that they will make of each

EHRi component. Refer to *Electronic Health Record Privacy and Security Use Cases,* 2004, (see the References section at the end of this document).

c) an analysis of the privacy and security requirements for the handling of personal health information (PHI) that evolved over a six month period in 2004-2005[6] culminating in jurisdictional workshops to review and vet the requirements that took place in January of 2005. The analysis separated the privacy and security requirements for the handling of personal health information (PHI) into two categories: (1) privacy requirements and (2) security requirements. Infoway used the 10 principles of the CSA Model Code[7] as an organisational framework for the privacy requirements. The ISO standard *Code of Practice for Information Security* (ISO/IEC 17799) was used as an organisational framework for the security requirements. See the Reference section at the end of this document.

   The analysis describes each requirement, explains why Infoway selected each requirement, and outlines how each requirement relates to an interoperable EHR. All privacy and security requirements outlined in legislation that are relevant to an interoperable EHR are contained in this analysis. See *Electronic Health Record (EHR) Privacy and Security Requirements, revised February 2005,* available at **www.canadahealthinfoway.ca**

d) a privacy and security standards analysis that considered the available standards for privacy and security and their potential applicability to the EHRi.

Additional sources of information were also considered, more specifically the *Pan-Canadian Health Information Privacy And Confidentiality Framework*, Advisory Council on Information and Emerging Technologies (ACIET), January 27, 2005 (www.hc-sc.gc.ca/ohih-bsi/theme/priv/index_e.html). The P&S conceptual architecture is designed to be supportive of the guidelines expressed in the ACIET privacy and confidentiality framework document. In addition to supporting the implied knowledgeable consent for care and treatment model defined in the ACIET framework, the Infoway privacy and security architecture supports alternative models of consent.

Building upon the work above, a set of P&S services were crafted to meet all of these requirements (see Appendix C). Services with a major impact in P&S such as consent and identity protection were then mapped out in detail.

An expert panel of reviewers read a preliminary draft of the architecture and met with the P&S team on April 21, 2005 to discuss the draft and suggest improvements to content and structure. Their suggestions were incorporated in a completed first draft that was prepared for jurisdictional representatives on April 29, 2005. A series of validation workshops (both within Infoway, and with jurisdictions and vendors) were held during May of 2005 to review and validate this work. In addition, a web forum operational from February to June 2005 provided further feedback and comments.

This revised version of the P&S conceptual architecture has been significantly influenced by feedback from the various workshops and forums listed above. The authors are especially indebted to jurisdictional representatives of British Columbia, Ontario, Saskatchewan, and the Office of the Privacy Commissioner of Canada, for their many detailed comments and insights. These have strengthened and complemented the P&S team's work.

1.6 Terminology

ACIET Framework – The *Pan-Canadian Health Information Privacy and Confidentiality Framework* was published in January of 2005 after review of domestic and international approaches to protecting PHI privacy; consultation by participating jurisdictions with their respective government departments, ministries and stakeholder communities; consultation by Health Canada with national care provider associations. The Framework is comprised of core provisions aimed at protecting the privacy of

[6] Canada Health Infoway, *Electronic Health Record Privacy and Security Requirements,* 2005.
[7] The CSA Model Code also forms the basis of Schedule 1 of PIPEDA (the *Personal Information Protection and Electronic Documents Act*, 2001).

individuals and the confidentiality of their health information, while enabling the flow of that information where appropriate to support effective health care, the management of the health system and an interoperable EHR. Core provisions are consistent with the *Canadian Charter of Rights and Freedoms, PIPEDA* and current realities of the health system. An underlying principle of the Framework is that the collection, use and disclosure of PHI is to be carried out in the most limited manner, on a need-to-know basis and with the highest degree of anonymity possible in the circumstances. The Framework proposes an implied knowledgeable consent model for the collection, use and disclosure of personal health information within the circle of care.

Authentication – corroboration that the source of the data is as claimed, based on information used to establish the validity of a claimed identity (ISO 7498-2).

Authentication Token – An authentication token is a cryptographically protected, binary encoded string or object containing minimal user information, a timestamp, and an expiry time. It is created by the EHRi after it has first authenticated a user as part of the login process. This token is then returned to the user's system to be used for subsequent access to EHR functions during that session without the user having to re-login.

Availability – the property of being accessible and useable upon demand by an authorised entity (ISO 7498-2).

Collection of PHI – means to gather, acquire, receive or obtain personal health information by any means from any source.[8] See also **Disclosure of PHI** and **Use of PHI.**

Conceptual architecture – A conceptual architecture provides a view of the key high level services and data repositories and where they will be hosted in the enterprise[9]. The EHRi conceptual architecture outlines the various systems that must exist in order to enable the creation of an EHRi. A conceptual architecture makes no assumptions about the physical location of servers or services.

Confidentiality – the property that information is not made available or disclosed to unauthorised individuals, entities or processes (ISO 7498-2).

Deemed consent – In the context of a statutory requirement, means that it does not matter whether the patient/person has actually consented; the law permits organisations to act as if the patient/person has consented; there is no right to withdraw or withhold consent. See also **express consent**, **implied consent** and **no consent**.

Desired Future state of the P&S conceptual architecture - a mature P&S architecture where a fully integrated, fully interoperable EHR infostructure has been implemented in all (or most) of Canada's healthcare jurisdictions. The desired future state presupposes that most legacy systems have been retired from service or upgraded and that POS systems in use have been built, refreshed or supplemented to seamlessly integrate with the EHRi. Ideally, this future state will be achieved within fifteen years, although the retirement of superannuated legacy systems from service has been notoriously difficult to achieve in healthcare in a timely fashion.

Disclosure of PHI – means to make personal health information available or to release it to another health information custodian, trustee or to another person, but does not include to use the information.[10] See also **Collection of PHI** and **Use of PHI**.

Domain repository – "A Domain Repository is a component of an EHRi that stores, manages and persists a specific clinical subset of data, typically at a jurisdictional level. These may be domain-level operational systems for the given jurisdiction as well. The key data domains recognised as part of an EHR are drugs, laboratory and diagnostic imaging."[11]

---

[8] Ontario *Personal Health Information Protection Act, 2004,* S.O. 2004, c. 3, s. 2.
[9] EHRS Blueprint: An Interoperable EHR Framework, Canada Health Infoway, July 2003, forward p. ii.
[10] Ontario *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, s. 2.
[11] EHRS Blueprint: An Interoperable EHR Framework, Canada Health Infoway, July 2003, p.4.

EHRi data domain – EHRi data domains are fully defined in the Blueprint, version 1, page 43, ff. The key data domains recognised as part of an EHR are health profile, drugs, laboratory and diagnostic imaging.

EHRi security domain – The collection of EHRi servers, data repositories and services that are controlled by a single security policy. Ideally, a single security policy would cover the operation of the EHRi within a given jurisdiction, but as domain repositories connected to the EHRi may be governed by their own security policies, a single security policy may not be attainable in the short term.

EHRi Trusted User Management.—user registration (i.e., identity management), privilege management (enrolment to access specific EHRi services) and user authentication; all performed directly by the EHRi on behalf of EHRi users (who would separately register and enrol in various EHRi services to access the EHRi. Contrast with **Organisational Trusted User Management** (which see).

Electronic Health Record – an electronic record that provides each individual in Canada with a secure and private lifetime record of his or her key health history and care within the health system. The record is available electronically to authorised healthcare providers and the individual anywhere, anytime in support of high quality care.12 In an Electronic Health Record Infostructure (EHRi), the EHR is the central component that stores, maintains and manages clinical information about patients/persons. The extent of the clinical information sustained by the EHR component may vary based namely on the presence or absence of Domain Repositories in any given jurisdiction.

Electronic Health Record Infostructure (EHRi) – a collection of common and reusable components in support of a diverse set of health information management applications.[13] It consists of software solutions for the EHR, data definitions for the EHR and messaging standards for the EHR.

Express consent – A voluntary agreement with what is being done or proposed that is unequivocal and does not require any inference on the part of the organisation seeking consent. See also **deemed consent**, **implied consent** and **no consent**..

Health Information Custodian – an individual or organisation that collects, uses, or discloses personal health information for the purposes of care and treatment, planning and management of the health system or health research. The individual jurisdiction's legislation typically includes the following entities:

- Health service providers, i.e., persons who are licensed or registered to provide health services.
- The Federal/Provincial/Territorial Minister and Department of Health
- Regional Health Authorities (where they exist)
- Hospitals and nursing homes and other identified health care facilities
- Pharmacists and pharmacies
- Boards, agencies, committees and other organisations identified in regulations
- Affiliates/agents e.g. employees, volunteers
- Cancer Board
- Mental Health Board
- Ambulance Operators
- Persons who maintain and administer an EHR system[14]

Implied consent – A voluntary agreement with what is being done or proposed that can be reasonably determined through the actions or inactions of the patient/person. See also **deemed consent**, **express consent** and **no consent**.

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

Information asset – hardware, software, communications infrastructure, and information (used, processed or stored in any manner) that are recognised by the organisation that possesses the asset as being valuable.

Integrity – the property that data has not been altered or destroyed in an unauthorised manner (ISO 7498-2).

Interim states of the P&S conceptual architecture – transitional states of the P&S architecture that will support a variety of methods for user authentication, access control, consent directives management and other business processes. Some of these methods may be less than ideal in terms of cost and efficient business process but are supported because of the obvious need to support and transition legacy systems in widespread use within healthcare.

Legacy application/system – An application in which a company or organisation has already invested considerable time and money. Typically, legacy applications are database management systems (DBMS) running on mainframes or minicomputers. An important feature of new software products is the ability to work with a company's legacy applications, or at least be able to import data from them.[15]

Lockbox – The statutory right for an individual to restrict the use or disclosure of his or her PHI, although this term actually tends not to be used in legislation.

Masking – Masking is a term used to describe the process of restricting an access to or transfer of PHI. Typically, masking is applied at the data source and may be overridden, as permitted by law, by the accessing custodian (e.g. in emergency health situations).

No consent – In the context of a statutory requirement, means that consent is not required for a particular purpose. See also **deemed consent**, **express consent** and **implied consent**.

Organisational Trusted User Management.—the presence within a healthcare organisation of user registration (i.e., identity management), access control and user authentication (as performed by a POS system or clinical portal managed by the organisation); all carried out to a degree of rigour that would allow the EHRi to trust user identifiers associated with HL7 message requests received from the organisation's POS system(s) or clinical portal. Contrast with **EHRI Trusted User Management** (which see).

Organisation ID - a unique identifier assigned to an organisation which may represent multiple POS instance IDs.

Personal Health Information (PHI) – Recorded information about an identifiable individual that relates to the physical or mental health of the individual and to the provision of health services to the individual, including the identification of a person as a provider of health care to the individual. PHI may include:

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

PHI does not include information that, either by itself or when combined with other information available to the holder, does not permit individuals to be identified, i.e. the identity of the individual who is the subject of the information cannot be readily ascertained from the information.

[15] http://www.webopedia.com/TERM/l/legacy_application.html

Privacy – Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[16]

Point of Service (POS) System — The clinical application systems (e.g. ADT, CIS, LIS, etc.) that operate at the many locations where the healthcare services are delivered to patients/persons. These systems may have human computer interfaces or be medical equipment generating data on a user that is then fed into the EHR. These systems are the sources for all clinical information that make up the EHR Data. They may also access data from the EHRi when it is operational, as well as from their own data stores to provide a more complete view of a patient/person's health history and current information.[17]

POS System instance ID (POSSID) – a unique identifier assigned to an installation of a POS system.

Repudiation – denial by one of the entities involved in a communication of having participated in all or part of the communication ISO 7498-2).

Security – Maintaining availability, confidentiality, integrity and accountability of information assets.

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

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

Substitute decision maker – in relation to a patient/person, means, unless the context requires otherwise, a person who is authorised under legislation to consent on behalf of the patient/person to the collection, use or disclosure of personal health information about the patient/person.[18]

Use of PHI – means to handle or deal with personal health information, but does not include disclosing the information.[19] See also **Collection of PHI** and **Disclosure of PHI**.

1.7 Abbreviations Used

ANS	Anonymisation Service
CIS	Clinical Information System
CDMS	Consent Directives Management Service
DSS	Digital Signature Service
EHR	Electronic Health Record

[16] A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1968) p. 42-43.
[17] EHRS Blueprint: An Interoperable EHR Framework, Canada Health Infoway, July 2003, p. 37.
[18] Ontario *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, s. 5.
[19] Ontario *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, s. 2.

EHRi	Electronic Health Record Infostructure
EHRS	Electronic Health Record Solutions
ECID	EHRi Client Identifier
ES	Encryption Service
FID	Federated identifier
HIAL	Health Information Access Layer (also referred to as “EHRi common services” in this document)
IMS	Identity Management Service
IPS	Identity Protection Service
P&S	Privacy and Security
P&S CA	Privacy and Security Conceptual Architecture
PHI	Personal Health Information
PID	Public identifier
POS	Point of Service
POSSID	POS System Instance Identifier
PHS	Public Health Surveillance
Pseudo ID	Pseudonymous identifier
POS	Point of Service
UAS	User Authentication Service

2 Privacy and Security Architecture Project

2.1 Project Description

The *Infoway EHRS Blueprint* (the Blueprint)[20] presents the business and technical architecture for an interoperable EHR framework. Essential to the Blueprint are the services required to ensure the privacy and security of personal health information stored and/or referenced by the EHR. The first version of the Blueprint did not provide detailed information on the P&S requirements and architecture. The objective of the privacy and security project is to provide input to the Blueprint v2.0 on all aspects of P&S. Specifically, the privacy and security architecture project is intended to:

- define and validate the privacy and security requirements that an interoperable EHR must provide;
- define the privacy and security services to be included in the Blueprint as required to support common solution architecture and common standards needed to ensure inter-operability and re-use;
- design a flexible privacy and security conceptual architecture in support of current and future jurisdictional legislative, regulatory and policy requirements; and
- identify privacy & security initiatives that *Infoway* should pursue.

2.2 Background for P&S CA

The project has produced four documents:

1. a scan of legislative privacy and security obligations under law and regulation in Canada's provincial and territorial jurisdictions;
2. a privacy and security use case analysis of the EHRi and a discussion of the privacy and security issues that arise from this use case analysis;
3. an identification of the privacy and security requirements that an interoperable electronic health record (EHR) must satisfy to meet the legislative requirements and resolve the privacy and security issues discussed in the preceding two documents; and
4. a review and analysis of available standards that could be adopted to facilitate construction of the P&S architecture and promote interoperability.

These four reports provide the background for the design of P&S CA. The current document, the fifth in the series, is part of the second phase of the project; a phase that culminated in the development and validation of a privacy and security conceptual architecture, as well as in the identification of privacy and security initiatives, using the project documents above as a guide.

[20] The Canada Health Infoway *EHRS Blueprint: An Interoperable EHR Framework* is available online at www.canadahealthinfoway.ca.

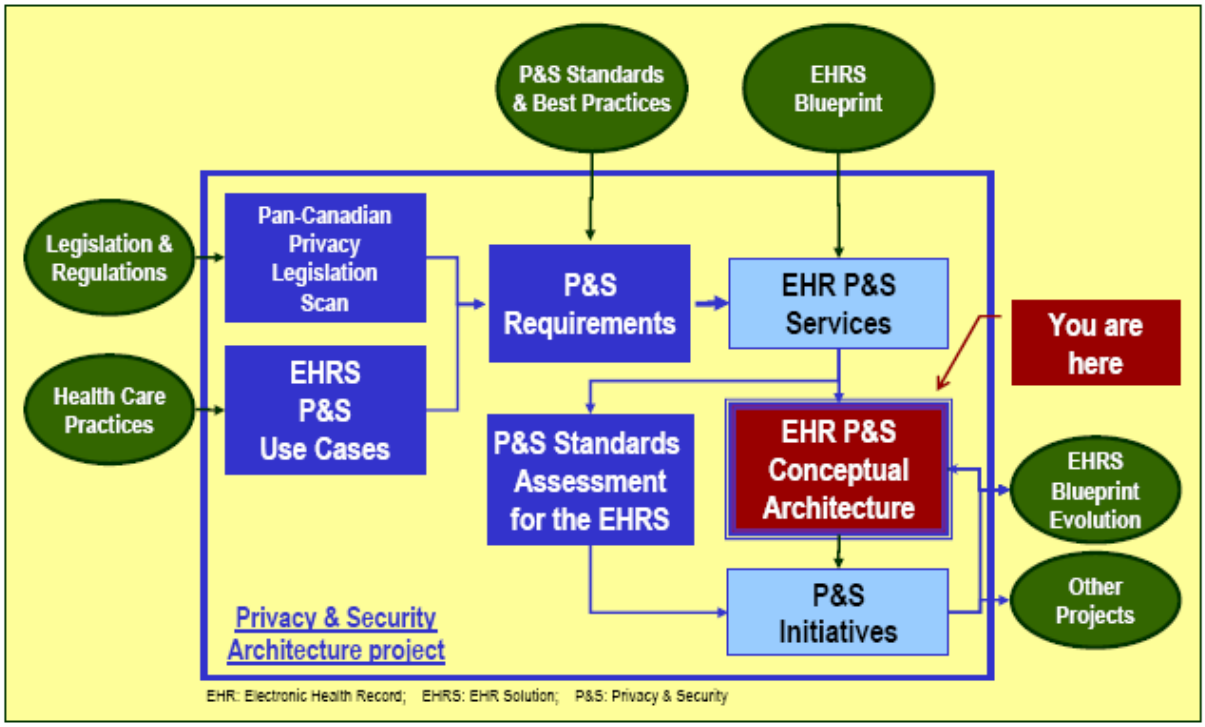

Figure 1: Context of P&S Conceptual Architecture document within the P&S Project

2.3 What is a Conceptual Architecture?

A conceptual architecture provides a view of key high-level services and data repositories and where they will be hosted in the enterprise. The Infoway EHRS Blueprint is designed to provide a comprehensive description of the solution components necessary for an interoperable EHR and as such, the Blueprint constitutes a conceptual architecture for the EHRi.

The Infoway business plan establishes, in broad terms, *what* the EHRi is intended to do—its "functionality". The Blueprint builds on this to specify in broad terms *how* the EHRi is to accomplish these functions—its "services".

The P&S requirements document[21] specifies the detailed P&S requirements that the EHRi and its connected systems must meet. The current document specifies *how* Infoway wants to achieve this functionality; in other words, it describes the detailed P&S capabilities of the EHRi and the P&S services that it will provide. The P&S Conceptual Architecture serves as a roadmap for the design and deployment of these common services. Although it remains technology neutral (i.e., it does not mandate the use of any particular technology, product or vendor service), it nevertheless specifies the architecture to a level of detail sufficient to ensure coherent planning of P&S services across the EHRi.

2.4 Why is a Conceptual Architecture Needed?

All members of the Canadian healthcare community share in the responsibility to maintain patient privacy and data protection of PHI. This responsibility is not easily borne. Overlapping privacy legislation, regulations that are open to interpretation, and complex security technology all combine to overwhelm the unwary, and most busy healthcare professionals are neither trained in depth in

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

information technology nor do they have the time to keep up with rapidly changing technology. This conceptual architecture for EHRi privacy and security is intended to surmount these difficulties by providing a solid foundation for the design and implementation of the EHRi that meets all of the legislative, regulatory, policy, administrative and technical requirements on patient/person privacy and the security of PHI. The P&S conceptual architecture fulfils several needs:

1. It describes all the services needed to meet the P&S requirements described in the requirements document.[22] Because the requirements are crafted in part to satisfy the legislative and regulatory requirements of Canada's healthcare jurisdictions, the conceptual architecture meets these legislative and regulatory requirements as well. Appendix B relates each requirement described in the Requirements document to the P&S service or services that fulfill the requirement.
2. It allows a single flexible EHRi architecture to meet the many requirements of Canadian healthcare jurisdictions without saddling one jurisdiction with unnecessary technical machinery required by the regulations of another jurisdiction. The philosophy of "build once and use many times" is central to Infoway's investment strategy and a unified conceptual architecture is an essential component of building an EHRi that meets the P&S requirements of multiple jurisdictions.
3. It maximises the effective use of resources by tackling P&S services in a coordinated and systematic way. The optimal use of P&S services reduces the number of interfaces, simplifies the architecture, and facilitates the achievement of cost savings due to the shared use of P&S services among applications.
4. Interoperability is simplified due to a common and unified approach to P&S. The EHRi must ultimately support inter-jurisdictional access and therefore interoperability across jurisdictions. Without a conceptual architecture for P&S, it is difficult to imagine how meaningful interoperability could be effectively achieved.
5. POS system and EHRi component vendors have a coherent roadmap from which to build and enhance their products with P&S features and services.

2.5 Architectural Principles

In addition to the general architectural principles identified in the EHRS Blueprint, several other architectural principles guide the design of the P&S conceptual architecture. The architecture must:

1. support a phased evolution that allows POS systems to connect with only modest changes to infrastructure and process flow and that minimises the changes to current POS systems that will be needed before the EHRi can be effectively utilised;
2. be scalable in two respects: to support small and large jurisdictions and to accommodate growth within a jurisdiction in the use of the EHRi;
3. support the custodial responsibilities of health information custodians by applying P&S rules whenever PHI flows into the EHRi (i.e., when PHI is uploaded to the EHRi and its repositories), and when PHI flows out of the EHRi (i.e., is supplied by the EHRi to fulfil an access request). Moreover, custodial responsibilities must be met when the EHRi fulfils access requests from within a jurisdiction (including PHI obtained from domain repositories), and must also ensure that a jurisdiction's custodial responsibilities are fulfilled before transmitting PHI to an EHRi in another jurisdiction.

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

3 Overview of Privacy and Information Security Requirements

3.1 Introduction

Privacy and security (P&S) requirements that the EHRi must meet in order to fully protect the privacy of patient/persons and maintain the confidentiality, integrity and availability of their data have already been defined. These requirements reflect:

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

The requirements are fully described in *Canada Health Infoway, Electronic Health Record Privacy and Security Requirements,* 2005. Section 4 of this document describes 29 privacy requirements for an interoperable EHR, organised according to the ten privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96). The Code was published in March 1996 as a national standard for Canada. These core principles constitute a widely recognised and principled approach to data protection in an EHR environment.

Section 5 of the *Requirements* document identifies 87 security requirements for an interoperable EHR using ISO/IEC 17799-1:2005 *Code of Practice for Information Security Management* as its organisational framework. The ISO/IEC 17799 Code of Practice is a widely adopted international standard for information security management. The Code opens with an introduction describing information security and detailing why it is needed, how to assess security requirements and how to assess risks and assign controls. The remainder of the standard is organised into eleven sections, each covering a key control area for information security. Together these describe the working objectives of the Code of Practice.

3.2 Privacy Requirements

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

1. **Accountability for PHI**: Organisations that collect, use or disclose PHI are responsible for PHI in their care or custody, including information transferred to third parties for processing (e.g. agents[23]), and must name someone who will be responsible for facilitating compliance with applicable data protection legislation and the privacy requirements described in Appendix C – Informational Consent.

   Four requirements for accountability are discussed in the Requirements document, section 4.1, page 20. While the whole of the P&S conceptual architecture promotes accountability for PHI, only the fourth of these four accountability requirements (the requirement for Privacy Impact

[23] "Agent" is defined in the Ontario *Personal Health Information Protection Act* as, "in relation to a health information custodian, a person that, with the authorisation of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated."

Assessments – Privacy Requirement 4) has technical implications for the P&S conceptual architecture.

2. **Identifying purposes for collection, use and disclosure of PHI:** 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. Requirements relating to identifying purposes for collection, use and disclosure of PHI are described in the Requirements document, section 4.2, page 22 ff.

3. **Consent**: Laws may require express, implied, deemed or no consent for specific collections, uses and disclosures of PHI. An organisation should be able to demonstrate that it complied with applicable legislative requirements and that the patient/person had a reasonable opportunity to know that information was going to be collected and used for specific purposes.

   Consent is a complex and multifaceted subject and is discussed in detail in Appendix C. Requirements regarding consent are stated in the Requirements document, section 4.3, page 24 ff. Consent directives management in the P&S conceptual architecture are designed to meet all of these requirements. Consent directives management and services are discussed in section 7.6

4. **Limiting collection of PHI**: Organisations connecting to the EHRi and organisations hosting components of the EHRi should limit collection of PHI to that which is necessary for the identified purposes; i.e. PHI should not be collected indiscriminately.

   The Requirements document states a single requirement for limiting collection of PHI in section 4.4, p. 31. This is an administrative requirement and does not directly influence the P&S conceptual architecture.

5. **Limiting use, disclosure and retention of PHI:** When organisations identify the purposes for which they collect PHI and seek the appropriate consent for these purposes, it is imperative that they then only use, disclose and retain information for these purposes.

   The requirements document states several requirements related to limiting use, disclosure and retention in section 4.5, p. 32 ff. Many P&S services are involved in limiting use, disclosure and retention. Appendix B relates each of the requirements for limiting PHI use, disclosure and retention to one or more P&S services.

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

   The Requirements document states a requirement on accuracy in section 4.6, p. 34. Several P&S services ensure the maintenance of accuracy and Appendix B discusses how these services meet the requirement for accuracy.

7. **Safeguards for the protection of personal health information**: The EHRi, organisations connecting to the EHRi, and organisations hosting components of the EHRi must, through the application of appropriate security safeguards, protect PHI against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification.

   The Requirements document lists many security requirements related to safeguards (section 5, p. 42, ff.). All of the P&S services taken together ensure that these requirements are met. Appendix B discusses which services relate to each requirement.

8. **Openness about practices concerning the management of PHI**: This privacy principle is closely related to the accountability discussed above. The intent is to make it possible for concerned patients/persons to know the purposes for collecting, using, and disclosing PHI about them. Privacy oversight bodies (e.g. Information and Privacy Commissioners) may also want assurance that healthcare organisations have privacy management plans in place.

A requirement for openness is stated in the Requirements document, section 4.8, page 36. Because this is an administrative requirement that has no technical components, the P&S conceptual architecture does not directly address this requirement.

9. **Individual access to personal health information**: Two related requirements are stated in the Requirements document (section 4.9, p. 37 ff.) and the P&S architecture contains specific provisions for patient/person access to their PHI and for amending inaccurate or incomplete information.
10. **Challenging compliance**: The right of any patient/person to lodge a privacy complaint has been a core fair information practice for thirty years. The Requirements document states several requirements related to challenging compliance (section 4.10, p. 40). Because these requirements are administrative and have no technical components, the P&S conceptual architecture does not directly address them.

3.3 Information Security Requirements

ISO/IEC 17799-1:2005 *Code of Practice for Information Security Management* is a widely adopted international standard for information security management. The Code opens with an introduction describing information security and detailing why it is needed, how to assess security requirements and how to assess risks and assign controls. The remainder of the standard is organised into eleven sections, each covering a key control area for information security. Together these describe the working objectives of the Code of Practice. The eleven information security control areas are:

1. **Information Security Policy**: Each jurisdictional implementation of the EHRi will operate under a security policy appropriate to the jurisdiction and the features of the EHRi that are operational in that jurisdiction. General security policy requirements are stated in Canada Health Infoway, Electronic Health Record Privacy and Security Requirements, 2005, section 5.3, page 45.
2. **Organising Information Security:** Requirements for information security management are stated in the Requirements document (see reference above), section 5.4, page 46. The Policy Management Service described in section 8.1 assists with security management.
3. **Asset Management:** Requirements for asset are stated in the Requirements document, section 5.5, page 45. Section 5 of the current document (page 22) discusses the EHRi assets that the P&S conceptual architecture is designed to secure.
4. **Human Resources Security:** The objectives of human resource 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; and prevent damage from security incidents and malfunctions caused by human error. The requirements for human resources security are discussed in the Requirements document, section 5.6, page 51 *ff*. Further discussion of human resources security is out of scope of this conceptual architecture document.
5. **Physical and Environmental Security:** Physical and environmental security aims to prevent unauthorised 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. Although it is an essential component of any robust security implementation, physical security will not be discussed further in this document because physical security is the responsibility of the implementing jurisdiction and must be customised to accommodate the exact physical environment in which each EHRi component operates

   The requirements for physical security are discussed in the Requirements document (see reference above), section 5.7, page 54 *ff*. Further discussion of physical security is out of scope of this conceptual architecture document, as physical security requirements will be the responsibility of the implementing jurisdiction.
6. **Communications and Operational Security:** The objectives of operational security are to ensure the correct and secure operation of information processing facilities; minimise the risk of

systems failures; protect the integrity of software and information; maintain the integrity and availability of information processing; ensure the safeguarding of information in databases and supporting infrastructure; prevent damage to assets and interruptions to business activities; and prevent loss, modification or misuse of information exchanged between organisations.

Requirements for operational security are specified in the Requirements document, section 5.8, page 56 *ff*. With the exception of data security (see below), most aspects of operational security for the EHRi are the responsibility of the implementing jurisdiction, further discussion of operational security is out of scope of this conceptual architecture document.

Data security aims to protect the confidentiality, integrity and availability of all data repositories. Requirements for data security are discussed in the Requirements document, section 5.8.7, pages 59 *ff*. The P&S conceptual architecture will ensure data security through a combination of identity protection services including pseudonymisation (see section 7.7), encryption services (see section 7.9, and physical security.

Communications security aims to protect (principally via encryption) the confidentiality and integrity of every message transmitted from, to, or within the EHRi. The EHRi common services will not accept message traffic whose confidentiality and integrity are not protected. Requirements for communications security are discussed in the Requirements document section 5.8, page 56 *ff*. Communications security is covered below in the discussion of encryption services (see section 7.7).

7. **Access Control:** Access control includes identification of users during registration, their subsequent authentication during log in, and their authorisation prior to being granted access to services and data. Access control is intended to prevent unauthorised access to information systems; ensure the protection of services; prevent unauthorised computer access; detect unauthorised activities; and ensure information security when using mobile computing and tele-networking facilities.

   User identification requirements are stated in the Requirements document, section 5.9.2, pages 68 *ff*. Authentication requirements are stated in section 5.9.6, pages 75 ff. User authorisation requirements are stated in section 5.9.2.2, pages 70 *ff*.

   There are so many issues related to access control that this document deals separately with user registration (see section 7.3), user authentication during log in (see section 7.4), and other aspects of user access control and authorisation (see section 7.5).

   This document discusses two distinct approaches to the whole topic of access control (including user registration, authentication, and authorisation). These separate approaches are discussed in section 7.2.

8. **Information Systems Acquisition, Development and Maintenance**: The objective is 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.

   The relevant security requirements are stated in section 5.10 of the Requirements document, pages 77 *ff*. Many of the P&S services support these services. Appendix B relates each of the requirements for Information Systems Acquisition, Development and Maintenance to one or more P&S services.

9. **Security Incident Handling**: The objectives of security incident management are to build a reporting infrastructure for reporting incidents and weaknesses; to minimise the damage from security incidents and malfunctions; and to manage incidents and institute improvements to prevent their future occurrence.

   Requirements are stated in the Requirements document, section 5.11, pages 80 *ff.* Security incident handling in the EHRi is supported by Secure Auditing Services (see section 7.11). It also makes use of the EHRi notification and alerts service.

10. **Business Continuity**: This is largely dependant on specific implementation details and so detailed consideration of business continuity considerations is beyond the scope of a conceptual architecture. Nevertheless, some essential aspects of business continuity such as secure backup 1 are briefly discussed in this document.
11. **Compliance**: The secure auditing services (see section 7.11) greatly support compliance efforts but ultimately, compliance is a jurisdictional concern and clear policies for compliance audits must be set by those in each jurisdiction who are responsible for governance of the EHRi.

4 P&S Conceptual Architecture

This section provides an overview of the conceptual architecture and introduces ten P&S services that together will satisfy all the P&S requirements discussed in the previous section. The architecture is based on a vision of a desired future state of how the EHRi should operate in years to come. This future state has certain key characteristics that are briefly described and also comes with a set of assumptions that must first be met.

4.1 Overview

The EHRi is a message based architecture that allows users to access data in an EHRi data repository as well as one or more domain repositories (e.g.: a repository of laboratory test results or a repository of patient/person prescription drug profiles). Users access this data by interacting with either a POS system connected to the EHRi or with a clinical portal whose back end is connected to the EHRi. In every case, the user interaction causes an HL7 version 3 message to be constructed (by the POS system, by middleware connected to the POS system, or by the clinical portal system) and then sent to the EHRi common services.

Conceptually, the Health Information Access Layer (HIAL) acts as a filter to ensure that confidential PHI is never collected, used or disclosed inappropriately. The ten P&S services shown in the diagram – part of a larger suite of common services built into the HIAL – work together to create the mesh in that filter:

The EHRi also draws upon several additional information repositories:

1. a client registry containing an entry for all (or most) patients/persons resident in the jurisdiction;
2. a provider registry containing an entry for each regulated healthcare provider practicing in the jurisdiction; and
3. a user registry containing an entry for each EHRi user who is registered under the EHRi trusted user management model (see section 7.2 and 7.3 for a discussion of the user registry).

In addition to these data repositories, the EHRi also provides accessing systems with common services that facilitate access to and update of the repositories. P&S services are among the many common services that the EHRi will provide. Figure 2 below lists all of the EHRi common services, including the P&S services. Figure 3 presents the ten P&S services.

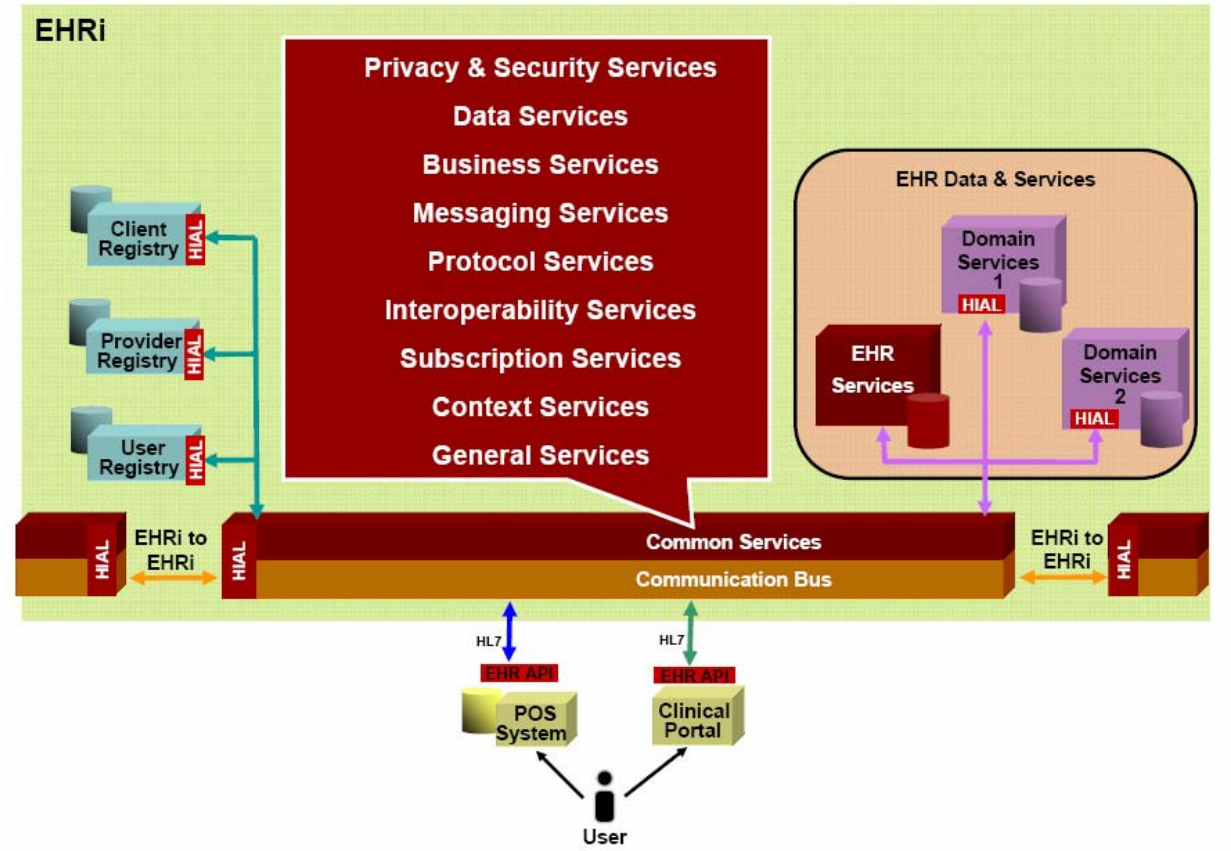

Figure 2: P&S services and their relation to EHRi common services

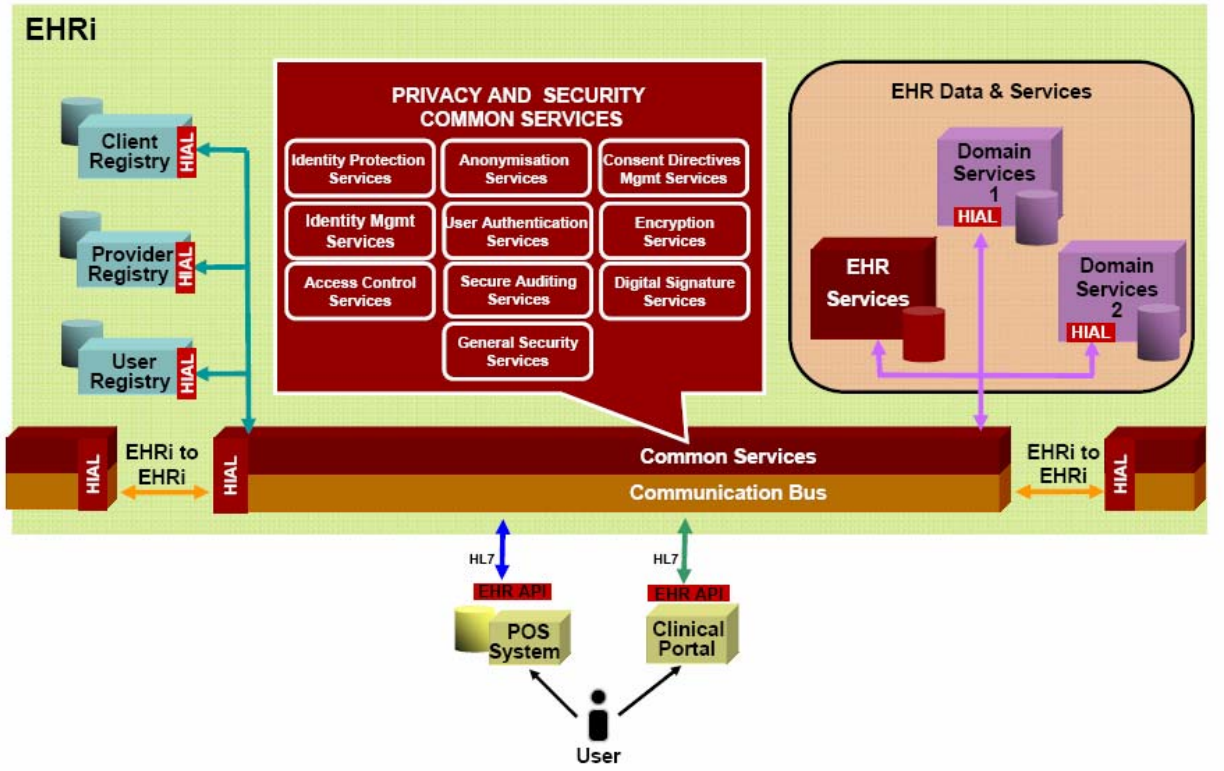

Figure 3: The ten P&S Services

4.2 Future and Interim States

An interoperable EHR will not be built in a day. When it is, not every POS system in Canada will immediately connect to it. It is essential that Infoway plan for the implementation of the EHRi to evolve over a period of years. For the purposes of this document therefore, a distinction is drawn between the desired future state of P&S in the EHRi (i.e., the long-term vision of how these services will operate), and interim states that allow existing POS systems to be connected with only modest changes to existing systems and workflows. The P&S services discussed in section 7 describe a desired future state where the P&S conceptual architecture is fully deployed. Section 9 discusses potential interim states that jurisdictions and healthcare organisations may pass through on their way to a full deployment.

The desired future state of the P&S architecture will have the following key characteristics:

1. a user registry will play an important role in user registration, authentication, and access control for the EHRi;
2. the architecture will support multiple approaches to managing user identity, authentication and authorisation;[24]
3. the architecture will support domain repositories that retain their own identity management, user authorisation and consent directives management and will provide identity management, access

[24] It is important to note that support for multiple approaches to authentication does not imply multiple standards of rigour for authentication. There will be no "back doors" to the EHRi. Nor will there be "screen doors" (i.e., approaches to authentication that are easily surmounted).

control and consent directives management configurations that accommodate these domain repositories;

4. the architecture will manage consent at the EHRi common services level (where possible) and at the domain repository level (where necessary);
5. the architecture will support a variety of consent directives (e.g., record and field level) for EHR repository data at the EHRi common services level (see section 7.6.9 below);
6. the architecture will strive to lower administration effort.
7. the architecture will enforce secure communication between jurisdictions for EHRi-to-EHRi interactions and between POS systems or clinical portals and the EHRi.

Several assumptions underlie this proposed future state:

Assumption 15	Each jurisdictional domain either trusts the jurisdictional EHRi or else the EHRi is a registered "user" of the domain services and has appropriate levels of controlled access needed to perform its functions.
Assumption 16	Each EHRi trusts every other EHRi based upon implementing data sharing agreements, trusted connection requirements and the P&S services described in this document.
Assumption 17	Consent directives will be obtained from patients/persons and entered into a POS system or clinical portal and thence transferred to the EHRi. These consent directives will then be accessible to the EHRi.
Assumption 18	Consent directives pertaining to PHI in the EHRi will be managed by the EHRi common services and the directives will be applied by the EHRi before any access request is granted.
Assumption 19	Patients'/persons' consent directives will be stored and transmitted as outlined in section 7.6.7 (Approaches to Consent Directives Management).

5 EHRi Information Assets To Be Secured

This section lists the information assets that must be protected, identifies the aspects of confidentiality, data integrity, system availability, and auditability requirements that must be met, and presents how these assets are classified for the purposes of security.

5.1 Inventory of Assets

The P&S CA is designed to secure the following EHRi information assets:

Information Asset	Aspects to Be Protected			
	Confidentiality	Integrity	System Availability	Auditability
1. data in the EHR data repository	√	√	√	√
2. data in domain repositories connected to the EHRi	√	√	√	√
3. data in the client registry[25]	√	√	√	√
4. data in the provider registry	√	√	√	√
5. data in the user registry, including data obtained during registration	√	√	√	√
6. security critical data	√	√	√	√
7. messages to, from and within the EHRi	√	√	√	√
8. all EHRi common services and their supporting applications	**N/A**[26]	√	√	√
9. EHRi applications that support the client registry, provider registry, user registry and domain repository	**N/A**	√	√	√
10. clinical portals to the EHRi and their supporting applications	**N/A**[27]	**N/A**	√	√

[25] The Client Registry refers to a jurisdictional registry of all patients/persons within the jurisdiction or who have received healthcare within the jurisdiction. The client registry will contain, by definition, identifying information. To the extent that this information may be linked with information in the EHRi data repository or domain repositories (and it will be of scant use if it isn't) then this client registry information will also be, by definition, personal health information. It therefore falls under the general umbrella of information assets whose confidentiality, integrity and availability must be protected. Refer to Infoway's EHRS Blueprint for further details on the Client Registry.

[26] Although the confidentiality of application source code is not being explicitly protected within the architecture, access to such applications is fully secured.

[27] All data to and from the clinical portal will be protected and access to the portal will be strictly controlled by means of common authentication services and access control services. As noted in section 1.3 (Scope), network security and server security are a jurisdictional responsibility and while it is presumed by this architecture that robust network and server security are in place, they are not discussed further in this document.

5.2 Data Classification

The P&S services are constructed to safeguard personal information in general and PHI in particular. For the purposes of protecting the **confidentiality** and **integrity** of EHRi information assets, these assets will be classified as follows:

1. All PHI will be uniformly classified[28].
2. All data in the EHR repository[29] will be deemed PHI (and hence uniformly classified within the EHRi as *PHI*).
3. All data in the domain repositories connected to the EHRi will be deemed to be (from the point of view of the EHRi) PHI (and hence uniformly classified within the EHRi as *PHI*).
4. All messages to/from the EHRi that contain any personal information will be deemed to be (from the point of view of the EHRi) PHI[30].
5. All data in the client registry will be uniformly classified as PHI.
6. All data in the provider registry and in the user registry will be uniformly classified as personal information.
7. Security critical data not listed above, including

- data used during user authentication;
- data used in authorisation and user privilege management to determine what actions an individual user can perform and which data the user can access;
- configuration data for firewalls, intrusion detection systems and other software and hardware resources used to secure components of the EHRS; and
- private or secret cryptographic keys used for encrypting or decrypting data or for generating digital signatures.

For the purposes of protecting the **availability** of EHRi information assets from denial of service attack, equipment failures, or disasters (fire, flood, power failure, etc.), these assets will be classified as follows:

---

[28] The important point about the uniform classification of data for the purposes of confidentiality and integrity is that *all* PHI will be treated in the strictest confidence while residing in or transmitted by the EHRi. Readers are cautioned not to infer from uniform classification that all EHRi users will therefore be able to access all data. On the contrary, a variety of access control methodologies will strictly limit the access of users to just that data needed to perform their professional duties as healthcare providers; as determined by their role(s), work groups and relationships to patients/persons (see section 7.5). Readers are also cautioned not to infer from uniform classification that patients/persons will not be able to place their own restrictions on who can access their data and what data is accessible. A variety of means will exist to allow patients/persons to withdraw or revoke their consent to disclose their data. These consent mechanisms are discussed in section 7.6.

[29] From a conceptual view, data in the EHR repository consists entirely of electronic health records on patients/person (or portions thereof). Actual implementations of EHR repositories may contain other non-personal, non-health related information (e.g.: configuration data, meta-data, etc.). Classification of such extraneous information (where appropriate) is beyond the scope of this document.

[30] The EHRi common services could conceivably send messages containing personal information (i.e., information that identifies, alone or in combination with other information, a specific individual) without these messages containing any health information. Yet surely such messages will be rare (if they exist at all), since the EHRi common services are constructed for the express purpose of enhancing health care and is unlikely therefore to ever convey personal information bereft of a healthcare context. For this reason, all EHRi messages containing personal information will be classified for the purposes of confidentiality and integrity as PHI.

1. All PHI will be uniformly classified.
2. All data in the EHR repository will be deemed PHI (and hence will have the same availability classification as all other EHRI information assets deemed to be PHI).
3. All data in the domain repositories connected to the EHRi will be deemed to be (from the point of view of the EHRI) PHI (and hence will have the same availability classification as all other EHRi information assets deemed to be PHI).
4. All messages to/from the EHRi that contain any personal information will be deemed to be (from the point of view of the EHRi) PHI (hence will have the same availability classification as all other EHRi information assets deemed to be PHI).
5. All data in the client registry, provider registry, and the user registry and all security critical data required to authenticate and authorise EHRi users will be uniformly classified for the purposes of availability.
6. All EHRi common services and all clinical portals connect to the EHRi will be uniformly classified for the purposes of availability.

6 Overview of P&S Services

This document identifies ten P&S services that are critical to the protection of PHI in the EHRi. These services are part of a larger suite of data protection tools that all users of PHI in an EHRi environment must adopt, including various data protection policies and procedures, privacy and security training for EHRi users, as well as potential accreditation of EHRi users and the organisations they represent in order to ensure that they have met their responsibilities for protecting PHI in the EHRi. Infoway thus recognises that the successful protection of PHI in the EHRi depends on an optimal mix of both policy *and* technology instruments[31].

The ten P&S services described here would be classified as "technology", rather than "policy", instruments for protecting PHI. Because the document provides a P&S *conceptual* architecture, these services do not prescribe specific technologies, vendor products or operating system environments. Infoway recognises, however, that EHRi users will eventually adopt specific privacy and security technologies to support the implementation of the P&S services identified in this document.

The research and practical applications aimed at developing privacy enhancing technologies are not as mature as other initiatives in the field of information security, at least from a standards-setting perspective. For this reason, Infoway encourages users of PHI to work closely with system developers, privacy architects and other privacy stakeholders such as community representatives and Privacy Officers at health information custodians to support the development of system-specific design features that protect the privacy of patients/persons in the EHRi, as well as other privacy enhancing technologies. For this reason, the ten P&S services described here are also not categorised into separate privacy *or* security services. This is because Infoway believes that privacy and security must "reside together" [32] for effective data protection, in spite of the "lag" in research and development for privacy enhancing technologies, both generally and, specifically, for information systems in healthcare.

The following list summarises the ten P&S services that will provide most of the P&S functionality within the EHRi as well as a group of common services with P&S implications:

1. a **User Identity Management Service** that includes service components to address the need to accurately identify users of the system. It handles tasks such as registering users, assigning roles that define their access privileges (e.g. a podiatrist may not be able to access mental health data), and managing changes in user status.
2. a **User Authentication Service** – a transactional service that builds upon identity management to establish the validity of the claimed identity of a user logging into the system and thereby providing protection against fraudulent transactions. In order to rationalise management of sessions in which users have access to confidential information, authentication tokens are generated with protective characters such as user ID and time-out.
3. an **Access Control Service** that provides access control methodologies as part of a unified privilege management service for EHRI users[33]. This service is essential for ensuring the

[31] Section 10.3 lists some of the many policies that will need to be developed before operation of EHRi can be fully realised.

[32] "The Security-Privacy Paradox: Issues, Misconceptions and Strategies", a joint report by the Office of the Ontario Information and Privacy Commission and Deloitte & Touche, August 2003. The report is available at: http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=14447&N_ID=1&PT_ID=11351&U_ID=9101929818.

[33] Readers familiar with ISO/IEC 17799, an international standard that Infoway has used as an organising framework for the EHRi security requirements (see References at the end of this document), will be aware that ISO/IEC 17799 includes user identification and registration, user authentication, and authorisation within its section on Access Control. Because of the complexity of these topics, this document discusses both user identification and user authentication in their own sections. The access

confidentiality and integrity of PHI. Three models may be followed: (1) role-based access control, where access to specific types of PHI is based on the role played by the user as determined by (for example) their professional accreditation), (2) work group based access control, which bases access to a given patient/person's EHR upon the user's membership in one or more work groups (such as clinical teams or staff of a family practice), and (3) discretionary access control**,** which allows users with a legitimate access to a patient/person's EHR (e.g., a family physician) to grant access to other users who have no previously established relationship to that patient/person's EHR (e.g., a specialist). Subcomponents of the access control service include management of business rules for access control (translating access control policy into automated business rules that can be applied in real time); assignment of roles to users; associating individual users with groups of users (e.g.: care teams, and clinic staff); managing the association between users and the patients/persons whose care they will participate in; rapid suspension of user access privileges; and authorising users.

4. a **Consent Directives Management Service** that translates privacy requirements arising from sources such as legislation, policies, and individuals' specific consent directives, and applies these requirements in an EHR environment. The service relies on a common privacy vocabulary based on Canadian health data protection statutes and other privacy laws, as well as on recognised best practices in privacy protection such as the CSA Model Code. A component service manages consent related business rules, e.g., procedures for recording patient consent directives, validating consent, or overriding consent directives. Another component allows individuals to grant, withhold or withdraw their consent for the collection, use or disclosure of their PHI in accordance with applicable privacy legislation and policies. It also allows input such as the identification of an authorised substitute decision maker (where applicable), and the involved patient/person's stipulations of which EHR infostructure system users are allowed access to his/her PHI. Transactional components serve to validate consent, to map consent directives among jurisdictions and, where necessary, to override consent. A patient access control service allows patients to restrict access to specific components of their EHR, e.g., their prescription drug profile. A prototype of this type of patient access control is seen in the BC Pharmanet system. For more information on consent, including a description of jurisdictional consent requirements, see Appendix C – Informational Consent.
5. an **Identity Protection Service** that will facilitate the separate storage of personal information that uniquely identifies individuals (e.g. name, address, health card number, etc.) from health information relating to their care and treatment, diagnosis, etc. This service would provide authorised users with seamless access to PHI through the use of a linking table or service connecting an individual's public identifier (PID) with his/her personal health information (PHI) without the two data sets residing in the same physical location. Conceptually, the service would be made up of four tables or data stores: one table containing identifying information (e.g. name, address, emergency contact information) stored under an individual's PID (such as a health card or health insurance number), a second table containing health information stored under an individual's EHRi client identifier (ECID), a meaningless but unique number that is only known or used within the jurisdictional implementation of the EHRi[34] and the client registry for the purpose of resolving an individual's identity, a third table that maps an individual's PID to his/her corresponding ECID and, lastly, for the purpose of facilitating cross-jurisdictional access to PHI, a fourth table that would contain a patient's/person's ECID (at least one EHRi client ID would exist for a patient/person in each jurisdiction where they have received care or treatment)

---

control section of this document builds upon these two previous sections to discuss user privilege management and authorisation of users who have already been identified during to registration and authenticated during log in.

[34] A number of identity protection services could be deployed within any single region (e.g. within each domain repository as well as the EHR). However, Infoway recommends that the identity protection service be deployed at the EHRi common services level of the EHRi – i.e. provincially or multi-provincially.

mapped to another meaningless but unique number known as a federated identifier (FID).[35] FIDs will allow for PHI to be shared between jurisdictional implementations of the EHRi without disclosing a patient's/person's ECID. The identity protection service would resolve a patient's/person's PID (provided by an authorised EHRi user) to an ECID that could be used to retrieve the patient's/person's PHI stored within the EHRi or could be again resolved to an FID to retrieve PHI stored in other jurisdictions. In addition, a pseudonymisation service will provide pseudonymised health information to authorised researchers, public health surveillance officials and other authorised users; such pseudonymised information will contain a meaningless but unique identifier that operates in much the same manner as the ECID described above – e.g. the pseudonymous ID is linked to the patient/person's PHI in such a way that the patient/person's identity is never revealed (this identifier functions as a pseudonym for the patient/person, hence the name pseudonymisation). However, the pseudonymised identifier *would not be* linked to a patient/person's PID and the related identifying information. Such pseudonymised data allows for longitudinal studies.

6. an **Anonymisation Service** that takes PHI representing an identifiable individual and then removes all personal identifiers. The goal is to make information accessible to secondary users of healthcare data (healthcare researchers and administrators) without infringing on patient privacy. In some cases, pseudonymisation (use of a unique code designation in place of identity-revealing material) may be preferred to complete anonymisation. Both anonymisation and pseudonymisation are technically complex, and all means of inferring identities must be forestalled by the service, particularly where data subjects are persons with rare or distinctive attributes or situations.[36]
7. an **Encryption Service** that maintains data confidentiality using cryptography. Component services include key management (creating, renewing, and revoking encryption keys); encryption of EHR data within databases; encryption of stored data such as backup files and

[35] FIDs are meaningless but unique numbers used for the purpose of linking ECIDs in different jurisdictions under a unique identifier and would typically only be generated when the patient/person had received healthcare services in more than one jurisdictions – i.e. one FID would link two or more ECIDs corresponding to the same patient/person.

[36] The ACIET report "Preliminary Draft Of The Pan-Canadian Health Information Privacy And Confidentiality Framework" defines several methods by which information can be rendered anonymous. Non-identifying information may have identifiers removed or altered using the following methods:

1) Two-way encrypted/scrambled information means personal health information that has been processed by mathematically converting the information, so as to render it unidentifiable without the key to decode it.
2) Stripped information means personal health information that is altered in a consistent manner over time, so that the subject individual cannot be identified, directly or by a reasonably foreseeable method, either from the information itself or in combination with other available information.
3) Anonymous information (or Non-Nominal Information) means personal health information that has been altered by removing personal identifiers such as names, addresses, phone numbers and identifying numbers such that the resulting records are essentially anonymised when viewed in isolation from other contextual information. However, information representing distinguishing characteristics may be sufficient to re-identify the individual when compared with other information sources which have both the distinguishing characteristics and the names.

If personal health information is rendered non-identifying, it is no longer personal health information as defined and therefore, the rules relating to personal health information do not apply. Notwithstanding the above, a jurisdiction may wish to implement best practice guidelines for protecting non-identifying information, or to include provisions related to the protection of non-identifying information in a data access agreement.

archives; and encryption of data (such as messages) during transmission. Several other services in this list will rely upon the encryption service.

8. a **Digital Signature Service** that allows a health care professional to sign a digital document (e-mail, electronic health record, etc.) in much the same way that they would apply a signature to paper, and with the assurance that that the signature cannot be forged and neither the document nor the signature can be altered without rendering the signature invalid. Component services include generating digital signature key pairs, ensuring that private digital signature keys remain protected, and publishing each participant's identification and signature verification key in a document called a "digital certificate." Other component services include application of digital signatures to data; digital signature verification; and digital time stamping as well as a "digital notary service" ensuring that the value of the digital signatures does not degrade over time due to technical obsolescence.
9. a **Secure Audit Service** to record significant privacy and security-related events in an event log. Component services include event logging and log analysis.
10. **General Security Services** such as scanning for viruses, secure backup and restoration of data, secure data archiving, and secure data destruction.
11. Other EHRi common services that have P&S implications, such as:
    a. a **policy management service** that works as a uniform way to access, modify and coordinate the privacy-related business rules that the P&S services (among others) operationalise. Examples of services that rely upon these privacy-related business rules include the Access Control Services, User Identity Management Services, Identity Protection Services, and Consent Directives Management Services.
    b. **session management** (opening, closing and terminating user sessions),
    c. **client registry** (to the extent that it might be used to note patients/persons whose privacy and security are at elevated risk),
    d. **provider registry and user registry** (resolution of provider identifiers),
    e. **notification** (notifying a privacy officer of a user over-riding consent directives or accessing locked data, or notifying a security officer of a security-related event or potential security breach),
    f. **messaging**, and
    g. management of access by patients/persons to their EHR.

Each of the privacy and security services are shown in the following diagram, together with the EHRi's other services (data services, business services, messaging services, protocol services, subscription management services, context services and general services). These other EHRi services are described in the EHRS Blueprint.

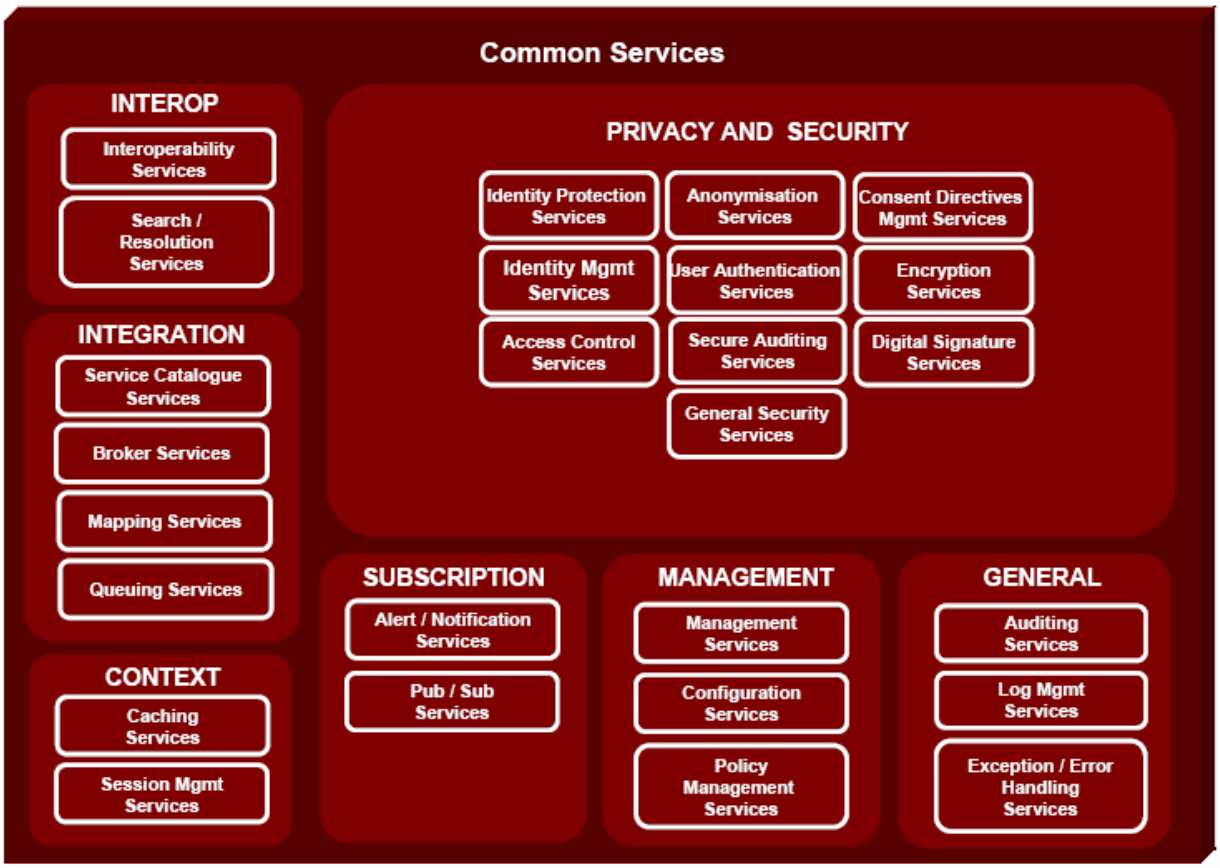

Figure 4: EHRi services, including P&S services

6.1 Types of Services

In addition to P&S services and service components (all of which are described in detail), several services and service components listed below are referred to as "*called* EHRS services" or "*called* EHRS service components." These services and components are not P&S specific; rather, they are more general services that are provided by the broader EHR Infostructure. Examples of such are the "Notification Services" that are needed to alert healthcare providers and EHRS administrators to a variety of events (e.g., the delivery of a critical lab test result). These notification services are also needed to alert privacy officers of potential privacy policy violations and to alert security officers of critical security events, but since the current document is limited to a discussion of P&S-specific services and service components, the general notification services are not described further in this document.

6.2 Categorisation of Services

Each P&S service is categorised into one of three groups:

1. Services that are administrative in nature – these services are used episodically to perform tasks such as registering an EHRi user, recording a patient/person consent directive, or revoking a digital signature certificate.
2. Services that are transactional in nature – these services are continually called upon to perform tasks such as authenticating a user, applying consent directs to determine whether a user has

access to an EHR, or encrypting data. Services may call and / or be composed of service components.

3. Services that support general IT security infrastructure – these provide essential and well-understood support for tasks such as securely backing up data and protecting against malware (computer viruses). These common and well-known services are only briefly described in this document in section 1.

6.3 Summary of Service Components for Privacy and Security Services

Service	Type	Category
User Identity Management Service[37]	**Service**	
• Register user	Called service (no details)	Administrative
• Assign role(s) to user	Service component	Administrative
• Manage user identity (includes generate unique identifier for user, looking up unique identifier for a user, suspend/revoke user access)	Service component	Administrative
User Authentication Service	**Service**	
• Authenticate user	Service component	Transactional
• Generate authentication token	Service component	Transactional
Access Control Service	**Service**	
• Manage business rules for user privilege management (e.g., which roles can access which data and services, etc.)	Service component	Administrative
• Manage user's role	Service component	Administrative
• Manage association between user and work group	Service component	Administrative
• Manage association between user and patient/person	Service component	Administrative
• Authorise user (e.g.: determine for a given user with a given role and in a given work group whether the user can access a data field from a given patient/person's EHR)	Service component	Transactional
Consent Directives Management Service	**Service**	
• Manage consent-related business rules (e.g., revoking consent for use automatically revokes consent for disclosure; enumeration of valid collection purposes, etc.)	Service Component	Administrative

[37] Users may be patient/persons who have direct online access to portions of their EHR as well as substitute decision makers. Users may also be systems and applications.

Service	Type	Category
• Manage patient/person consent directives (grant or withhold, withdraw or revoke) -- includes flagging to users the existence of blocked or masked data	Service Component	Administrative and Transactional
• Validate consent (includes validation of collection purpose)	Service Component	Transactional
• Map consent (between and among jurisdictions)	Service Component	Administrative
• Override consent (e.g. emergency override)	Service Component	Transactional
• Patient/person access control service (allows patient/person to grant access and/or override previous consent directives)	Service component	Administrative/transactional
• Log consent directives and their application	Called EHRS service component	Transactional
Identity Protection Service	**Service**	
• Retrieve public identifier	Called EHRS service component	Transactional
• Resolve jurisdiction identifier for patients/persons	Service component	Transactional
• Manage internal and federated identifiers for patients/persons	Service component	Transactional
• Pseudonymise data (for secondary purposes such as research)	Service component	Administrative and Transactional
Anonymisation Service	**Service**	
• Anonymise data (for secondary purposes such as research)	Service component	Administrative and Transactional
Encryption Service	**Service**	
• Key Mgmt Service (generation, key revocation, backup)	Service components	Administrative
• Data Storage Encryption (files, data stores)	Service component	Transactional
• Database Encryption	Service component	Transactional
• Encrypt/decrypt message (data in transit)	Service component	Transactional
Digital Signature Service	**Service**	
• Digital Signature Key Mgmt Service (generation, key revocation) – see also key mgmt services for encryption/decryption	Service components	Administrative
• Digitally sign data	Service components	Transactional

Service	Type	Category
• Verify digital signature	Service components	Transactional
• Digital Timestamp and Digital Notary service (including refresh of old digital signatures)	Service components	Transactional
Secure Audit Logging Service	**Service**	
• Securely log events (includes access to data, Changes to Data, Consent Override, Denial of Access, EHR transaction, message transmission)	Called service component	Transactional
• Analyse log (includes all records accessed by a user, all users who have accessed a patient/person's EHR, all users who have accessed EHRS of patient/persons at elevated privacy risk, and all users with suspicious patterns of use)	Service component	Administrative and/or transactional
General Security Service	**Service**	
• Scan for and protect against malware	Service component	IT Infrastructure Mgmt
• Secure backup/restoration of data	Service component	IT Infrastructure Mgmt
• Data Archiving	Service component	IT Infrastructure Mgmt
• Secure data destruction	Called EHRS service component	IT Infrastructure Mgmt

6.4 Summary of Other EHRi Common Services With P&S Implications

Service	Type	Category
Session Management Service	**Service**	
• Session mgmt (includes opening, securing, closing and timing out sessions)	Called EHRS service component	Transactional
EHR Services	**Service**	
• Mark EHR of patient/person at elevated privacy risk	Service component	Administrative
Notification Service	**Service**	
• Notify on override of consent directive	Called EHRS service component	Transactional
• Notify on security event occurrence	Called EHRS service component	Transactional
Messaging Service	**Service**	

Service	Type	Category
• Send acknowledgement of message receipt	Called EHRS service component	Transactional
Patient/Person PHI Access Service		
• Manage patient/person PHI requests (request amendment to PHI; attach patient/person statement of disagreement with PHI;[38] attach reason for denying request; notify prior recipients of amendments)	Service component or issue to be addressed or EHRi common service component	Administrative

6.5 A Conceptual Data Model for the P&S Services

Appendix D contains conceptual data models for all the major data components of the EHRi P&S architecture. Readers familiar with data modelling concepts and with the Unified Modelling Language (UML) are encouraged to examine the two figures in Appendix D in detail. Non-technical readers or those not familiar with UML are advised to skip to the next section.

[38] Although no specific P&S service exists to facilitate this requirement, the EHRi data model will allow for the recording of patients'/persons' challenge to the accuracy of their PHI.

7 P&S Services

7.1 Introduction

Full implementation of the P&S requirements requires implementation of all ten of the P&S services described in the sub-sections that follow. Each sub-section contains the following:

1. a description of the service,
2. a rationale for each service,
3. a diagram that describes the service as part of the EHRi common services framework. The connection of POS systems and clinical portals to the EHRi are illustrated.
4. policy management requirements for the service, where applicable.
5. an example of process flow for the service, and
6. requisites for the operationalisation of the service.

However, before describing the P&S services, one must consider the whole dimension of trust in connections to the EHRi.

7.2 Trusting Connections to the EHRi

Trust is a chain built from many links. Are policies adequate? Are they effectively implemented by administrative procedures? Are technical requirements sufficiently rigorous? Have these requirements been met? Careful analysis of every link in the chain of trust is an essential component of EHRi governance (see section 10). What links are required to ensure that healthcare providers trust the EHRi as a timely and accurate source of clinical information? What links will promote patient/person trust in the EHRi as a safe repository for their PHI? What does each jurisdiction implementing the EHRi need to trust other jurisdictional implementations of the EHRi; i.e., what is needed before disclosures of PHI can cross jurisdictional boundaries? Infoway will work in collaboration with stakeholders to comprehensively answer these questions in a manner that ensures interoperability and that the chains of trust are forged to last.

Organisations must meet many administrative and technical requirements before establishing a trusted connection to the EHRi (more than two dozen administrative and eighty technical requirements are defined in the Requirements document). Furthermore, several of these technical requirements listed in the Requirements document have a profound impact on the design of the following three P&S services:

1. **identity management** – who will register the many tens (perhaps hundreds) of thousands of healthcare professionals who may ultimately make use of the EHRi? Many organisations (including large hospitals) have robust user identification and registration. Should users of such hospital systems need to register all over again to obtain access to the EHRi? This would be no trivial undertaking – given the recent trend in hospital amalgamations in some jurisdictions, a single large hospital may have over a thousand users of its POS system. Moreover, the added security would be questionable – who better knows the identities of its users than the institution that employs them? Regardless of whether organisational identity management can be trusted in a given organisation, many tens of thousands of potential users of the EHRi will not belong to an organisation (e.g.: sole practitioners and their medical receptionists; the latter likely needing access to selected EHRi data such as demographics and patient/person identifiers). Such users will require a means to directly register for access to the EHRi. The conceptual architecture therefore supports two methods of identity management: one where user registration is performed by healthcare organisations and then leveraged by the EHRi (see identity management deployment model 1 in section7.3.2) and one where user registration is performed as a direct service of the EHRi (see identity management deployment model 2 in section 7.3.2).
2. **authentication** – what constitutes sufficiently secure authentication of users by POS systems and clinical portals? This a non-trivial question, as no minimum standards for authentication for access to systems containing PHI exists in Canada (or most other countries, for that matter).

Whatever technologies are ultimately implemented, good security practice dictates that all users having access to a given security classification of data must be authenticated to a uniform level of rigour. As all PHI is uniformly classified (see 5.2), this mean that the overwhelming majority of EHRi users must be authenticated to the same level.

3. **access control** – which EHRi services and patient/person records can a given authenticated user access? At first glance, the question appears similar to the issue of identity management: this can either be administered by trusted organisations or administered directly by the EHRi. But administration of user privileges by trusted organisations carries with it additional complexities, since many aspects of access control varies among organisations; including roles, privileges and the grouping of EHR data and services for the purposes of access control. To allow organisational privilege management to be meaningfully applied to the EHRi, some form of mapping must take place between each organisation's user authorisations and the EHRi's. This important topic is pursued further in section 7.5.

In short, the EHRi needs to ensure that all users of EHRi services have verified identities, are authenticated during each EHRi session, and are authorised to access data and services. This document will focus on these three services with respect to determining trusted connections to the EHRi. Infoway does not suggest that multiple trust models will be supported by the EHRi. The P&S conceptual architecture proposes two components that make up the trusted EHRi connections: organisational trusted user management and EHRi trusted user management. These components are further discussed below.

7.2.1 Approaches to Trusted User Management

The three needs elaborated above (user identity versification during registration, user authentication during access, and authorisation prior to granting access), come together to create two models of what will hereafter be referred to as trusted user management:

- **Organisational trusted user management** – a healthcare organisation (a hospital, say) has a POS system that is capable of connection to the EHRi (directly or via middleware) and an adequate level of authentication. The organisation robustly registers all its POS system users, verifies their identities and assigns them unique user IDs. It manages its user privileges in a responsible manner that can also be rendered technically interoperable with the EHRi. The organisation's POS systems robustly authenticate each POS user upon login. In short, the organisation fulfills the requirements for trusted connections. When one of the organisation's users accesses the EHRi via the organisation's POS system, the EHRi will trust the user ID and role supplied by the POS system within the appropriate fields of an HL7 message. The EHRi does not know the name of the user and the user's contact info, but it has a (relatively distinguished) identifier from the POS system that the EHRi can record for audit purposes and a role that the EHRi can use to determine whether the user is authorised to access a given type of data. While an EHRi administrator may lack the information to contact the user directly, they can contact the user's organisation and the organisation *does* know the identity of the user and how to contact them.

  This approach has some significant advantage:

  - the management of user IDs is devolved to each organisation. These organisations already manage this registration information for their POS system users today, so both the administrative processes and the registries of such users already exist (albeit often embedded within proprietary POS systems);
  - user registration for this user community (largely centred on acute care) is a fait accompli. Given the large number of users, this is no small advantage;
  - this approach will furnish the EHRi with a comprehensive list of all trusted POS systems instantiated in trusted organisations (obtained through some yet-to-be-determined manual registration process for organisations and their POS systems establishing connections to the EHRi). This in turn facilitates the administration of trusted connections to the EHRi (a task that, one way or another, must be tackled if the EHRi is

to maintain control over connections and hence ensure the security of these connections); and

- it allows a staggered deployment of trusted connections to the EHRi; i.e., start with organisations that can be most trusted in terms of administrative rigour in the registration of their POS system users and choose first those POS systems that most readily comply with the P&S requirements for authentication.

This approach also has some disadvantages:

1. the EHRi will have to maintain the comprehensive list (mentioned in item 3 above) of all trusted POS systems instantiated in trusted organisations. There will be hundreds of organisations that may connect to the EHRi and potentially thousands of instantiations[39] of POS systems.
2. each POS instantiation will need its own unique ID and the EHRi will have to administer these IDs in the list mentioned above. Without such IDs, the user IDs stored within the appropriate fields of an HL7 message would likely not be unique and hence the EHRi would not be able to unique identify users accessing PHI (a core privacy requirement). These POS instance organisation IDs will therefore also be required within the HL7 message.[40]
3. the approach requires that the HL7 message also contain the user's role. This role must be meaningful to the EHRi. The mapping or transformation or substitution of EHRi roles for POS system roles is not a trivial undertaking (see the discussion of roles in section 7.5.3).
4. it is possible that the same user is registered in two distinct POS systems with two distinct IDs. Audits within the EHRi of user activity will not be able to relate these two user IDs to the same individual without first manually contacting the organisation involved and obtaining relevant user information. This lack of a unique electronic credential for each user makes detection of abnormal patterns of activity more complex.

- **EHRi trusted user management** – a would-be user of the EHRi who either does not already have access via an organisation (as above) or who wishes to obtain access outside the confines of an organisation's POS system (e.g.: via a web browse and a clinical portal). The user directly registers with the EHRi for subsequent access. The user's identity is verified during this registration. The user's role(s) is (are) captured and verified where necessary. When the user accesses the EHRi (via a clinical portal, say), the EHRi will prompt the user for their unique EHRi user ID and some secure form of user authentication will then take place (more on authentication in section 7.4.3). The EHRi trusts the user ID supplied by the user because it implements its own trustworthy user authentication process and the user ID is the one that was issued by the EHRi's own registration process. The user's role is retrieved from the EHRi in the user registry where it was recorded during user registration (or from the provider registry if the user is a regulated healthcare provider) and hence is implicitly trusted.

  There are advantages to this approach:

[39] By instantiation we mean the implementation of a specific POS system vendor product in a specific organisation, including the differentiation of two or implementations of the same system in those limited cases where mergers of healthcare institutions (hospitals, say) have created independent implementation of the same system.

[40] The reader might at first thought consider it sufficient to merely identify the organisation (i.e., with an organisation ID). But if more than one system from a single organization connects to the EHRi, we may need POS system information to resolve user identity, as it is possible that two POS systems in an organization may have the same user IDs for two different users; e.g. Dr. Robert Brown registered as RobB in POS1 and Dr. Robert Black registered as RobB in POS2.

1. users registered under this approach are all registered via a uniform (high quality) registration process. There is no possibility of variations in quality of registration as there are with the organisational trusted user management approach.
2. there is potentially less cost in retrofitting POS systems to merely act as a pass-through to an EHRi user login and authentication mechanism than there is in dealing with the complexities of trustworthy POS system authentication and insertion of meaningful role information into HL7 messages required by the organisational trusted user management approach.
3. No mapping or transformation or substitution of EHRi roles for POS system roles needs to take place, as it does with organisational trusted user management. Indeed, the user's role does not need to be included in the HL7 message. The user's roles within the EHRi are unequivocally established during EHRi user registration and directly tied to the user's EHRi user ID.
4. each user registered via this approach is issued exactly one unique electronic credential. This eliminates the potential disadvantage discussed above regarding the same user registered in two distinct POS systems with two distinct IDs (item 3 in the list of disadvantages for organisational trusted user management). This in turn simplifies auditing within the EHRi of user activity.
5. the registration model is very well suited to primary care and allows physicians and other healthcare providers not associated with a healthcare organisation (other than their own practice) to immediately register and reap the benefits of access to the EHRi via a clinical portal.

There are also disadvantages to this approach:

1. it does not leverage the significant investment in user registration within the acute care environment;
2. it does not allow users accessing the EHRi to be tied to an organisation, even where such ties exist, unless this is made part of the EHRi user registration process;
3. this approach is not readily amendable to providing users of POS systems with a single sign-on capability. Users who are already logged into a POS system may find themselves in the frustrating position of having to separately log into the EHRi.

Table 1 summarises the differences between organisational trusted user management and EHRi trusted user management.

Table 1: Organisational Trusted User Management vs. EHRi Trusted User Management

	Organisational Trusted User Management	EHRi Trusted User Management
Who registers users accessing the EHRi?	The organisation (via its internal user registration practices)	The EHRi, via its jurisdiction-wide user registration practices)
Who determines the user's role?	The organisation (as part of its user registration practices)	The EHRi, via its jurisdiction-wide user registration practices and its access to provider registries that contain professional role

	Organisational Trusted User Management	EHRi Trusted User Management
Who authenticates the user?	The organisation's POS system or clinical portal. The authentication of the user will take place when the user logs into the POS system.	The EHRi, via interaction with the user. This interaction can be: • direct (the user successfully navigates past an authentication page while using a web browser, say) • indirect (the user accesses EHRi services via a POS system that provides the user with an EHRi login service with a dialog box and related authentication functions in conformance with some EHRi user authentication protocol – see section 7.4.3) • (as an interim measure), scripted (the POS system stores the user's EHRi ID and supplies it to the EHRi login service.
What user data is contained in HL7 v3 messages sent from the POS system to the EHRi?	• Organisation ID • POS System Instance or Organisation ID (where required) • POS User ID • User Role [see the discussion of role based access control in section 7.5.3]	• EHRi user ID (role is already stored in the user registry, or obtainable by a link to the provider registry)
Who authorises the user to access a given EHRi service or patient/person data?	The EHRi (based on the user role provided by the organisation's POS within the HL7 message)	The EHRi (based on the user role provided during EHRi user registration and looked up by the EHRi)
What user identification is recorded by the EHRi's secure audit service?	The organisation's user ID and the Organisation ID (both are supplied by the POS system within the HL7 message requesting access)	The EHRi user ID (supplied by the user during log in and maintained for the duration of the user's session)

Throughout the rest of the document, connections by users to the EHRi (i.e. via POS systems and clinical portals) will be diagrammatically represented as either organisational trusted user management (green rectangle) or EHRi trusted user management (blue rectangle).

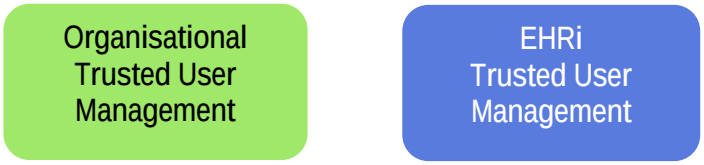

Figure 5: Trust Models for User Identity Management and Authentication

Revisiting Figure 3 on page 20, access to the EHRi would more accurate be represented as follows:

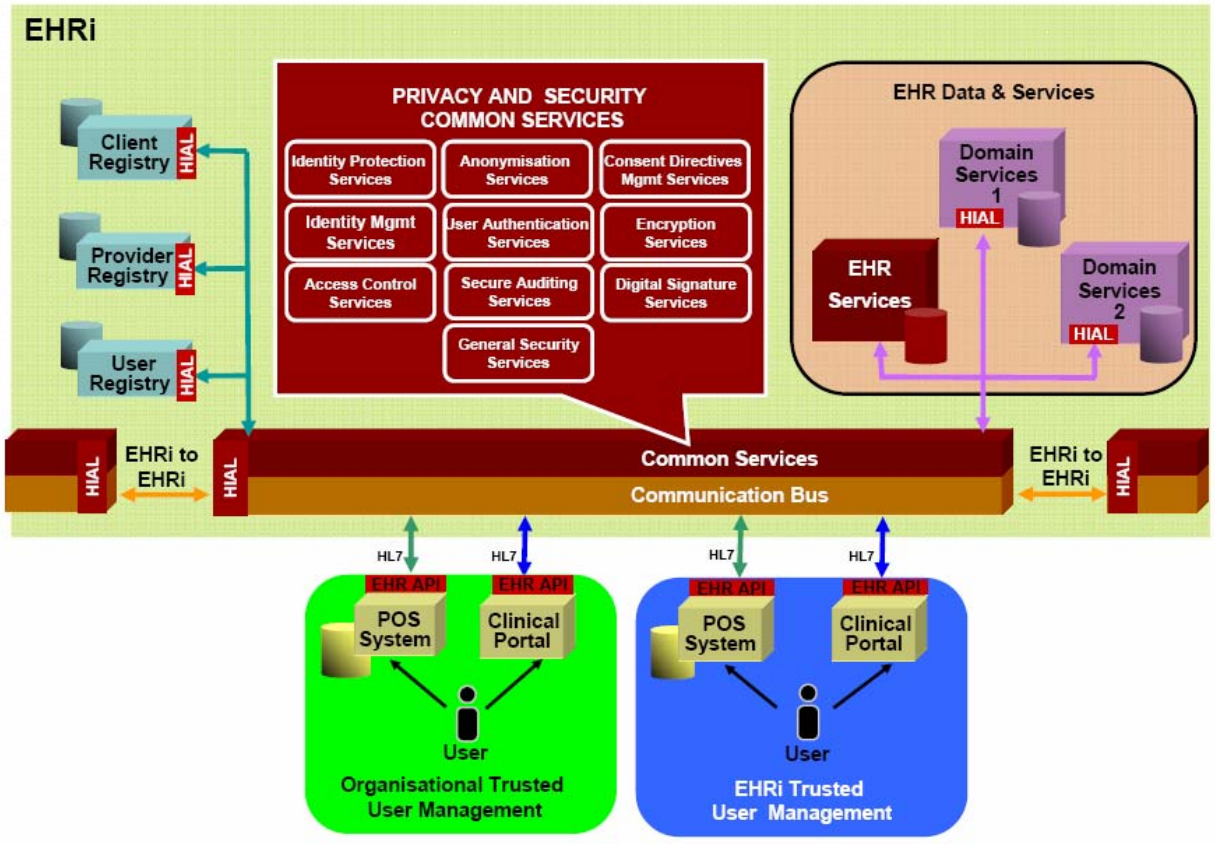

Figure 6: Access to the EHRi via Organisational Trusted User Management or EHRi Trusted User Management

The discussion above does *not* suggest that multiple trust levels will be supported by the EHRi. The combination of policies, procedures and technologies used to grant user access to PHI under organisation trusted user management must provide the same overall level of trust as the combination of policies, procedures and technologies used to grant user access to PHI under EHRi trusted user management. This leads to a fundamental assumption of the P&S Conceptual Architecture:

Assumption 20 Implementations of the EHRi exist within a uniform high trust model.

The same may not be true of organisations and POS systems connecting to the EHRi.

It is unlikely that every jurisdiction will support both models. EHRi trusted user management is especially useful where users can access the EHRi via a clinical portal. In the absence of such access, the advantages of this model may be considerably diminished.

For the interest of readers familiar with UML, a data model is presented on Appendix D for organisational trusted user management (see Figure 20) and for EHRi trusted user management (see Figure 21).

7.2.2 Who will be the users of the EHRi?

Many regulated healthcare providers[41] would benefit from access to the EHRi. Even in its early stages of deployment, the list that follows are just some of the following regulated healthcare providers could make use of access to the EHRi to improve the healthcare of Canadians:

- **physicians who are general practitioners**. Family physicians are an essential group of EHRi users. Without their active participation (both as information accessors and as providers of healthcare information to the EHRi via their clinical POS systems), the EHRi will reach only a fraction of its potential.
- **physicians and other emergency care providers who practice emergency medicine**. Much of the justification for an *interoperable* EHRi comes from its potential to provide timely access to PHI during a medical emergency for a patient/person far from home. These users require special privacy and security considerations related to the nature of emergency medicine. For example, the patient/person may be unconscious and therefore unable to give consent to information access. Emergency care providers include physicians and nurses who work in emergency departments of hospitals.
- **medical specialists**. While not all specialists would benefit from access to the EHRi (at least not in the short term), access to domain repositories such as prescription drug profiles and laboratory test results are compelling reasons for virtually all specialists to access the EHRi, at least on an occasional basis.
- **nurse practitioners, public health nurses and many other nursing professionals** who provide front-line healthcare to patients/persons in clinics, community care settings, schools and other relevant settings.
- **pharmacists and other dispensing healthcare providers** who manage the fulfillment of prescriptions, claims processing and other administrative functions associated with dispensing prescription drugs. Pharmacists, unlike other dispensing healthcare providers, are also responsible for ensuring patients/persons receive the maximum benefit from prescription drugs by providing knowledge based services that would be enhanced by having access to the patient's health profile, diagnosis and prescription drug profile[42].
- **radiologists accessing diagnostic images** via the EHRi. Significant investment has been made in diagnostic imagining capabilities for the EHRi such as x-rays, CT, MRI, and PET scans. These investments benefit all healthcare providers who need online access to DI data.
- **dental surgeons**, who would benefit from access to basic medical information on patients (allergies, drug sensitivities, etc.).

[41] Regulated healthcare providers are members of professional colleges who have official standing in the provincial jurisdiction in which they operate. Examples include the B.C. College of Physicians and the Ontario College of Nurses.

[42] For more information on pharmacists and the services they provide see the National Association of Pharmacy Regulatory Authorities' website at www.napra.org or the Canadian Pharmacists Association's website at www.pharmacists.ca

- paramedics to assist in the delivery of emergency medical care. Like emergency care providers, paramedics may have certain access privileges available in emergencies that surmount access restrictions in place for other healthcare providers. Unlike emergency care providers, paramedics cannot order tests, write prescriptions or perform some functions that may only be carried out by regulated healthcare professionals.
- **laboratory technicians**[43] who will manage the data entry of laboratory exam results into the EHRi.
- **public health officers** will access the EHRi for the purpose of public health surveillance.

Ultimately, there will be many EHRi users who are *not* regulated healthcare professionals. Examples of such users[44] include:

- patients/persons who are entitled to access their own PHI in the EHRi where such access is not prohibited by legislation.[45]
- medical receptionists in physician offices, who update demographic information, schedule appointments, direct patients with lab test requisitions to appropriate specimen collection centres where necessary, retrieve lab test results and distribute them to physicians in their clinics, and perform many other tasks that would greatly benefit from access to the EHRi;
- laboratory assistants, who manually enter some lab test results for patients;
- admissions clerks in hospitals, who obtain relevant medical information at the time of admission;
- ward clerks in hospitals, who obtain and collate relevant medical information for patients on their wards; and
- medical records clerks, who ensure that patient charts are up to date;
- medical transcriptionists who transform physician and that patient charts are up to date;
- medical researchers who will access the EHRi for the purpose of authorised health research; and
- EHRi system administrators will access the EHRi for the purpose of system maintenance and administration.[46]

7.2.3 Implications for Provider Registries and User Registries

To implement EHRi trusted user management, every user registered will need to be entered into a user registry. The professional role of each regulated healthcare provider must be obtainable from the provider registry. This basic role information consists of the regulated healthcare profession that the regulated healthcare professional belongs to and the specialisation involved where applicable (e.g. the medical specialty, if any, that a physician licensed to practice). This information will later be used as a

[43] Laboratory technicians are not regulated health care providers in all provinces.

[44] Whether a given health profession is a regulated health profession varies somewhat from on Canadian jurisdiction to another.

[45] 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.

[46] EHRi system administrators must not have access to PHI. System level testing, diagnosis and maintenance should be done, to the greatest extent possible, using test data, not actual PHI. An EHRi that effectively encrypts PHI during storage and when in transit will avoid these unintended disclosures to system administrators and other EHRi insiders (see section 7.9 on encryption). There are many other options as well, including the identity protection services described in section 7.7 below.

basis for role based access control (see section 7.5.3). There will also be a need to register EHRi users who are *not* regulated healthcare professional. These users will also need to be registered in the user registry. Their identities will need verification by others (see 7.3.4, Registration of Delegated EHRi Users) as will the determination of their role(s).

7.2.4 Privacy and Security Policy Management

Each of the P&S services requires some form of policy for its proper implementation. In most instances, a policy management service will be available to EHRi administrators to set the policy parameters needed for the appropriate operation of the EHRi within a jurisdiction. Policy management services will provide an interface for configuration and management of policies for access, auditing, logging, and consent. This will provide a means of coordinating these services in a manner that builds upon each jurisdiction's existing privacy policies and procedures; functioning, as a central location to access, modify and coordinate the underlying privacy and security related business rules for all P&S services. The interface will also operate with other policies that may be required for a streamlined and smoothly running EHR. Policy implementation is discussed in relation to each of the services.

7.2.5 Process Flow

Process flow in an **organisational trusted user management** environment has the following steps:

1. A qualified organisation – i.e. an organisation that meets (yet to be determined) minimum criteria for robust administration of their POS system users – is registered with the administrators of a jurisdiction's EHRi implementation prior to connecting to the EHRi. Details of this registration process would ultimately be jurisdiction-specific.
2. The organisation is assigned an Organisation ID.
3. Each of the organisation's POS systems that are to be connected is accredited against a (yet to be determined) set of minimum criteria for trusted connection to the EHRi.
4. Each accredited POS system is assigned a POS system instance ID (POSSID) by the EHRi's administrators.

NB: Later in this document, 7.3 will describe the details of user identity management more fully and section 7.5 will discuss access control; including assigning the user one or more POS roles and concomitant user access privileges.

The process flow for **EHRi trusted user management** is as follows:

NB: In EHRi trusted user management, registration of a prospective user does not require the prior registration of an organisation. A physician in a solo private practice could (at least in theory) register to access EHRi data and services directly via a web portal.

1. The verification of a potential EHRi user could take place in one of several ways:
    a. by remote registration with an administrators of the EHRi within a given jurisdiction using shared secrets or other means of proving the identity of the prospective user, or
    b. by having a local healthcare organisation act as a "local registration authority" to attest to the identity of a prospective user.

    Section 7.3.11 describes the above two options in detail.
2. Once the user's identity has been confirmed, the EHRi user registration is completed online and the user is assigned an EHRi user ID. Section 7.5 will discuss access control; including assigning the user one or more POS roles and the user access privileges that flow from those roles.

7.3 User Identity Management in the Desired Future State

7.3.1 Description

The user identity management service includes service components that address the need to accurately identify users of the system. Users include those who access PHI and those that need to administer the system. Identity Management services include the registration of the user and managing identity information. Identity management services include the generation of unique IDs for users, the looking up of unique IDs for users and the rapid suspension/revocation of all access for a given user.

Section 7.5 discusses the closely related activity of assigning roles to users. Role assignment typically takes place during user registration and in the case of users who are regulated health professionals, it is anticipated that their role information (general practitioner, dentist, etc.) will be obtainable from the provider registry. The desired future state of identity management is shown in Figure 7 below.

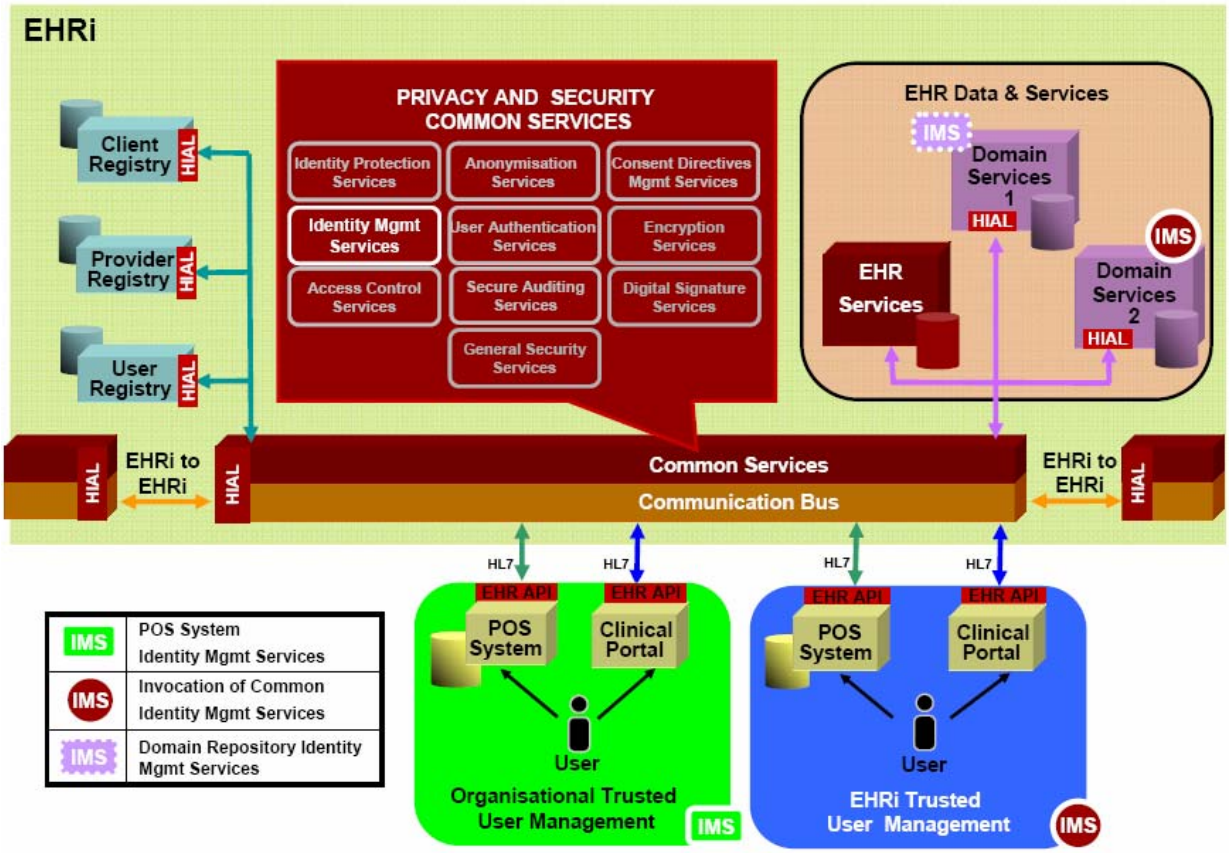

Figure 7: Identity Management in the Desired Future State

7.3.2 Rationale

Identity management services are fundamental functions in a system in which access to data and functions is based on user roles. They are also essential for support of auditing and consent directives management (at least insofar as it supports consent directive that withhold consent to disclose PHI to selected EHRi users).

The current practice of healthcare is rife with the use of group user IDs. Indeed, a group or generic user id may represent the entire staff on a hospital ward. Yet such group user IDs frustrate the expectation of patient/persons that they be able to find out who has accessed their records. Such a question can never

be meaningfully answered without recourse to unique user identification of all users. Indeed, healthcare is virtually the only industrial sector where group access to IT system containing confidential data is still common practice, Whichever of the two trusted user management approaches described above is followed, the conceptual architecture is constructed to require each user to have a unique user ID.

7.3.3 Approaches to Identity Management

As discussed above in section 7.2 (Trusting Connections to the EHRi) and as shown in Figure 7, there are two approaches to user identity management:

- **Identity management deployment model 1: use organisational trusted user management.** In an organisational trusted user management environment, identity management takes place entirely within the organisation. Messages to the EHRi from POS systems or clinical portals within such an environment will contain a (relatively) distinguished identifier for the user, together with a unique (EHRi supplied) organisational instance or Organisation ID to identify the organisation (and POS system within the organisation where there is more than one POS system or organisationally distinct instance of a POS system).

  This approach has two advantages:

  1. it provides users with trusted “single sign-on” functionality when accessing the EHRi via their organisational POS system, and
  2. it is relatively cheap to administer as it builds on existing organisational user registration and user administration which is a mainstay of just about every hospital and large clinic in Canada.

  It also has some disadvantages:

  1. it leaves users who access the EHRi through an organisational POS system as well as through a clinical portal (from their homes for example) with the likelihood of having to manage multiple user IDs, and
  2. it has implications for the management of certain types of consent directives (i.e., those directed against specific providers or user; see discussion in section 7.6.10).

- **Identity management deployment model 2: use EHRi trusted user management.** By contrast to deployment model 1, EHRi trusted user management takes place almost entirely within the EHRi. An EHRi user ID is obtained directly by the EHRi from the user, who will need to sign on to the EHRi, even if the user is already signed on to a POS system.

  This deployment model has one principle advantage: it ensures that identity and role information on regulated providers is centrally administered and completely trusted. For the registration of regulated healthcare providers, the provider registry will be an authoritative source of information to draw upon during user registration (since user identity and provider role in the provider registry will typically come from authoritative sources such as the jurisdiction's regulatory colleges, and who better knows the identities and roles of, say, physicians in BC than their regulatory body, the BC College of Physicians and Surgeons?). For the registration of users who are not regulated healthcare providers, each registration must take place under the direction of a qualified regulated healthcare provider or entity having the responsibility for local registration functions who can attest to the prospective user's identity and role (see the following section "Registration of Delegated EHRi Users").

  This model also has one significant disadvantage: cost. The potential healthcare users across Canada who could ultimately benefit from access to a fully deployed EHRi number in the hundreds of thousands. The direct registration would be an expensive undertaking.

Neither model has definitive advantages over the other. It is anticipated therefore that the EHRi will support both deployment models in virtually all jurisdictional deployments.

7.3.4 Registration of Delegated EHRi Users

In some situations it may be appropriate for an authorised EHRi user to be able to designate a subordinate staff member to whom the user will subsequently delegate a subset of their access privileges (e.g. medical receptionist or transcriptionist). EHRi users with authority to carry out such delegation must be able to equip their staff with their own, auditable unique identity; i.e., they must be able to register these staff. Staff with delegated authority to access the EHRi will subsequently be provided with role based access to those components of the EHRi to which they require access *under the authorisation of the delegating EHRi user*. The delegating user will be accountable for the actions of those users to whom they delegate access.[47] Some private laboratories have deployed this approach to authorisation in order to provide access to laboratory test results.

7.3.5 Patients/Persons as Users of the EHRi

As noted in section 7.2.2 above, the P&S conceptual architecture allows for direct access by patients/persons to relevant portions of their own EHR. In certain cases, treatment and care of chronic diseases (e.g., diabetes) may benefit from allowing unmediated access by a patient/person to portions of his/her record (through a portal, say). In many other situations, it may be more appropriate to provide indirect access mediated by a healthcare provider who can explain to the patient/person what the content of the record actually means in non-technical terms. In any event, specific policy decisions about how and what portions of records are amendable to direct and unmediated access by patients/persons are outside the scope of this architecture document. Where unmediated access is warranted, the architecture supports such direct access by patients/persons using the same services that support access by healthcare providers. In such cases, the patient/person becomes an EHRi user and must be registered as such, either through the organisational trusted user management model (in those cases where the patient/person is a registered user of some POS system that has a trusted connection to the EHRi) or through the EHRi trusted user management model (in those cases where the patient/person has the means to register directly as an EHRi user through a clinical portal).

7.3.6 Implications for Domain Repositories

To further complicate identity management, domain repositories connected to the EHRi may also have their own identity management systems. It will be the responsibility of the EHRi to navigate such a domain repository IMS on behalf of the EHRi user whenever possible and the EHRi architecture must support this.

7.3.7 Identifiers for Users, Organisations, and POS Systems

At least four different types of identifiers are discussed in this section:

1. **EHRi user IDs** that a user of the EHRi uses to log directly into the EHRi (via a portal), without first logging into an organisational POS system. Each EHRi user ID is administered by the EHRi's implementing jurisdiction.
2. **organisation IDs**. These are assigned by administrators of an EHRi implementation within a given jurisdiction to uniquely identify each organisation connecting to the EHRi.
3. **POS system user IDs** that a user of a POS system within a given healthcare organisation uses to log into that POS system. Each POS system user ID is administered by the organisation in question (its human resources department, IT department, etc.).
4. **POS system instance IDs (POSSIDs)**. These would be assigned either by the jurisdictional administrators of an EHRi.

[47] The chain of accountability required to facilitate this process will need, at a minimum, to be supported via contractual means (e.g. confidentiality agreements, data sharing agreements, etc.).

7.3.8 Protection of Personal Information Obtained During User Registration

While the emphasis in this document is on protecting the privacy of patients/persons, the privacy of healthcare providers is no less important. As noted in 0, confidential information obtained during the registration process includes personal information and must be protected as such.

7.3.9 Availability Requirements

The existence of user registries creates significant availability requirements for these repositories. Because of their pivotal use in access control, they must be continuously available (i.e., with no scheduled downtime and robust resistance to equipment outage or denial of service attack). The availability requirements of user registries will be at least as high as the availability requirements of EHR data.

7.3.10 Policy Enforcement

Policy enforcement of user identity management in an organisational trusted user management environment is not a trivial task. There are no widely accepted best practices currently in place for the registration of users by healthcare organisation. Defining minimum requirements for such registration would require careful consideration. There will also be a requirement to map user roles as defined in POS systems implemented by the organisation to user roles that are meaningfully be used in EHRi access control (see section 7.5 below).

By contrast, policy enforcement for EHRi trusted user management is considerably simpler as all aspects of this policy will be under the control of those who govern the operation of the EHRi. Important aspects of identity management such as acceptable use agreements can be tightly controlled (i.e. successfully registration of a user requires users to comply with the terms of use set by those operating the EHRi).

7.3.11 Process Flow

The process flow for user management within the **organisational trusted user management** model as follows:

1. After a qualified organisation has been registered and has been assigned an Organisation ID (see section 7.2.1 above), and each of the organisation's POS systems that are to be connected has been accredited against a (yet to be determined) set of minimum criteria for trusted connection to the EHRi and assigned a POS system instance ID (POSSID) by the EHRi's administrators, the organisation's previously registered users may, where qualified, be able to immediately access the EHRi..
2. The organisation registers a new user within one of its POS systems and assigns the user a POS user ID[48]. The organisation must perform an identity check to verify the identity of the prospective user, must confirm the user's professional role within the organisation, and record sufficient information to later determine exactly who an authenticated user with a given user ID actually is.
   NB: Later in this document, section 7.5 will discuss access control; including assigning the user one or more POS roles and concomitant user access privileges. While conceptually separate from identity management, access privileges are often assigned to users at the same time as

[48] A user might be assigned multiple POS system user IDs in the case of an organisation that has multiple POS systems and does not have a federated ID scheme or single sign-on capability. Such multiple IDs should be avoided for two reasons:

a) they hinder adoption,
b) they potentially weaken security by making it more difficult to audit the activity of a user whose activities may appear in audit logs under multiple IDs, and
c) they drive users to distraction.

their initial user registration for reasons of efficiency and expediency. While this conceptual architecture treats these processes separately (and from a security perspective they are separate), the user may see them as one continuous process.

The process flow for user management within the **EHRi trusted user management** model is as follows:

NB: Registration of a prospective user does not require the prior registration of an organisation. A physician in a solo private practice could (at least in theory) register to access EHRi data and services directly via a web portal.

1. The registration of a potential EHRi user could take place in one of several ways:
    a. A prospective user might be able to remotely register with the administrators of the EHRi within a given jurisdiction (perhaps via a web portal) provided that a pre-populated repository of information is available that can be used to positively verify the identities of such prospective users and authenticate them for the purposes of establishing secure communications. For potential users who are regulated healthcare providers, this would require a provider registry or other personal information repository with sufficient information (practice address, for example) so that an EHRi user ID and activation data can be securely delivered to the user out-of-band (a smart card delivered by registered mail and a password delivered by phone, for example).[49]
    b. Registration could also take place by having a local healthcare organisation act as a "local registration authority" to attest to the identity of a prospective user (the latter is sometimes referred to as passing an "active in the community" test – the identity of the prospective user is beyond question because he/she is well known to administrators of, say, a local hospital). A secure communication from the local authority to the administrators of the EHRi (via a secure web portal, for example) would enable initial registration to be securely commenced. The prospective user might subsequently receive a (possibly temporary) user ID and activation data (a PIN number mailed to the user, for example, that would permit an initial sign-on in order to complete the registration process).
2. The EHRi user registration is completed and the user is assigned an EHRi user ID. Section 7.5 will discuss access control; including assigning the user one or more POS roles and concomitant user access privileges. While conceptually separate from identity management, access privileges are often assigned to users at the same time as their initial user registration.

EHRi trusted user management requires authoritative sources of information. Provider registries are among these important sources (presuming they are populated with information from authoritative sources such as relevant regulatory colleges or from government sources of equal rigour).

7.3.12 Requisites

Provider and user registries are prerequisites for identity management for both organisational trusted user management and EHRi trusted user management.

7.3.13 Service Components

The following service components of the User Identity Management Service are fully described in Appendix A:

- A.1.1 Register EHRi user
- A.1.2 Manage User Identity

[49] The reader is cautioned not to read too much significance into examples such as the one above. Only a Threat and Risk Assessment of a fully elaborated procedure and detailed technical specifications can determine whether a given method is sufficiently secure.

7.4 Authentication in the Desired Future State

7.4.1 Overview

Authentication establishes the validity of the claimed identity of a user and provides protection against access by unauthorised users. User authentication services provide service components that are needed to validate the user accessing the EHR. The approach to authentication depends upon which of the two trusted user management environments the user is in. In an organisational trusted user management environment, all user authentications takes place within the accessing user's POS system or clinical portal system (the EHRi user authentication service is not involved in the process). In an EHRi trusted user management environment, user authentication takes place via direct interaction with the EHRi. The desired future state of the user authentication service is shown in Figure 8 below.

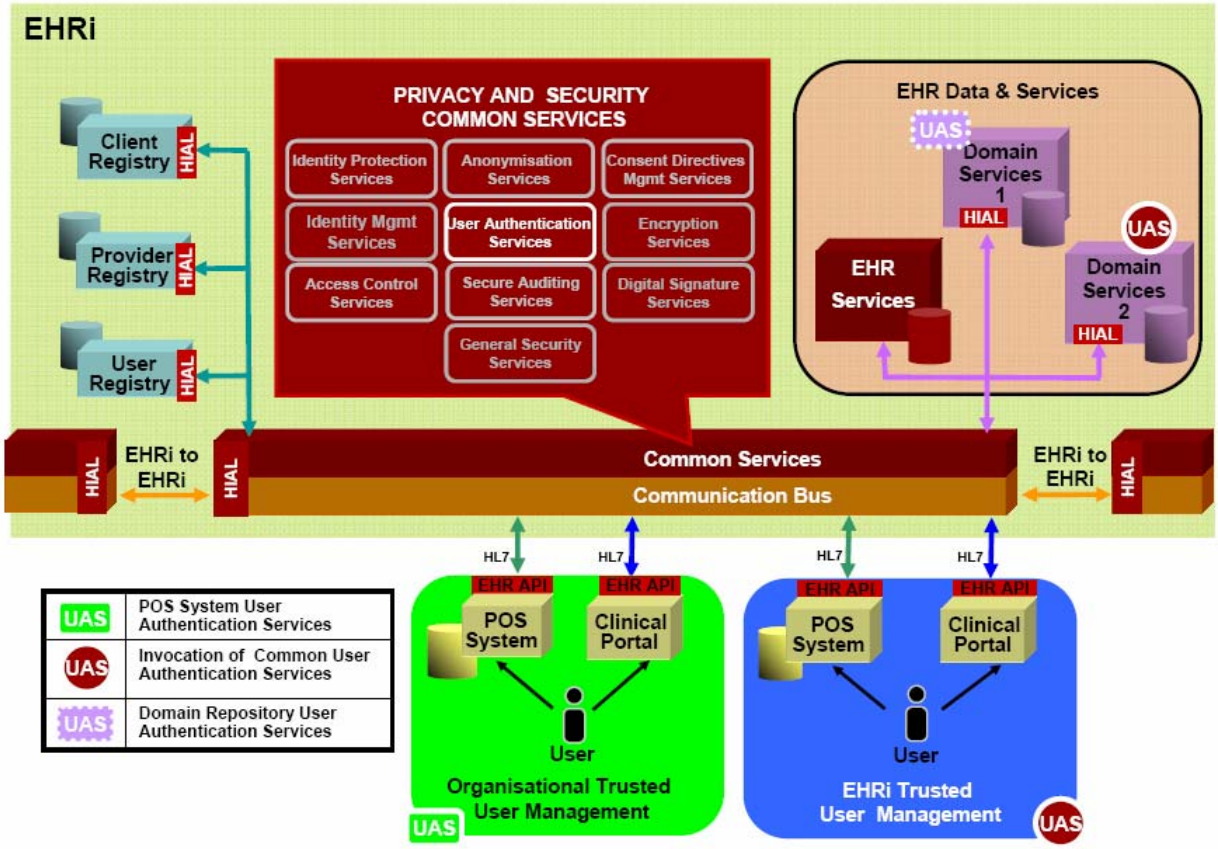

Figure 8: Authentication in the Desired Future State

7.4.2 Rationale

Every EHRi must establish the validity of a claimed user identity and provide protection against identity fraud (a false claim to be an authorised EHRi user) or identity theft (using information stored in the EHRi to steal the identity of an individual) during access to a patient/person EHR. The user authentication might include multiple authentication factors, such as passwords, digital signature mechanisms, biometrics, or other technical means of confirming the user's claimed identity. These users make a claim of identity by one of several common means, such as logging into the system with a user ID, presenting the system with a token such as a smart card, or permitting the system to take a biometric scan. The user authentication service provides the function that validates user identity.

The examples in the preceding paragraph are by way of illustration only. This conceptual architecture does not advocate any given authentication technology.

There are two technical requirements relating to authentication that the P&S conceptual architecture must honour:

- Security Requirement 70 (Restricting Connection Times to EHRi Applications), and
- Security Requirement 71 (Robustly Authenticating Users).

7.4.3 Approaches to User Authentication

Architecturally significant questions surround the topic of authentication. From a process perspective, the user authentication process for a POS system will take place once when the user logs into the POS application. Currently this process will is sometimes automated where organisations use single sign-on solutions or context transfer solutions such as the Clinical Context Management Specification [CCOW]. For POS systems that operate in an organisation trusted user management environment, when should the EHRi become aware of the POS system user? For POS or clinical portal systems that operate in an EHRi trusted user management environment, should EHRi attend to authentication once at the beginning of a user session and then maintain authentication information as part of a whole transaction session or should this be done every time that a transaction is processed?

There are many different ways to obtain an adequate level of assurance. Can a user log on with a user name, digital certificate and password? Would a smart card or other physical authentication token (a USB fob, say) used in combination with a password be acceptable. Might the user enter a user name and a one-time password generated by a physical token (typically a card that displays a 6 digit number that changes every 30 seconds)? Are these methods equally secure? The latter question can only be answered by a threat and risk analysis of the alternatives. Answers to the former questions rely in part on how easily busy users can make use of the methods and how cost effective they are to deploy. Ultimately, the question of which combinations of authentication technologies provide an adequate level of authentication is an EHRi governance issue (see section 10).

7.4.4 Availability Requirements

Depending upon the authentication technology chosen, authentication for EHRi Trusted User Management may depend in part upon data stored by user repositories[50]. To the extent that this is the case, significant availability requirements will be placed on these user repositories and the associated authentication service. Without them, users registered under the EHRi Trusted User Management model will not be able to log into the EHRi. This will in turn require that these repositories and the authentication service be continuously available (i.e., with no scheduled downtime and robust resistance to equipment outage or denial of service attack).

There is no such availability requirement for users registered under the Organisational Trusted User Management model. In this model, the POS system connected to the EHRi authenticates users locally. The EHRi does not need to depend in this case upon user registries to carry out authentication.

7.4.5 Policy Enforcement

Whatever decisions are made regarding what constitutes an adequate level of authentication and which combinations of authentication technologies meet that level, POS system vendors will need published specifications for the authentication of EHRi users by POS systems. Users of POS systems which do not meet these specifications will need to authenticate themselves directly to the EHRi when accessing EHRi data or services. See section 7.2 above for a full discussion of options for identity management and their impact on authentication.

[50] In general, user authentication depends upon "something you have" (e.g.: a physical token such as a smart card), "something you know" (e.g.: a password or PIN), or "something you are" (as measured by a biometric). Authentication technologies of the "something you know" variety require access to a repository of data unique to each user that can be used to determine if the information supplied by the user is correct (e.g.: a list of values derived from hashed user passwords).

In the organisational trusted user management context, policy enforcement points would be situated in the POS system or its middleware.

7.4.6 Process Flow

The process flow for authentication under **organisational trusted user management** is as follows:

1. The user logs into the organisation's POS system and is authenticated by the POS system.
2. The user attempts to access EHRi data or an EHRi service.
3. The POS system determines whether the user is authorised to access the EHRi.
4. The EHRi authenticates the POS system if it has not already done so. The EHRi generates a trusted authentication token for the POS system that the EHRi can use to rapidly re-authenticate the POS system during future access[51].
5. The user's POS user ID and the POS instance ID (POSSID) and Organisation ID are all sent to the EHRi by the POS system as part of the HL7 message and both are used by the EHRi for audit and logging purposes.
6. For a request for data from a domain repository, the domain repository authenticates the EHRi if it has not already done so. An authentication token may be generated by the domain repository for future access. The EHRi provides the POS instance or Organisation ID and POS user ID to the domain repository for logging and auditing purposes.

Process flow in an **EHRi trusted user management environment** presumes that the user has registered as an EHRi user through a web registration process.

The process is then as follows:

1. The user logs into the EHRi in one of three ways: via a clinical portal, via a pass-through from a POS system (requires that the POS system will need to allow for access to the EHRi user authentication service) or via the POS system where it has recorded the EHRi user ID and provides it on your behalf.
2. The user is asked for an EHRi user login ID.
3. The EHRi authenticates the user. An authentication token is validated for future access.
4. The user's EHRi user ID is used by the EHRi for audit and logging purposes.
5. For a request for data from a domain repository, the domain repository authenticates the EHRi if it has not already done so. An authentication token is generated by the domain repository for future access. The EHRi provides the EHRi user ID to the domain repository for logging and auditing purposes.

7.4.7 Requisites

In a trusted organisation user management environment, the following are needed:

- a provider registry, user registry, and unique identification of POS systems and organisations

Organisational trusted user management environment requires that the following first be in place:

1. the organisation's POS system has met certain technical criteria, as specified by the jurisdiction, for trusted authentication;

[51] "Future" is a relative term, but typically, authentication tokens have a lifetime measured in minutes or hours. The specific length of time allowable is best determined through a Threat and Risk Assessment, taking into account the specific details of the authentication protocols used.

2. the installation of the organisation's POS system is registered with the EHRi and the POS system has a unique POS instance ID;
3. the organisation has met certain administrative criteria, as specified by the jurisdiction, for trusted user management; and
4. the user has registered with the organisation and has a unique POS system user ID (i.e., unique within that organisation and POS system).

7.4.8 Service Components

The following authentication service components are described in detail in Appendix A:

- A.2.1 Authenticate user
- A.2.2 Generate Authentication Token

7.5 Access Control in the Desired Future State

Not all bona-fide users of the EHRi can access all available EHRi services and few (if any) users outside of emergency medicine would be entitled to access an arbitrarily selected patient/person's EHR. Access control aims to manage and apply the permission rule sets that restrict access to PHI and other information assets/functions to authorised users only. Best practice is to assign access privileges at the most fine-grained level that is practically possible to ensure that access is granted to the minimum PHI required for a user to perform a specific job function related to a specific role. Limitations can come by way of limiting access to the system as a whole, limiting access to specific functions, limiting access to data at different levels such as an entire database, specific data subjects or entities, specific data records, specific data fields within records, and specific data operations in the form of read, add, update, etc. The set of conditions applied to determine these access privileges can also be determined at different levels, from very broad: “user does not have access to any EHR” to very specific: “user has access to patient/person events data only if user is working in facility X under role Y, and if data does not pertain to data set Z”.

The essence of access control is in determining what access privileges a given user can exercise in a given context. Can Alice look up a specific patient/person's EHR? Can she view the entire record or just of portion of the record? Can she update the record? Can she enter or update consent directives on behalf of this patient/person? Can she search for records matching some search criteria she specifies? Can she place orders (e.g.: for a lab test) through the EHRi? Some of these questions have not yet been answered for any user, much less for Alice, as they require further elaboration of the underlying (non-privacy, non-security related) EHRi architecture and its capabilities. For example, will users accessing the EHRi via a web portal have access to e-prescription capability? If not, there is little point in determining who has the access privileges to write a prescription. Whatever final functions the EHRi supports, an access control system must determine, for every EHRi user, whether the user has the privilege of exercising that function.

As a practical matter, large numbers of users cannot be assigned a custom designed set of privileges that is unique for each user. It is inefficient, expensive and worst of all, highly insecure – such exquisitely fine-tuned access controls have been shown to inevitably lead to mistakes in administration and to users gaining access to privileges they should never have obtained. Role based access control is typically used to reduce the number of access privilege decisions by assigning users to one or more roles from a (hopefully short) list. Another approach to access control involves grouping users together into work groups that then share access to the same resources or sets of records (e.g.: all physicians in a practice can access the records of all the patients treated within that practice).

Access control decisions are driven by access control policy. Such policy is among the most important of the many policies listed in section 10.3 that are required for the effective functioning of this architecture.

Several access control methodologies must therefore be provided as part of a unified access control service. This service ensures the confidentiality and integrity of PHI. The 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[52].

b) **work group based access control**, which relies upon the assignment of users to work groups (such as clinical teams) to determine which records they can access. Group-based access control allows users to be assigned to working groups such as a primary care clinic, the emergency department of a hospital, or a community-based health and social care team. Users can then rapidly be given access to all the records of patients in the care of that team.

c) **discretionary access control**, which relies upon users with a legitimate relationship to a patient/person's EHR (a family physician, say) to grant access to other users who have no previously established relationship to that patient/person's EHR (a specialist, say)[53].

7.5.1 Description

As Figure 9 below shows, in an organisational trusted user management environment, the privilege management aspects of access control takes place entirely within the organisation. Messages to the EHRi from POS systems or clinical portals within such an environment will contain a role for the user.

By contrast, EHRi trusted user management takes place entirely within the EHRi. An EHRi user ID is obtained directly by the EHRi from the user (who will need to sign on to the EHRi, even if the user is already signed on to a POS system).

Domain repositories connected to the EHRi may also have their own access control systems. It will be the responsibility of the EHRi to navigate such a domain repository system on behalf of the EHRi user whenever possible. The EHRi common services will access domain repositories on behalf of the user based on user role and user privileges.

[52] 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”.

[53] 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). As described in the text, it is presumed that when user A confers discretionary access to a specific patient/person's EHR onto user B, user B has already been registered as a bona fide user of the EHRi. User A is responsible only for granting access, not for attesting or in any other way verifying the identity of user B prior to B becoming registered as a user.

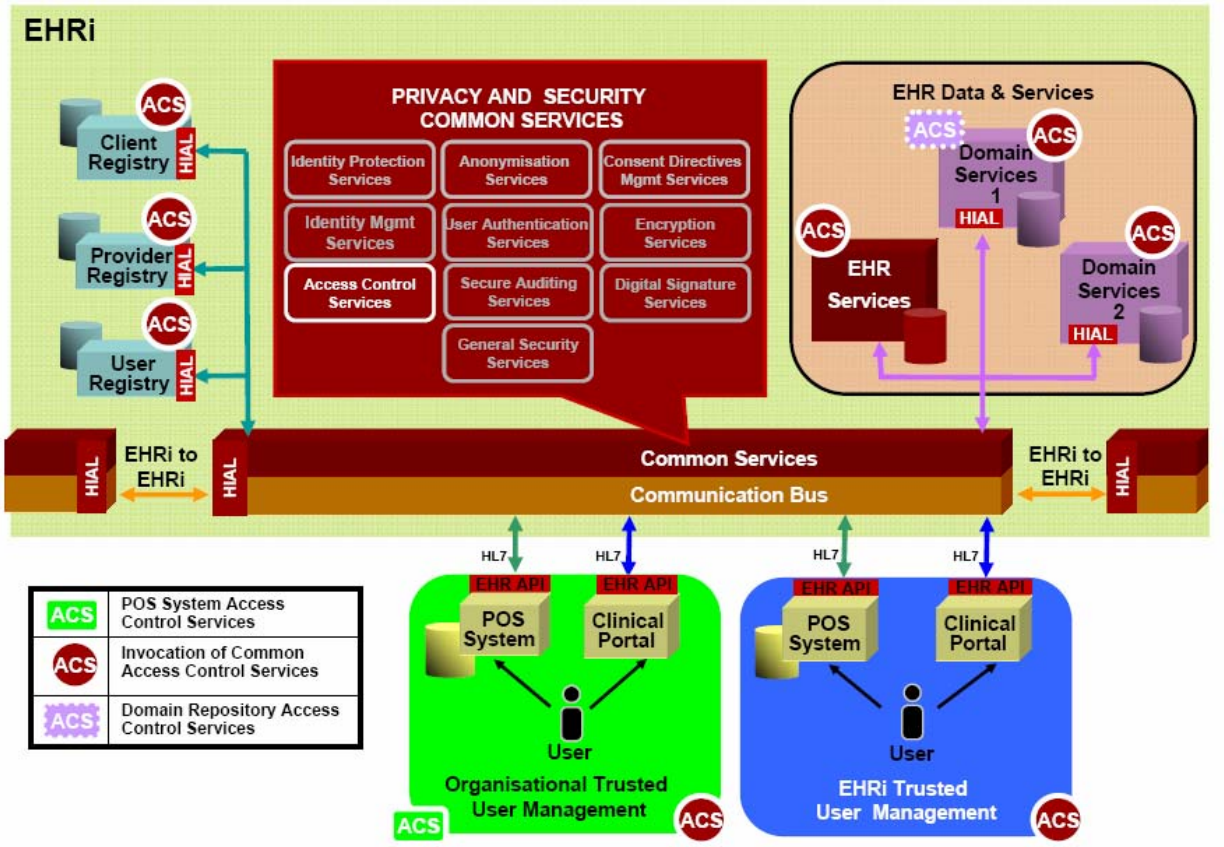

Figure 9: Access Control in the Desired Future State

7.5.2 Rationale

Role-based access control is already well established in health informatics and often forms the basis of access control to hospital information systems. The administrative burden of determining access privileges on a user-by-user basis is too onerous for institutions that have hundreds, perhaps thousands, of users. By assigning users to roles, each user immediately inherits the access privileges commensurate with the user's role. In this way, the administrative burden of managing access privileges for large numbers of users is reduced by orders of magnitude.

Group-based access control facilitates the rapid deployment of users who may move frequently from one team to another (for example, based on assignment to hospital care teams). While such groups are usually administered locally (within a hospital, say), the ability of the EHRi to support group-based access control can greatly enhance the security and utility of administering access control in situations where the access privileges of users are largely dependent on the team to which they are currently assigned.

Discretionary access control is needed in healthcare in those situations where a user who has full access to a record (a responsible physician, say) needs to rapidly grant access to a user who has never had a previous legitimate relationship with the patient (a specialist, say). The patient may not be present or even conscious when this access control decision is made. Discretionary access control occupies a middle ground between the two extremes of, on the one hand, allowing all users in a given role access to a huge pool of electronic health records; and on the other hand, requiring explicit consent for each user to access each record.

7.5.3 Approaches to Role Based Access Control

At the operational level, permissions associated with users and/or roles are used to allow/deny use of functions in an application or to allow/deny access to data. These systems are typically tightly coupled with the application especially for data access. Third party products now provide management for role based access control for application functions, but administering permissions for data access is still a major challenge. Access control approaches that work well within an organisation may not fit well when mapped to the data and services provided by the EHRi as they may lead to not having access to the right function or data at the right time to provide proper care.

Before discussing role based access control further, it is important to first differentiate between professional roles, EHRi Roles, and POS system roles:

- Professional roles evolved over time to meet the needs of treatment and care; they were not designed with information access in mind. Nevertheless, each regulated healthcare professional is governed (e.g.: in legislation or regulation) by the professional practices as set out in the governing law or regulation that define the nature of the practice. This can be used as a basis of determining the types of information and services needed in the conduct of that profession.
- EHRi roles determine which data elements and functions can be accessed within the EHRi. They do *not* apply to system functions and data within a POS system. The complexity of EHRi roles depends largely on the complexity of EHRI services, data grouping and access privileges. By way of example, an EHRi that allowed users to view, but not update, EHR data grouped into a few basic categories (health profile, prescription drug profile, lab results, and diagnostic images, say) would not require a large number of roles to be defined. The question of whether professional roles can be mapped effectively to EHRi roles depends in part on the complexity of EHRi roles and therefore depends ultimately on the complexity of EHRi services, data grouping and access privileges.
- POS system roles are determined by the implementing organisation and in some cases by a pre-set role functionality built into the POS system. These roles are often geared to the (sometimes idiosyncratic) features of the POS system and may not map in a straightforward manner to EHRi roles.

Organisational trusted user management requires some level of mapping between POS system roles and EHRi roles. Professional roles and (yet to be determined) EHRi access control policies may act as additional sources of information in completing this mapping.

There are three approaches to management of EHRi user roles within a jurisdiction:

1. **Role deployment model 1: POS system uses EHRi roles when communicating with the EHRi.** Standardise a set of EHRi roles for use across an entire jurisdiction in which the EHRi has been implemented. Each organisation connecting to the EHRi would have to ensure that the organisation's POS system(s) used these standardised EHRi roles within HL7 messages directed to the EHRi. Each organisation would be responsible for mapping their local POS system roles to the EHRi roles and the organisation's POS system(s) or middleware would be responsible for inserting the standardised EHRi role into each HL7 message directed to the EHRi.
2. **Role deployment model 2: POS system roles are mapped to EHRi roles.** Standardise a set of EHRi roles as in 1 above and then map POS system roles defined within an organisation to standardised EHRi roles for every organisation connecting to the EHRi within a jurisdiction. There are two ways of technically accomplishing this:

    a) by having each organisation adopt a jurisdictional POS system role schema and then i) have the organisation's POS system or middleware include the jurisdictional POS system role within HL7 messages and ii) have the EHRi map the jurisdictional POS system role to the standardised EHRi role; or

    b) by taking each organisation's roles, mapping them (in consultation with the organisation) to the standardised EHRi roles, and then performing this mapping each time the organisation's POS system includes a local POS system role within an HL7 message. Option b may be easier for

an organisation to implement technically because it transfers the mechanics of role mapping to the EHRi. This transfer comes at a cost in terms of implementing and maintaining these role mappings within the EHRi and a cost in terms of transactional overhead on each transaction. Either way, the exercise of mapping roles will be organisationally painful.

3. **Role deployment model 3: POS system roles are partially mapped to EHRi roles.** Record role information as received from diverse POS systems and use it to make access control decisions if it can be interpreted, but don't attempt to interpret it or to further process the access request if it cannot. This approach relies heavily on the Pareto principle: 80% or more of the requests will come from users with 20% or fewer of the roles. Even if roles were only mapped for physicians (i.e., general practitioners and specialists), this would allow a significant number of access requests to be processed. Amongst other problems, the EHRi might provide a wealth of services that are not available through the user's local POS system. The local organisational lists of roles and access privileges may not even be constructed to differentiate among EHRi services that clearly demand restrictions on their use. For example, if a local POS system does not support e-prescribing, the roles used in the local system may not draw a distinction between healthcare providers who can issue a prescription (physicians, selected dentists, and nurse practitioners, say) and those who cannot.

These three approaches are summarised in Table 2.

Table 2: Approaches to Role Based Access Control

Approach	What role schema is used in HL7 messages?	Who maps the roles?
Role Deployment 1: POS system uses EHRi roles when communicating with the EHRi	EHRi roles standardised across the jurisdiction	Organisation's POS System
Role Deployment model 2a: POS system roles are mapped to EHRi roles – standardised POS role schema	POS system roles standardised across the jurisdiction	EHRi
Role Deployment model 2b: POS system roles are mapped to EHRi roles – POS role schemas vary by organisation	Organisation specific standardised roles	EHRi
Role deployment model 3: POS system roles are partially mapped to EHRi roles	A few heavily used roles	EHRi

Whichever of the three options above are pursued, there will still be the additional issue of how POS system roles in one jurisdiction map to those in another to allow cross-jurisdictional access to PHI. Where necessary, standardised EHRi roles in one jurisdiction must be mapped to those in another to allow cross-jurisdictional access to PHI.

7.5.3.1 A Role for Patients/Persons as Users of the EHRi

As noted in section 7.2.2 and 7.3.5, the P&S conceptual architecture allows for direct access by patients/persons to relevant portions of their own EHR. In such cases, the accessing patient/person as a user of the EHRi would be assigned the role of "patient" and would be able to access their own record. The architecture also allows a substitute decision maker to access a patient/person's record where permitted by the implementing jurisdiction. In such a case, the accessing user would have the role of "substitute decision maker" and would be able to access only the records of selected patients/persons for whom they had substitute decision-making responsibility.

7.5.4 Approaches to Work Group Based Access Control

For the EHRI, work group based access control allows a set of users to be associated with a set of patients/persons. Users can be assigned to working groups such as a primary care clinic, the emergency department of a hospital, or a community-based health and social care team. Users can then rapidly be given access to records of all the patients in the care of that team.

Workgroups can be formulated in several ways, not all of which work well for access control of the EHRi:

- **geographic work groups** – where all the qualified healthcare providers in a given geographic area can access the EHRs of patients/persons living within that geographic area. Geographic work groups are fairly static in their composition; with individual healthcare providers sometimes remaining in a given geographic area for many years.

  Automatically associating patients/persons to geographic work groups requires that the client registry contain address information, at least at some level of granularity.

  Geographic work groups may be relatively straightforward to implement, but they are more effective at controlling access in small towns and rural areas than in large cities. Restricting the access of an EHRi user to just those patient/persons living in, say, Toronto would still allow access to the health records of one-quarter of the Ontario's population of eleven million.

- **organisational work groups** – where some subset of the qualified healthcare providers working within an institution can access the EHRs of patients/persons whose EHRs are stored with the POS systems of the organisation. Such work groups allow users of large hospital systems to be segregated into departments, campuses, etc. Organisational work groups tend to be of two types:

  a) **structural work groups** that are tied to a healthcare organisation's structure (e.g.: the staff of an outpatient clinic). Users remain assigned to a structural work group for extended periods of time, sometimes many years.

  b) **functional work groups** that consist of a group of health care providers and support staff who are brought together to carry out a specific function; e.g. any heath care provider in a clinical care team can access the EHRs of all patient/person assigned to that team. The assignment of users to functional work groups may be fairly dynamic; changing perhaps over days and weeks, rather than months and years (as is more typical of organisational or geographic work groups).

  Organisational work groups that are structural in nature and stable for long periods of time may be suitable candidates for work group based access control, provided a means can be found to associate patients/persons with each workgroup. For example, primary care practices are typically very stable over long periods of time in terms of the physicians who are working within the practice. Few patients would be surprised to find themselves being treated by another physician in their primary care practice if their regular primary care provider were sick, or otherwise unavailable. Likewise few would be surprised or dismayed if the other practice physician in the practice accessed their health record under such circumstances. Despite their long-term stability, organisational work groups are organisationally still painful to administer, as there must be a mechanism to securely inform the EHRi that Dr. Leger is in the same organisational work group as Dr. Schwartz, even if the assignment won't need updating for many years. Such mechanisms could be difficult to implement in a straightforward and cost effective way.

  To be effective for access control, there must be some means of associating patients/persons with each work group. While it may work well for organisations and clinics, structural work group based access control has some disadvantages when applied to the EHRi because this assignment of patients/persons to work groups is difficult to administer. In healthcare institutions such as hospitals, this is a function of patient admitting and works well for hospital POS systems but there are no automated means by which the EHRi could independently infer which persons are currently admitted as patients to a given hospital, A POS system could report this

information to the EHRi, but subsequently using this information to restrict the access of users of those same POS system may be, from a security point of view, of questionable utility. For clinics too, the association of patients/persons to primary care groups is a registration function fulfilled within the clinic. As rostering of patients/persons to primary care providers is relatively uncommon in Canadian jurisdictions, there is no current source of information available to automate the assignment of patients/persons to primary care work groups.

Automatically associating patients/persons to organisational work groups requires that information in the EHR repository be attributable to health care providers. Certain types of data in the EHR such as the patient/person's health profile especially lend themselves to inferring a relationship between registry contain address information, at least at some level of granularity. Were a jurisdiction to allow a primary care provider (or group of primary care providers in a practice) to take on the role of maintaining the health profile component of the EHR for a given patient, then authorship of the information in a patient's/person's health profile would provide the basis for the EHRi to automatically infer a relationship between the patient and the provider(s) in the practice. See For example, If Dr. Leger is Bob Smith's primary care provider (as inferred from the fact that Dr. Leger is the source of much of the information in Bob's health profile, and if Dr. Leger and Dr. Schwartz are both members of the same primary care practice, it may be reasonable for Dr. Schwartz to be able to access Bob's record. Nevertheless, there are many access control policy issues that must be resolved before such access rules could be automated. "Circle of Care Work Groups" in the discussion below.

Whether they are structural or functional, organisational work groups can suffer from the disadvantages indicated above when applied to the EHRi:

1. it can be difficult to maintain group membership and keep it up to date. This is especially true of functional work groups that can change membership frequently. Only work groups based on very stable structural relationships would be readily amenable to providing basis for access control for the EHRi.
2. it can be difficult to infer the relationships of patients/persons to the work group without their being explicitly assigned. There is one notable exception as mentioned above: when the work group consists of a given person's past care providers, it may be possible to infer the composition of this group and its relationship to the patient based on the origin of data in the patient's EHR. This special case could be referred to as a "circle of care" work group (see below).

- **Circle-of-care work groups** – any member of a patient's circle of care can use the EHRi to access the EHR of that patient/person. This is the special case of organisational work groups discussed above where a relationship between a patient/person and his/her healthcare providers can be inferred from the source of the information in the patient/person's EHR. One might infer for example, that if Dr. Leger has written a prescription for Bob Smith that is listed in Bob's prescription drug profile, then Dr. Smith is a member of Bob's circle of care. Dr. Leger might then be allowed to access other selected portions of Bob's EHR.

From an architectural point of view, Infoway considers geographic work groups and circle-of-care work groups to be the most viable forms of work group based access control. Whether they can (and should) be implemented in a given jurisdiction will require careful consideration.

7.5.5 Approaches to Discretionary Access Control

There are several instances where a healthcare provider (a primary care physician, say) should be able to confer to another qualified EHRi user access to a given patient/person's EHR. Several obvious examples are:

1. when a family physician refers a patient/person to a specialist.
2. when a family physician transfers care of a patient/person (and also a copy of attendant health records) to another family physician. In jurisdictions that have arranged for custodial control of the health profile portion of a patient/person's EHRi to be placed in the hands of the

patient/person's primary care provider (with attendant responsibility for update and maintenance), this transfer of control would be a necessary component of administering the health profile.

3. when a responsible physician cc's the results of a lab test or a diagnostic image to other consulting physicians attending to a patient/person who is critically ill. Some of those physicians would benefit for access to the EHR of the patient/person to gain valuable contextual information with which to interpret results and form a professional opinion on diagnosis or treatment.

Note that security requirement 63[54] ensures that discretionary access control does not "trump" role based access control; i.e., conferring access to a patient/person's record to another healthcare provider does not expand their role based access privileges. If a healthcare provider does not have a role that allows access to a prescription drug profile for example, then granting them access to a patient/person's EHR will not allow them to access the prescription drug profile of that patient/person – the point being that their role does not allow them access to the prescription drug profile of *any* patient/person.

While discretionary access control may be a viable adjunct to the EHRi's access control mechanisms, implementing jurisdictions need to carefully consider:

- the operational impact on healthcare providers (who must be able to unambiguously choose a delegate from a list and know with certainty that the "Dr. Smith" chosen is the right Dr. Smith, and
- ongoing management of these links, both for system administrators and for healthcare custodians.

7.5.6 Availability Requirements

The Access Control Service must remain continuously operational (i.e., with no scheduled downtime and robust resistance to equipment outage or denial of service attack), as without it, no user will be able to access a patient EHR.

In addition, user role information on users must be continuously available for user registered via the EHRi Trusted User Management model. By contrast, for users accessing the EHRi via the Organisational Trusted User Management model, role information is provided by the POS system through which the user has logged into the EHRi.

7.5.7 Implications of Access Control for Provider Registries and User Registries

Information on a user's role could come from one of three sources:

1. In the case of EHRi trusted user management, a user who is also a regulated healthcare provider will have a record in the provider registry. To implement EHRi trusted user management, professional roles (family physician, dentist, pharmacist, …) must be recorded in the provider registry for regulated health professionals This basic role information would consist of the regulated healthcare profession that the regulated healthcare professional belongs to and the specialisation involved where applicable (e.g. the medical specialty, if any, that a physician licensed to practice).
2. As there will also be a need to register EHRi users who are *not* regulated healthcare professionals, the user registry will need to contain role information captured during the registration of, for example, delegated EHRi users (see section 7.3.4 above).
3. POS systems will transmit role information as per section 7.5.3 and this information will be available during a user's EHRi session.

[54] See the Requirements document listed in the Reference section at the end of this document.

The above contains an implicit assumption about user registries:

Assumption 21	The user registry will contain (or link to) the professional role for each regulated healthcare provider who is registered as a user by way of EHRi trusted user management and will also contain the professional role of each non-regulated healthcare provider who is registered by way of EHRi delegated user registration.

7.5.8 Policy Enforcement

The access control service will require the definition and enforcement of access control policies. These policies will apply to all areas of access control. Examples of the definition and management of access control policies are:

1. establishing EHRi roles (including EHRi to EHRi roles),
2. establishing access privileges associated with EHRi roles,
3. POS user role to EHRi role mappings (to the extent that deployment model 2 above is instantiated), and
4. policies associated with authorised organisations connecting their POS systems to the EHRi.

The administration of access control policies (e.g.: the creation, update, merging and deletion of roles) would be, at least conceptually, a function of the general EHRi policy management service.

As with all privacy and security services defined in the conceptual architecture, it is expected that the access control service will enforce access control policies for all transaction requests within the EHRi common services.

7.5.9 Process Flow

Process flow in an **organisational trusted user management** environment presumes the following:

1. the user has a role assigned by the user's organisation, and
2. the POS system and user have already been authenticated (see section 7.4).

The Process is then as follows:

1. When a request comes in (1a), the HL7 message will contain the user's organisational role (e.g., Physician).
2. The access control service checks if the user's role authorises the user to perform the requested function.
3. The EHRi then makes request to the EHR data repository and other repositories on behalf of the user to get the PHI data. The EHRi passes the POS instance or Organisation ID, POS user ID, and the role of the user for further authorisation if necessary and uses all three for audit and logging.

Process flow in an **EHRi trusted user management environment** presumes the following:

1. the user has registered as an EHRi user through a web registration process and has been assigned an EHRi role during this registration process; and
2. the POS system and user have already been authenticated.

The Process

1. When a request comes in (1a), the EHRi uses the access control service (1b) to get the user's role (e.g., Physician).
2. The access control service checks if the user's role authorises the user to perform the requested function.

3. The EHRi then makes request to the EHR data repository and other repositories on behalf of the user to get the PHI data. The EHRi passes the EHRi user ID and the role of the user for further authorisation if necessary and uses the EHRi user ID for audit and logging.

7.5.10 Requisites

EHRi components required are:

1. the provider registry and/or user registries which contain professional roles that could be mapped to one or more EHRi roles,
2. creation of a jurisdictional EHRi role schema that addresses mapping of provider or professional role to an EHRi role which are then mapped to a POS system role,
3. HL7 standard messaging that allows for the inclusion of user role in the messaging, and
4. standardisation or harmonisation that maps roles from a jurisdiction to jurisdiction to be used for inter-jurisdictional transfers of PHI.

7.5.11 Service Components

Access control services include the following service components, which are described in Appendix A:

- A.3.1 Manage access control related business rules
- A.3.2 Manage user's role
- A.3.3 Manage association between user and work group
- A.3.4 Manage association between user and patient/person
- A.3.5 Authorise user

7.6 Consent Directives Management in the Desired Future State

7.6.1 Overview

The consent directives management service is intended to help EHRi users and their organisations comply with requirements in applicable legislation, as well as requirements for the handling of PHI found in various privacy policies and in patients'/persons' specific consent directives. The service works by applying requirements for the handling of PHI prior to providing access to or transmitting PHI via the EHRi. The service determines whether or not patients'/persons' consent directives allow or restrict the use and/or disclosure of PHI. If no such directives exist, then the service will respond to authorised access requests to PHI. The service also allows EHRi users to manage a patient/person's specific consent directives, such as blocking or masking PHI from a certain care provider or disclosing PHI without consent for emergency treatment, as required or permitted by law.

The service relies on a common privacy vocabulary to translate and apply consent requirements from legislation, policies and individuals' specific consent directives in an interoperable manner. Such a consent vocabulary is not yet fully developed or universally agreed upon and will need to be developed through a future Infoway or other jurisdictional and pan-Canadian initiatives. A common consent vocabulary would allow for the consistent labelling of consent-relevant objects and actions within and across jurisdictions in an EHR environment. The consent vocabulary would have to be based on Canadian health data protection statutes and other relevant privacy laws, as well as on internationally recognised best practices in privacy protection such as the CSA Model Code. A messaging schema for consent directives (which has yet to be developed) would rely on this vocabulary for universally accepted definitions of terms such as "implied consent", "consent revoked", etc.

The service consists of several service components described below in section 7.6.21. A full understanding of consent directives and the policy issues discussed in Appendix C is a pre-requisite for understanding this is service.

7.6.2 Rationale

Considerations of consent are essential to the successful operation of the EHRi. The consent directives management service is critical to the P&S Architecture since it allows for the clear, consistent translation and application of consent related business rules, including specific consent directives from individuals, in an EHR environment. Since these rules and directives may vary from organisation to organisation and from jurisdiction to jurisdiction, this service is fundamental not only to the assurance of privacy rights of Canadians but also to Infoway's goal of an interoperable EHR.

Finally, the consent directives management service is required for compliance with the basic privacy principle that consent in some form is required in order to ensure that individuals enjoy at least a certain degree of "control" over the collection, use and disclosure of their PHI in the Canadian healthcare system, even in jurisdictions with a "no-consent" model (the latter still require express consent for the disclosure of PHI for certain activities such as marketing).

7.6.3 Types of Consent

The type of consent required (express, implied, deemed or no consent) will vary depending on the purposes for which the information is collected, used or disclosed and the jurisdiction's statutory requirements.[55] There are four types of informational consent models governing the collection, use and disclosure of PHI for the purposes of health care treatment and delivery in Canada. They are:

1. a "no-consent" model (in British Columbia, Alberta, Manitoba and the Atlantic provinces);
2. a "deemed consent" model (in Saskatchewan);
3. an "implied consent" model (in Ontario); and
4. an "express consent" model (in Quebec).

Note that not all of these models are contained in separate health information legislation (e.g. as is the case in British Columbia, Quebec and the Atlantic provinces). See the consent appendix for additional information on each of these models. All four of the informational consent models are critical to the successful implementation of an interoperable EHR, where users from multiple jurisdictions will need to collect, access, use, disclose and retain PHI from the EHR in compliance with these different models.

These four types of informational consent models have specific architectural implications:

- **No Consent:** The jurisdictions in Canada operating under a "no-consent" model allow PHI to be collected, used and disclosed for treatment and care (e.g. Alberta and Manitoba)[56] without a patient's/person's consent. Note, however, that in these jurisdictions, individuals may still enjoy lockbox rights (i.e. be able to withhold or withdraw their consent for the disclosure of their PHI) that necessitate the ability for the consent directives management service to record, interpret and apply consent directives. In such jurisdictions the consent directives management system only requires functionality to record when patients/persons withdraw or revoke their consent for the disclosure of their PHI for treatment and care purposes – not that the patient/person has

[55] Note that the terms "knowledgeable" and "informed" are often used to describe the level of understanding a patient/person must have in order for consent to be considered valid. These terms have important policy implications – e.g., the posting of notices regarding a health information custodian's information practices in order to ensure consent is informed in Ontario – but these terms are not discussed further in this document since they do not have a direct technical impact on the P&S Architecture.

[56] See section 35(1) of the Alberta *Health Information Act* and section 22(2)(a) *Personal Health Information Act.* There remains a responsibility upon the healthcare custodian to collect, use and disclose PHI based on the over-riding principles of least amount of information, at the highest level of anonymity and within the context of a need to know.

given his or her consent to such a disclosure. From an architectural perspective, therefore, there is no functional difference between the "no consent" model where a patient can revoke or withhold their consent to disclosures of their PHI for treatment and care purposes and the "implied consent model" in regards to disclosure (see below).

- **Deemed Consent:** In those jurisdictions where consent for use or disclosure of PHI for treatment and care is "deemed" (e.g. Saskatchewan), the consent directives management system does not need to record any information related to the granting or revocation of consent for treatment and care, for the simple reason that patient/persons cannot withhold or revoke their consent for the use or disclose PHI for treatment and care.
- **Implied Consent:** In those jurisdictions with an "implied consent" model[57] for collection, use or disclosure of PHI for treatment and care, the consent directives management system need only record information related to the revocation of consent for use or disclosure of PHI. As noted above, there is no functional difference, from an architectural perspective, between the "no consent" model (with lockbox provisions) and the "implied consent model" in regards to the disclosure of PHI. However, for an “implied consent” to be valid, health information custodians or trustees must fulfill a number of policy and procedural requirements. These requirements are discussed in Appendix - C.
- **Express Consent:** Currently, only Quebec adopts an "express consent" model for use or disclosure of PHI for treatment and care (though this legislation is currently under review). Generally, express consent is required when PHI is disclosed to someone other than a health information custodian or trustee or for purposes other than provision of healthcare or those purposes permitted or required by law. Where express consent is required, the consent directives management service should record both the granting and the revocation of consent.

Health related legislation (e.g. public health statutes, health data protection statutes) typically allows, under certain conditions, for PHI to be used and disclosed for secondary purposes, such as health research authorised by a research ethics board,[58] public health surveillance and health care delivery quality assurance/improvement *without* a patient/person’s consent. Jurisdictions requiring a patient’s express consent or allowing a patient to opt-out of such uses and/or disclosures could use the architectural mechanisms for the withholding or revocation of consent (specifically consent directives tied to the role of researcher – see section 7.6.9 below) to effectively handle consent directives involving research. The primary focus of the architecture however is on consent related to the use and disclosure of PHI for the purpose of *health care and treatment*. Lastly, the terms “use” and “disclosure” of PHI are defined differently in various provincial health data protection statutes. Therefore, the P&S Conceptual Architecture must support the varying legislative definitions and interpretations of these terms.

7.6.4 Substitute Decision Makers

One of the fundamental tenets of informational consent is that, where it is required, the person providing consent must be competent to do so. As such, the consent directives management service must also allow for consent directives to be given not only by a patient/person who is the subject of the PHI at hand but also by an authorised representative (such as the patient’s/person’s legal guardian, a substitute decision maker, or a person having power of attorney), including providing functionality to store the identity and contact information of the patient’s/person’s substitute decision maker and identifying when consent directives have been given by the patient’s/person’s substitute decision maker rather than the patient/person.

[57] Organisations collecting information in such jurisdictions have additional non-technical requirements for the administration of implied consent (such as posting notices of their information practices).
[58] Consent is generally required by research ethics boards unless obtaining consent for a *bona fide* research protocol is determined to be impracticable.

The list of persons who are authorised to act as substitute decision-makers varies depending on the jurisdiction.[59] 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 of authorised substitute decision makers can be found (e.g. spouse or guardian), then the custodian must attempt to locate the next potential substitute decision maker in the ranking process (e.g. sibling). When a substitute decision maker has been found, the custodian must document the relationship that the substitute decision maker has vis-à-vis the patient/person to ensure that the substitute decision maker is sufficiently knowledgeable about the patient's/person's health conditions and wishes. (The recent U.S. case of Terri Schiavo illustrates the complexity that healthcare providers – and the courts – may face in identifying an "appropriate" substitute decision maker for an incompetent patient/person). Thus, establishing capacity to consent and providing for substitute decision-making are two of the most complex aspects of data protection.

7.6.5 Consent Directives, the Lockbox, and Masking of Personal Health Information

Individuals are able to make "express instructions" concerning allowable uses and disclosures of their PHI under sections 37(1)(a), 38(1)(a), and 50(1) of the Ontario *Personal Health Information Protection Act, 2004.* 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 individual who is the subject of the information relating to disclosure of the information, together with any other factors the custodian considers relevant.

The statutory right for an individual to restrict the use or disclosure of his or her PHI is known as a "lockbox", although this term actually tends not to be used in legislation. Note, however, that individuals may enjoy lockbox rights under different informational consent models in different jurisdictions (e.g. a "no-consent" model in Manitoba and an "implied consent" model in Ontario – see section 7.6.3 above). This means that EHRi users should *not* assume that there is an absence of restrictions on the use or disclosure of any PHI they access in an EHR from jurisdictions bound by a "no-consent" model simply because consent was not required for the collection, use or disclosure of that information; as illustrated above, the lockbox provisions clearly demonstrate that healthcare providers may have consent directives to manage even in a "no-consent" model. This is one of the many challenges of developing an appropriate consent directives management service – the service must be sufficiently flexible to support important commonalities between various informational consent models such as the lockbox, as well as support critical differences between the various models.

The ability for individuals to restrict uses and disclosures of their PHI may be implemented through a "masking" function provided by an EHRi, which, as the term implies, allows certain PHI to be masked or hidden from view.[60] Under specific circumstances outlined in law, PHI can be "unmasked" or

---

[59] See the Manitoba *Personal Health Information Act,* s. 60(d), the Saskatchewan *Health Information Protection Act,* s. 27(4)(d), and the Ontario *Personal Health Information Protection Act*, ss. 21-28.

[60] Masking is a term used to describe the process of restricting a transfer of PHI between two entities (e.g. regional health authorities, healthcare providers or jurisdictions). Typically, masking is applied at the data source and may be overridden, as permitted by law, by the accessing custodian (e.g. in emergency health situations). Organisations or jurisdictions may elect to apply masking functionality at differing levels of data granularity or by specific EHRi users, or roles. Custodians may be required to include a reason for overriding masked data (e.g. for unmasking PHI that was previously masked). It is considered privacy best practice to audit reasons for overriding masked data with a higher degree of regularity than "standard" accesses to non-masked PHI in support of ensuring that information is "unmasked" only on a need-to-know basis. A masking functionality can be used to restrict access to PHI for a variety of reasons, and not only when consent is withdrawn or withheld. For example, a jurisdiction or organisation may choose to automatically mask certain sexually

"unlocked". Generally, this can only occur when there is a perceived threat to the health or safety of the individual whose PHI is locked or to the health and safety of other individuals or for other legislatively required or permitted purposes (e.g. billing for health services rendered). For example, "locked" or "masked" PHI may be "unmasked" or "unlocked" for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons under section 40(1) of the Ontario *Personal Health Information Protection Act, 2004*.

The lockbox provisions are important to the consent directives management service because they raise difficult issues of how such provisions could or should be implemented. For example, legislation does not comment on the types of PHI or at what level of granularity an individual may "lock" or "mask" PHI, such as whether an individual can request that his or her entire record be locked, or only a subset of his or her PHI, such as a diagnosis, the individual's prescription data, or the individual's visits to a particular healthcare provider (e.g. mental health clinic). Similarly, legislation does not comment on a healthcare provider's obligation to provide services or treatment to a patient/person who has refused to "unlock" certain PHI. Note, however, that some healthcare provider associations have offered their own policy guidelines on this issue. For example, the College of Physicians and Surgeons of Ontario suggests to its members that they may refuse to treat individuals in non-emergency situations who will not disclose all of their PHI: "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."[61]

There are also other difficult EHRi implementation issues raised by the lockbox provisions, including whether the lockbox provisions give individuals the right to "opt-out" of the EHR entirely (e.g. can a patient/person instruct his or her healthcare provider to lock any and all references to his or her PHI in the EHR thereby "masking" the fact that he or she has ever been recorded in an EHR)?[62] In addition, it is not clear from the perspective of an EHR user how he or she would be expected to know whether an individual has PHI in a lockbox. Note that the under section 20(3) of the Ontario *Personal Health Information Protection Act*, however, that "if the disclosing custodian does not have the consent of the individual to disclose all the PHI about the individual that it considers reasonably necessary for that purpose" and that "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."[63] There is thus a legal requirement for Ontario health information custodians disclosing an individual's PHI in cases where they believe information in the lockbox to be relevant to the individual's care to inform the receiving custodian that the individual has not consented to the disclosure of all of his or her relevant PHI.

Healthcare providers in other jurisdictions do not appear to share the same legal "duty to notify" other healthcare providers to whom they are disclosing PHI that some PHI may be "locked" and, therefore, unavailable. However, it is important to note that some professional codes of practice imply such a responsibility. For example, the Canadian Nurses Association's "Code of Ethics for Registered Nurses" 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*" (emphasis added, p. 8).

---

transmitted disease test results. For this reason, the terms "lockbox" and "masking" are closely related, but are not synonymous.

[61] http://www.cpso.on.ca/Publications/Dialogue/1104/privacy.htm

[62] Under section 8 of the Saskatchewan *Health Information Protection Act,* patients/persons can opt-out of access to and disclosure of their "comprehensive health record."

[63] Ontario *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, s. 38(2).

7.6.6 Disclosures of PHI

One of the greatest challenges in applying the various informational consent models discussed in section 7.6.3 to a consent directives management service relates to the disclosure of PHI between jurisdictions where different informational consent models are in effect.[64] In legal terms, disclosures generally occur when PHI is released from one health information custodian or trustee to another health information custodian or trustee or to another organisation. Disclosures generally do *not* include transactions that occur for the purpose of information processing within a single health information custodian, trustee or organisation (which could involve multiple healthcare organisations in a single health region, for example) or if the information is processed by an agent of the organisation (e.g. individuals or organisations who act on behalf of the custodian or trustee such as nursing staff from a private agency or a vendor that provides technical support for a POS system).

Privacy and health information legislation generally requires healthcare providers who are *disclosing* PHI to jurisdictions other than those wherein the PHI currently resides (usually where the PHI was originally collected) to ensure that the receiving jurisdiction has "comparable safeguards" in place to protect the privacy and security of the PHI it will receive. But it is difficult to apply this requirement from a consent perspective in an interoperable EHRi environment. For example, does this mean that jurisdictions with an express or implied consent model should not disclose PHI to jurisdictions with a deemed or a no-consent model unless they can first obtain the express consent of the patient/person about whom the PHI relates? What if it is not possible to obtain such consent? This issue is further complicated by the lockbox provisions discussed in section 7.6.5 above. For example, what if express consent is not required for certain disclosures of PHI but a patient/person has expressly instructed his or her healthcare provider to lock certain PHI?

For this reason, the consent directive management service must have the ability to respect the consent directives wherein PHI was collected, and, wherein, presumably, consent directives were originally obtained. At the same time, however, the consent directives management service must also have the ability to respect new consent rights that a patient/person may enjoy in the *receiving* jurisdiction. For example, it is possible that PHI that was originally collected in a jurisdiction with a no-consent model may be legally disclosed to a jurisdiction with an express or an implied consent model or to a jurisdiction that permits a patient to now lock his or her PHI. This means that it is possible for the *same patient/person* to actually have *different* consent rights depending on the jurisdiction to which his or her PHI is disclosed; this is what makes the disclosure issue in an interoperable EHR environment so potentially complex. The consent directives management service must have sufficient flexibility to support the flow of PHI in multiple informational consent models that have both common *and* unique features (e.g. the "duty to notify" receiving health information custodians about locked PHI in Ontario). For this reason, section 7.6.7 outlines three potential deployment models for a consent directives management service and discusses the advantages and disadvantages of each model from a privacy and legislative compliance perspective. Infoway recognises that, depending on the informational consent model in effect, certain models may be more appropriate than others.

[64] Note that "disclosures" are different from "uses" of PHI. See section 1.6 above.

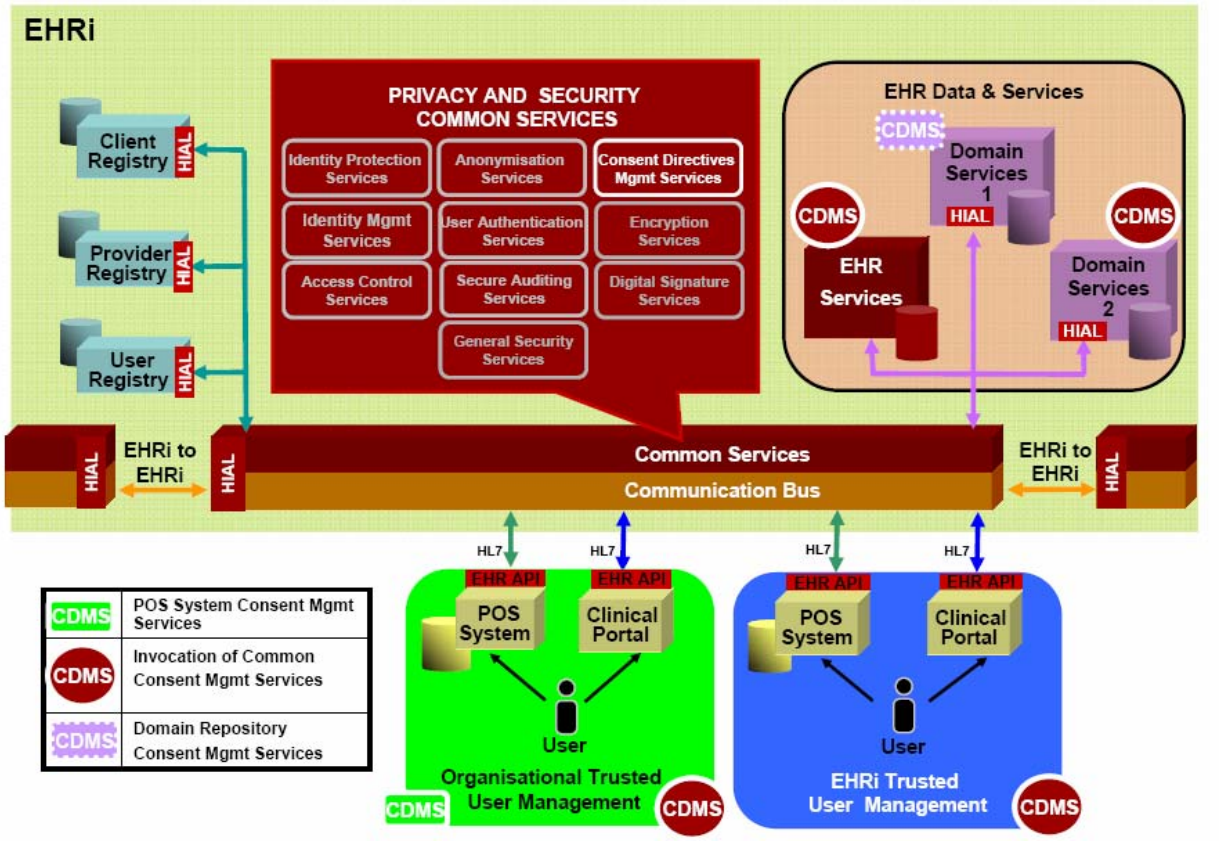

Figure 10: Consent Directives Management in the Desired Future State[65]

7.6.7 Approaches to Consent Directives Management

There are a number of potential approaches to managing consent in the EHRi, three of which are described below:

- **Consent Deployment Model 1 (Locally stored consent directives / Locally stored consent restricted PHI):** A POS System connected to the EHRi only sends PHI to the EHRi after locally applying consent directives. This means that PHI for which consent to use or disclose the PHI in question has been withheld does not appear in the EHR. Nor do the consent directives themselves. (In other words, the specific instructions from a patient/person to withhold certain PHI from the EHRi, or to withhold PHI from certain EHRi users, do not appear in the EHRi itself.) If consent is later revoked, the EHRi will take necessary actions to enforce the directive.

  Model 1 has the advantage that consent directives are applied at the data source (e.g. the information system that "originally" captures the patient's/person's PHI and associated consent directives) as is reasonably possible. PHI for which use and disclosure have been withheld would simply not appear within the EHRi. This model could potentially be used in jurisdictions where health privacy legislation enforces an "express consent" approach. (See Appendix C – Informational Consent for a description of the various informational consent models in effect in Canada).

[65] For more information on "informational consent", see Appendix C – Informational Consent.

This model has several disadvantages:

a) It does not comply with the legislative requirements of jurisdictions that require notifying health care custodians receiving PHI when the patient/person has not consented to the disclosure of all of his or her PHI.[66] For such jurisdictions, at least some information on consent directives would have to be stored in the EHRi to inform accessing users that patient/person PHI in the EHRi is incomplete (i.e., that other PHI has been withheld and such PHI could be deemed to be relevant to the patient's/person's care). This approach would also not support jurisdictional legislation which allows a health information custodian to disclose personal health information about a patient/person if they believe on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing the risk of serious bodily harm to a patient.[67]

b) The withheld PHI is simply not available via the EHRi, even in an emergency situation, and even if the affected patient/person is travelling and gives his or her express consent to access the information from another geographic location (another jurisdiction, say). This is a serious patient safety issue. It may also affect adoption of the EHRi by healthcare providers who will have legitimate concerns about the completeness of information provided by the EHRi under model 1.

c) Clinical information would likely be unavailable for research, even in anonymised form.

[66] For example, section 38(2) of Ontario's *Personal Health Information Protection Act* requires Ontario health information custodians disclosing a patient's PHI to inform the receiving custodian if the patient has not consented to the disclosure of all of his or her PHI in cases where the custodian believes that the information withheld by the patient to be relevant to the patient's care.

[67] See for example, section 41(1) of the Ontario *Personal Health Information Protection Act,* which allows a health information custodian to disclose personal health information about a patient/person if they believe on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

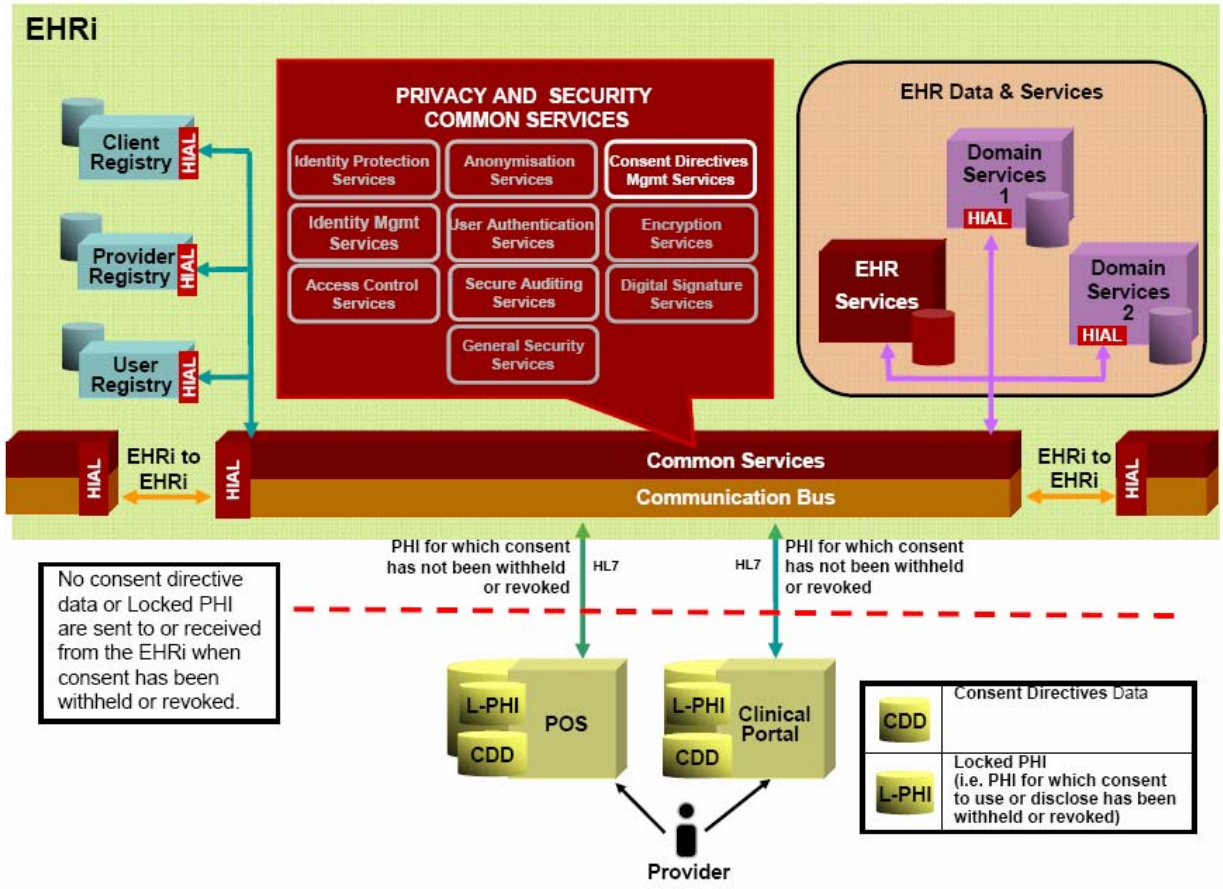

Figure 11: Consent Deployment Model 1 (Locally stored consent directives / Locally stored data)

- **Consent Deployment Model 2 (Centrally stored consent directives / Centrally stored consent restricted PHI):** PHI is copied to the EHRi along with any associated consent directives. This PHI data and the associated consent directives are then stored in the EHRi data repository or other storage system as outlined in the consent storage section. The EHRi then manages and applies consent rules based on these directives and provides the filtered information to the requestor.

  Model 2 has several advantages:

  a) It potentially complies with (or exceeds) the legislative requirements of all Canadian jurisdictions.

  b) It potentially allows PHI for which consent has been withheld to be made available in an emergency situation, or if the affected patient/person is later travelling and gives their express consent to access the information from another jurisdiction.

  c) It allows changes in consent directive to be deployed centrally, and respected across the jurisdiction immediately.

  d) Data stored centrally may (when anonymised) be available for research.

  e) The availability of clinical data does not depend upon the continuous availability of local POS systems and local networks and can therefore be potentially made more reliable.

  Model 2 has the disadvantage that it collects together (i.e., within the EHRi) PHI upon which a patient/person has expressly placed consent restrictions (i.e. has withheld or revoked consent to use or disclose of his/her PHI). This information must then be carefully protected, along with its

attached consent directives, and these directive must be processed upon every access to the record.

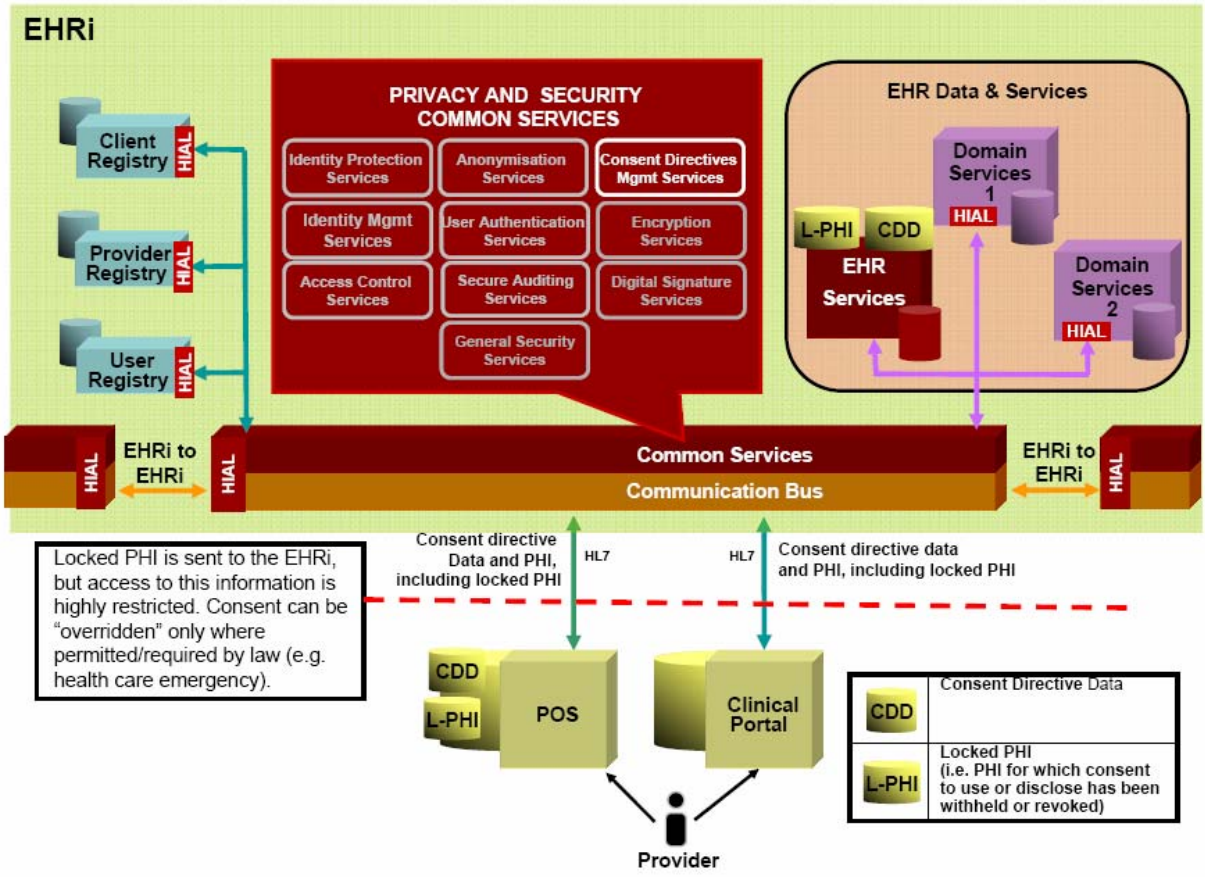

Figure 12: Consent Deployment Model 2 (Centrally stored consent directives / Centrally stored consent restricted PHI)

- **Consent Deployment Model 3 (Centrally stored consent directives / Locally stored consent restricted PHI):** A POS System connected to the EHRi, after locally applying consent directives (e.g. at the POS system level) and determining that PHI should be withheld, only sends information on the consent directive to the EHRi and does not send the withheld PHI. This means that PHI for which consent to use or disclose the PHI in question has been withheld does not appear in the EHR. Information on the consent directives themselves appears in the EHRi, at least in some rudimentary form (for example, that further PHI is available but that direct contact must be made with the patient's family physician before it can be obtained).

  Model 3 has three advantages:

  a) It potentially complies with (or exceeds) the legislative requirements of all Canadian jurisdictions.

  b) Consent directives are applied at the data source (e.g. POS system) as is reasonably possible. PHI for which use and disclosure have been withheld would not appear within the EHRi.

  c) It allows healthcare providers to strictly fulfil their custodial responsibilities with respect to the consent directives of their patients.

d) It potentially allows PHI for which consent has been withheld to be made available in an emergency situation, albeit by out-of-band methods (e.g. methods that are outside of the EHRi such as by telephone call). The practicality of obtaining this out-of-band information, especially from an EHRi in another time zone, is moot.

Model 3 has two disadvantages:

a) Information is not available online in an emergency situation. As most POS systems in physicians' offices will not be equipped to respond to asynchronous queries for PHI (much less enter into a productive automated consent directives negotiation exchange), PHI for which consent has been withheld will likely not be available via the EHRi. As with Model 1, this is a serious patient safety issue.

b) As with model 2, consent directives (which can themselves be of a highly confidential nature) must be stored centrally within the EHRi. From a patient privacy perspective, the very existence of some of these directives may be almost as confidential as (if not more than) the PHI they are intended to protect, hence vitiating some of the advantage that Model 3 conveys in not centrally storing withheld PHI within the EHRi. To mitigate this disadvantage, this section has discussed several other approaches to managing consent directives in an EHRi environment.

Table 3 summarised these considerations.

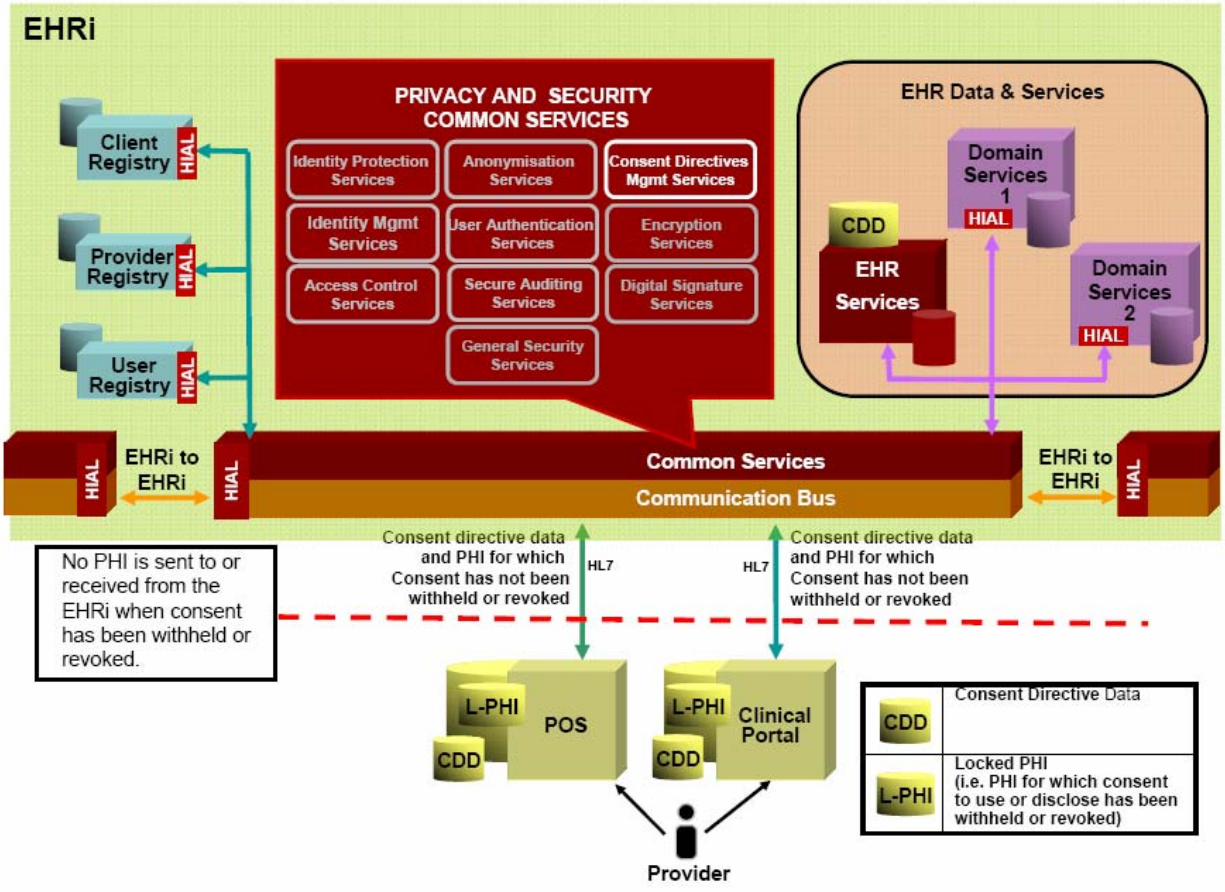

Figure 13: Consent Deployment Model 3 (Centrally stored consent directives / Locally stored consent restricted PHI)

Table 3: Consent Deployment Models Compared

	Consent Deployment Model 1	Consent Deployment Model 2	Consent Deployment Model 3
Where are Consent Directives Stored?			
Consent directives are centrally stored in the EHRi data repository or an associated consent repository.	No	Yes	Yes
Where is Consent Restricted PHI Stored?			
EHR data with consent restrictions attached are centrally stored in the EHRi data repository.	No	Yes	No
Advantages			
Potentially complies with (or exceeds) the legislative requirements of all Canadian jurisdictions.	No	Yes	Yes
Consent directives are applied as close to the data source (i.e. POS system) as is reasonably possible.	Yes	No	Yes
PHI is reliably available during medical emergencies.	No	Yes	No (except by out-of-band methods)

Of the three consent deployment models above, Infoway does not advocate pursuit of consent deployment model 1. The inability of the model to support compliance with applicable legislation in some jurisdictions, coupled with its associated patient safety risks, outweigh any advantages the model enjoys in protecting patient/person privacy. Of the remaining two models, deployment model 3 can in some sense be considered an architectural subset of model 2. This is because if the architecture can support model 2, it can also be made to support model 3. As such, both models will be supported by the EHRi conceptual architecture, and the model chosen for implementation in a given jurisdiction will depend upon the local jurisdiction's legislative and regulatory requirements.

7.6.8 Domain Repositories

Currently, domain repositories may have their own consent directives management system that is tightly coupled to the domain repository application. In such cases, only PHI that is filtered through the domain repository's consent system may be provided in response to a request from the EHRi. In the desired future state, consent directives management should ideally not take place at the domain repository level for reasons of economy and utility: three separate consent directives management systems for three separate domain repositories is expensive to develop and maintain and worse, may compromise the consistent and effective application of a patient/person's consent directives. .

7.6.9 Specificity of Consent Directives

Consent directives can also be specified at various levels of granularity:

- **All PHI:** a patient/person withholds or revokes consent to use or disclose any PHI stored in the EHRi;
- **PHI by Domain Repository**: a patient/person withholds or revokes consent to use or disclose all of his/her PHI stored in one or more domain repositories (e.g. place all pharmaceutical information into a "lockbox");,
- **PHI by Facilities:** a patient/person withholds or revokes consent to use or disclose his/her PHI by facility ID (e.g. this is a common request of staff within a healthcare facility);
- **PHI by Role –** a patient/person withholds or revokes consent to use or disclose his/her PHI by EHRi User role (e.g. researcher – see section 7.5.3 on approaches to role based access control);
- **PHI by EHRi User** – a patient/person withholds or revokes consent to use or disclosure of his/her PHI by EHRi User identity; and
- **Data element:** a patient/person may withhold or revoke consent to use or disclose a specific record or data field in the EHRi.

All of the above levels of granularity requires that the POS systems connected to the EHRi must be able to collect and transmit such directives. Consent directives may be enforced at different places within the EHRi, such as within data repositories or the EHRi common services.

At a minimum, EHR level granularity must be supported, as it is a legislative requirement of jurisdictions such as Saskatchewan where a patient/person may withhold consent to disclose his/her PHI to a comprehensive health record such as the EHRi. Domain repository level granularity must be provided because existing domains repositories (such as BC Pharmanet) allow patients/persons to restrict access to their PHI.

The extent to which data level granularity must be provided remains an open question. No jurisdiction explicitly demands field level granularity in the execution of consent directives, but this is not to say that such granularity might not be provided for by regulation, by a Commissioner's order, or by widespread public opinion at some future date. In the absence of firm guidelines to the contrary, it is prudent to presume that the P&S conceptual architecture must support the execution of data level consent directives (i.e. directed at specific fields or groupings of fields). Further work needs to be done in this area to standardise upon consent directives in terms of how coarse or fine-grained such directives can be.

7.6.10 Consent Directives Targeted At Specific Providers or EHRi Users

Can a patient/person formulate a consent directive that prohibits or otherwise limits access to the patient/person's PHI by a specific healthcare provider or other EHRi user (e.g.: medical receptionist, hospital ward clerk, etc.)? Privacy advocates have repeatedly raised the issue and patient rights advocates have articulated the need for directives of this kind to be honoured. Attempts to restrict access by a specific individual (a relative, ex-spouse or neighbour of the patient/person, for example) are amongst the most commonly articulated form of consent directive encountered by hospitals.

Because the EHRi relies on provider registries, support for this form of consent directive can be readily carried out, provided the individual in question is a regulated healthcare provider with a record in the provider registry and hence consistently identified throughout the EHRi and connected POS systems. Consent directives restricting access by users of the EHRi who are not regulated healthcare providers (and therefore would not have records in the provider registry) can only be carried out in an EHRi trusted user management environment where such providers have a unique EHRi user ID. An EHRi that supports one or more organisational trusted user management environments *cannot* effectively support

consent directives that restrict access by such organisational users, except in the following restricted case:[68]

1. the consent directive specifies a user by POS system user ID,
2. the user in question accesses the EHRi, via an organisational POS system, using the same POS system user ID that was specified in the consent directive (as opposed to accessing from some other organisation's POS system or directly via an EHRi user ID).

Table 4 summarises the available support for consent directive that target specific users.

Table 4: Support for Consent Directives Targeting Specific Users

	EHRi Trusted User Management	Organisational Trusted User Management
Consent directives that target specific regulated healthcare providers	**Yes**	**Yes**
Consent directives that target specific EHRi users who are not healthcare providers	**Yes**	**No** **- except where the accessing user is identified by the same POS system user ID that is used in specifying the consent directive**

7.6.11 Overriding Consent Directives

Jurisdictions allow consent directives to be overridden under certain limited circumstances and the conceptual architecture must therefore support an override capability. Not all users' roles will be able to exercise override ability, so this has implications for the Access Control Service 7.5. Overriding of consent directives must also be logged (see section 7.6.14).

Purposes for which patient/person consent directives can be overridden are outlined in legislation and vary across jurisdictions. Typical permissible uses and disclosures of PHI where the patient/person has withheld or revoked consent are:

- billing purposes (although this is not applicable to the operation of the EHRi),
- health research that is approved by a research ethics review board[69] (though the research capabilities provided by the identity protection service and the anonymisation service ought to render such an override unnecessary),
- compliance with a court order,
- reporting of specific communicable diseases,
- in situations where the custodian or trustee believes that the disclosure is necessary for the purpose of preventing or reducing a significant risk of serious bodily harm to a patient/person or a group of patients/persons.

However, in Alberta, the overriding of consent directives is more discretionary whereby a physician is not required to honour a consent directive, but only must “consider as an important factor any

[68] This is because the EHRi would not have a unique identifier for every EHRi user.
[69] As mentioned above, consent is generally required by research ethics boards unless obtaining consent for a *bona fide* research protocol is determined to be impracticable.

expressed wishes of the individual who is the subject of the information relating to disclosure of the information, together with any other factors the custodian considers relevant."[70] For this jurisdiction, a sixth reason for overriding consent would therefore be "at the discretion of the custodian". See Appendix A.4.6 for a discussion of patient/person access control service.

7.6.12 Storage of EHR Data That Has Associated Consent Directives

There are two broad approaches to the storage of consent directives within the EHRi:

1. **General storage of PHI with associated consent directives**: when EHR data is sent to the EHRi with associated consent directives, the affected EHR data would be stored no differently that other EHR data (i.e., EHR data would be stored with the associated consent directives and as such, would be stored no differently than EHR data that has no associated consent directives); or
2. **Separate secure storage of PHI with associated consent directives**: when EHR data is sent to the EHRi with associated consent directives, or when new consent directives are received for data previously uploaded to the EHRi, the affected EHR data would be stored in a highly secure and physically separate database, and in an encrypted format if required.

An argument can be made that *all* EHR data should be highly secure and hence whatever special precautions are to be taken for the storage of EHR data with associated consent directives should also be taken with regard to *all* EHR data.[71] This is in keeping with the uniform classification of PHI for the purposes of confidentiality and integrity (see section 5.2). Nevertheless, practical considerations such as the expectations of patients/persons to take extraordinary measures in the securing of so-called "lockbox" data and the expectations of healthcare custodians that such data is truly "locked away" suggest that EHR data with associated consent directives merits security and privacy provisions beyond what has been provided for with other EHR data. At a minimum, such data could be physically separate and stored in a format that prevents unencrypted access, even by database administrators. If all data in the EHRi data repository is encrypted while in storage (see 7.9) and the identity protection service is used to ensure the scrupulous separation of all identifying data (e.g.: name, health number, and other public identifiers) from non-identifying heath-related data (see section 7.7), then this discussion of separate secure storage of PHI with associated consent directives becomes redundant.

7.6.13 Storage of Consent Directives

The EHRi consent directives management service requires the storage and availability of consent directives. Infoway believes that this would involve the use of consent related metadata. The metadata for various domains will be based on templates that conform to a specific nationally adopted schema. Various storage options are possible, including:

a) Storing consent directives along with EHR data: This approach could work for the EHR data repository but may be difficult and costly to implement in a domain repository that has a tightly coupled consent directives management system. Our desired future state presupposes that domain repositories would rely on all of the EHRis' common services, including consent directives management. Moving to a common service approach to consent directives management from a domain repository consent directives management solution would require substantial modification to those domain repositories. Data inserts into and access from the domain repository will be slower because of storing and

[70] Section 58(2), Alberta *Health Information Act,*

[71] EHR data that yesterday had no associated consent directives may, at the discretion of the subject of care, acquire such consent directives today. The data hasn't changed, merely the perception of its confidentiality. So if special security provision must be put in place today to secure this data, and the data itself hasn't changed, shouldn't such provisions have been in place yesterday?

processing of the additional consent information but access to EHR data will be quick. Management of consent information will be a challenge.

b) Consolidated storage of consent directives: A consent profile conforming to a nationally adopted schema will be necessary for each domain to allow for appropriate information to be loaded in the consent repository. This approach will likely have a faster adoption rate and come at less cost due to its ability to integrate into legacy domain repositories. However, this will have an impact on performance as every request would need to access the consent repository.

There are several technological approaches to effectively securing such consent directives. Privacy enhancing technologies include identity protection services (see section 7.7 below) and encryption services (as applied to data storage; see section 7.9 below). These technologies should be applied not only to consent directives stored in the EHRi but also to consent directives stored in local POS systems.

7.6.14 Transmission of Consent Directives

Consent directives need to be applied *prior* to disclosure of PHI. Each jurisdiction needs to ensure that they comply with their own legal requirements for consent. Jurisdictional implementations of the EHRi must provide all consent functionalities necessary to comply with that jurisdiction's legal requirements regarding consent. Within a jurisdiction, the processing of consent directives has three components:

1. effective transfer of consent directives from POS systems to the EHRi;
2. processing by the EHRi of all consent directives prior to disclosing a patient's/person's PHI in response to an access request; and
3. transfer of associated consent directives from the EHRi to POS systems whenever PHI is disclosed in response to an access request.

Inter-jurisdictional disclosures of PHI cannot take place until all of the consent requirements of the disclosing jurisdiction have been met. Once this has been achieved, relevant PHI along with any related consent directives can be transmitted by the EHRi where the PHI is stored to the EHRi of the jurisdiction where the access request originates. The extent to which these consent directives are effectively enforced by POS systems with a receiving jurisdiction that does not have the same legal requirements (and hence technical functionality) with regards to consent, is a source of concern. Policy needs to be in place to effectively deal with this issue (see section 7.6.17 below).

7.6.15 Implications for Secure Audit Service

An important privacy requirement relates to the logging of consent directives. **Privacy Requirement 13 (Logging the Application of Consent Directives)**, states [in part] that the EHRi must be able to:

a) log when the processing of consent directives 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.

Security Requirement 38 (Logging Transactions in the EHRi) states in part that the EHRi must create a secure audit record each time a user …

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

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

7.6.16 Implications for Alerts and Notifications Service

The consent directives management service will call upon the notification service. An important privacy requirement relates to the logging of consent directives. **Privacy Requirement 13 (Logging the Application of Consent Directives)**, states [in part] that the EHRi must be able to:

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

7.6.17 Availability Requirements

The Consent Directives Management Service must remain continuously operational (i.e., with no scheduled downtime and robust resistance to equipment outage or denial of service attack), as without it, access requests cannot be processed in a privacy protective manner.

7.6.18 Policy Enforcement

Jurisdiction must create and enforce policies to ensure that they comply with their own legal requirements for consent, including when PHI is transmitted across jurisdictional boundaries. Jurisdictions need to agree upon and set policies as to how consent directives made in one jurisdiction will be managed following disclosure to another.

Enforcement of consent policy has five essential components:

1. process all applicable consent directives prior to disclosing PHI to an authorised EHRi user and prohibit disclosure where directed;
2. transmit applicable consent directives when information is disclosed;
3. log when disclosure has been prohibited as in 1) above;
4. log when a consent directive has been explicitly overridden (e.g. for purposes of emergency treatment) and the reason for the override as expressed by the overriding user; and
5. alert the individual accountable for facilitating privacy compliance in the organisation where the accessing user works as well as in the organisation where the information was collected when a consent override has occurred.

The EHRi will enforce consent policy at every access to EHR data and domain repository data. Consent directives will be processed whether an access request is received from a POS system or clinical portal connected to the EHRi, or from an EHRi in another jurisdiction.

7.6.19 Process Flow

The Process flow description below presumes the following:

- the user has already been authenticated;
- the user has been authorised to perform requested function;
- some domain repositories may maintain their own consent directives management mechanisms.

The Process is as follows:

1. The EHRi Consent directives management Service checks if the patient/person in question has consent directives at the EHR level. If "Yes", the user is informed that consent to disclose any data is withheld and proceeds to step 5. If "No", then proceed to step 2.
2. The Service checks if the patient/person in question has consent directives at the domain repository level. If "Yes", then the user is informed that consent to disclose domain repository data is withheld and proceeds to step 5. If "No", then proceed to step 3.
3. Where domain repositories have their own consent mechanisms (3a and 3b), such domain specific consent processing is carried out. If consent is withheld by the domain repository, then the user is informed that consent to disclose domain repository data is withheld and proceeds to step 5. If consent is not withheld, then proceed to step 4.

4. The Service checks if the patient/person in question has consent directives at the data level. If "Yes", then the user is informed that consent to disclose specific data is withheld. If "No", then proceed to step 5.
5. The user's role is examined. If the user's role does not permit overriding of consent directives, proceed to step 7. If the user's role permits overriding of consent directives, then the user is informed of the consequences for overriding consent (including notification of a privacy officer) and then queried as to whether to override consent. If "Yes", then the user chooses a reason for the consent override. Proceed to step 6.
6. Data is requested from the EHR data and domain repositories (2a) and returned to the user.
7. Data not withheld by the consent directives, if any, is requested from the EHR data and domain repositories (2a) and returned to the user.

7.6.20 Requisites

A user registry is required for general auditing of consent directives creation and overriding. The consent directives management service requires a robust client ID (PHI level consent revocation or withdrawal), provider/user (user and role level consent revocation or withdrawal), and Organisation ID (organisational level consent revocation or withdrawal).

The consent directives management service requires a nationally adopted messaging schema that allows for the effective conveyance of consent directives between two EHRis, and between each EHRi and POS systems connected to it. Jurisdictions would be required to adopt and apply with this schema.

Identity protection service and encryption services are also required to support the service.

Finally, jurisdictionally adopted and applied schema for the storage and application of consent directives are also required to support this service.

7.6.21 Service Components

- A.4.1 Manage Consent-Related Business Rules
- A.4.2 Manage Patient/Person Consent Directive
- A.4.3 Validate consent
- A.4.4 Map consent (between and among jurisdictions)
- A.4.5 Override Consent
- A.4.6 Patient/person access control service
- A.4.7 Log Consent Directives and Their Application

7.7 Identity Protection in the Desired Future State

7.7.1 Overview

To ensure the highest level of anonymity of PHI when stored or in transit between EHRis, information that uniquely identifies an individual should be separated to the greatest degree possible from other information about that individual's health status, diagnosis, treatment, etc. The Identity Protection Service would be more beneficial in those situations where the information being protected is stored centrally. Storing a patient's/person's identifying information in one location and the non-identifying portion of his or her EHR data in another location will reduce the potential impact of a privacy breach. Conceptually, this service will link an individual's public identifier(s) (PIDs) to a matching EHRi client identifier (ECID) – the latter a meaningless but unique number – in order to locate and retrieve PHI or any other personal identifying information stored in or accessible via the EHRi (e.g. a patient's/person's consent directive information) requested by an authorised EHRi user.

Other meaningless but unique numbers know as “federated identifiers” (FIDs) will exist to facilitate the matching of a patient/person’s ECIDs between jurisdictions or “identity domains”[72], without having to actually disclose the ECID across jurisdictions. This can be accomplished by assigning an FID to the related ECID in each identity domain in which they exist (e.g. if an ECID was created in Quebec for a patient/person, who already had an ECID in Ontario, an FID would be assigned to the two ECIDs to enable authorised users to retrieve the data in the future).[73] FIDs will allow for PHI to be shared between jurisdictional implementations of the EHRi without disclosing a patient’s/person’s ECID, which is a key design principle of the Identity Protection Service. ECIDs are used to resolve a patient’s/person’s identity *within* one or more EHRis and would not be published or otherwise made available to EHRi users or between EHRis.

Finally, a pseudonymisation service will provide pseudonymised health information to authorised researchers, public health surveillance officials and other authorised users; such pseudonymised information will contain a meaningless but unique identifier that serves operates in the same manner as the ECID described above – e.g. the pseudonymous identifier (pseudo-ID) is linked to the patient/person's PHI in such a way that the patient/person's identity is never revealed (this identifier functions as a pseudonym for the patient/person, hence the name pseudonymisation). Such pseudonymised data allows for longitudinal studies. In some ways, a pseudo-ID can be considered a special type of FID.

The diagram below shows the relationship between PIDs, CIDs, FIDs, and Pseudo IDs.

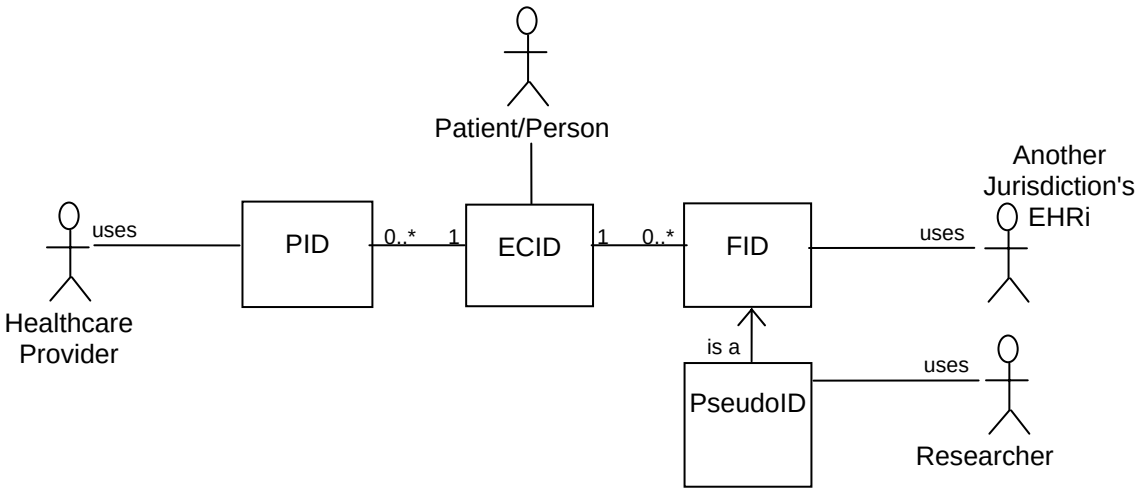

Figure 14: PIDs, ECIDs, FIDs, and Pseudo IDs

[72] Identity domain is an entity for which one ECID is used to identify an individual. Typically each EHRi would constitute an identity domain. However, jurisdictions could choose to implement ECIDs at the domain repository level, resulting in a number of identity domains per jurisdiction, or, alternatively, identity protection services could be deployed using a shared ECID between two or more jurisdictions. However, Infoway recommends that the identity protection service be deployed at the common services level of the EHRi – i.e. provincially or multi-provincially. Each EHRi implementation would therefore ideally have one ECID per patient/person.

[73] FIDs allow EHRis to rapidly share PHI in a manner that maximises patient/person privacy (i.e. shares information anonymised to the highest degree possible) and minimises the vulnerability of subsequent breaches in the event that the identifier is compromised during or subsequent to transit. For additional information on FIDs see section 7.7.4 below.

As illustrated Figure 15 below, domain repositories within the EHRi will use the common identity protection service provided by the EHRi common services. The service would not be called directly by POS systems nor will separate identity protection services exist within separate domain repositories in the EHRi.

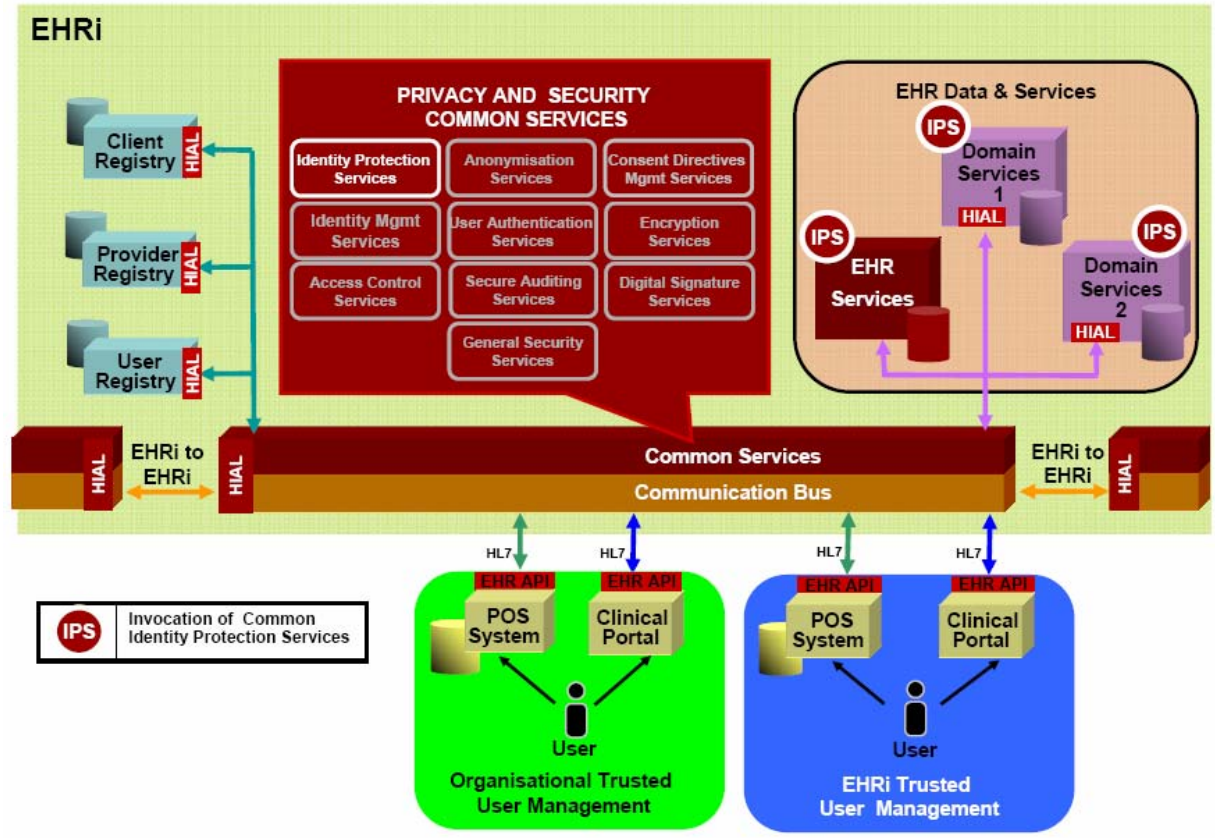

Figure 15: Identity Protection Service in the Desired Future State

Note: Infoway appreciates that identity protection technology is immature and no commercial off the shelf identity protection solutions or standards in support of an identity protection service currently exist. For this reason, Infoway encourages users of PHI to work closely with system developers, privacy architects and other privacy stakeholders such as community representatives and Privacy Officers at health information custodians to support the development identity protection applications and standards.

7.7.2 Rationale

Recently, several privacy breaches have occurred involving the theft of or inappropriate access to large databases containing significant quantities of personal information. Such a privacy breach to an EHR would erode public trust in an EHR for years to come. To reduce the potential of such privacy breaches, *Infoway* strongly suggests that based on risk assessments PHI not be stored with any associated identifying information. Decoupling identifying information from its related PHI means that if a security breach occurred relating to any of the information repositories (identifying information, the EHR or domain repositories, or the linking tables) the data disclosed by the breach would not lead to the identification of a patient/person and a loss of confidentiality of their PHI. In addition to limiting the risk of inadvertent disclosures of PHI through the separation of PHI from identifying information, expected benefits of a comprehensive Identity Protection Service include:

1. Maintaining the integrity of ECIDs requires by definition that those identifiers remain internal to the identity domain. Sharing an ECID between one jurisdiction's EHRi and another's, creates serious problems for the maintenance of referential integrity.

2. Providing a means for EHRis or identity domains to control their own ECIDs. ECIDs would not be shared amongst identity domains, which will assist in preserving the confidentiality of CIDs.
3. In an EHRi environment where PHI is not replicated from one EHRi to another or in POS systems, the identity protection service could be used as a means of ensuring confidentiality of PHI through providing a means by which patient/provider relationships can be established. Once an intra-EHRi exchange of PHI is determined to be necessary (e.g. an EHRi user accessing another EHRi has a need-to-know a patient's/person's PHI) and an FID is created, it eliminates the need to recreate an FID for access to the PHI in the future as well as, potentially, eliminating the need to recreate the FID for future access requests by members of the same care team or access requests related to the same episode of care. The FID that is created to facilitate the disclosure could contain logic that would allow the FID to persist only until the need to know the PHI - for which the FID was created to facilitate – no longer exists (e.g. at the conclusion of particular episode of care).[74] Once the need to know the PHI no longer exists, the FID could be deleted and the related PHI would become inaccessible until a new FID was created. This scenario presumes that certain processes (either through manual or automated means) exists that would allow the Identity Protection Service to determine the length of time a need-to-know would be valid, and that such a duration could be used to determine the length of time an FID would exist. Such a process would require rigorous oversight to ensure that valid access requests could be provided on a near real time basis and that potential malicious or invalid access requests were not granted.
4. Allowing for a relatively simple means by which to provide access to pseudonymised PHI for authorised purposes such as public health surveillance or health research.

Infoway believes that potential applications of an IPS could include: a consent repository, a privacy enhanced secure auditing services, an EHR data repository or domain repositories,

7.7.3 Identity Domains

An identity domain is the level at which a single ECID is deployed. Access to PHI within a specific identity domain will be managed and coordinated through the identity protection service within the EHRi common services. A patient/person would have one ECID in each identity domain where his/her PHI was located. Transfer of PHI between identity domains would utilise FIDs to identify data without requiring the exchange of ECIDs, a key privacy enhancing design feature of the Identity Protection Service.

As discussed above, identity domains could, in theory, be deployed within each domain repository or with a health region but such a deployment of identity domains would require FID mappings not only between EHRis, as discussed below, but also between each identity domain within the EHR. This would result in an overly burdensome process that may result in variations in the quality, effectiveness and efficiency of the identity domains and the related identity protection service. Infoway believes that such an approach would be overly burdensome and while reduced sharing of ECIDs would have a positive benefit on patient/person privacy, the complexity of such a system might prove operationally problematic. For this reason Infoway recommends the implementation of the identity protection service at the EHRi level, likely at the provincial or multi-provincial level. This would mean that in each deployment of an EHRi a patient/person would be provided with one or more public identifier, such as a health card, a medical insurance plan number, or an assigned PID for patients/persons without a PID. These numbers would be mapped to a single ECID. If the individual had received care or treatment in multiple jurisdictions, his/her ECID would also have an assigned federated identifier or FID.

[74] For more information on the creation of FIDs, see section 7.7.4 below.

7.7.4 Approaches to FID Deployment

FIDs are used to enable the sharing of PHI between identity domains without disclosing the patient's/person's ECID, the unique identifier under which PHI in the EHRi is stored

FIDs are created when a there is a justifiable need-to-know PHI in one jurisdiction and the information is stored in another jurisdiction.[75] Criteria for the matching of ECIDs for the purpose of uniquely identifying patients/persons[76] as well as authorised reasons for accessing PHI, EHRi user roles that may access PHI and to what PHI those roles would have access would need to be established as part of the development of an interoperable Identity Protection Service. The extent to which privacy protections are built into the FID creation process will determine the extent to which the Identity Protection Service provides an effective means of protecting patient privacy between identity domains. For example, if PHI can only be accessed for a particular episode-of-care, after which the FID would be deleted or an oversight body existed that manually facilitates the creation and deletion of FIDs, FIDs could be created that would only exist and provide access to PHI for the period of time a need existed to know the PHI. Such a process would be much more resource intensive than allowing EHRi users to create FIDs that would exist for an indefinite period of time for patients/persons to whom they may or may not be providing health care and treatment; the former approach, albeit more laborious, would be preferable as it is much more likely to protect patient privacy as well as jurisdictional statutory requirements with regards to disclosures of PHI outside of the province. Conceptually, upon receiving a request from an authorised EHRi user for a patient's/person's PHI stored in other jurisdictions, the identity protection service would locate or facilitate the location of all of a patient's/person's ECIDs in all jurisdictions where relevant PHI existed and link them under one FID. The FID could then be used to access all available and relevant PHI in all jurisdictions.

Deployment models for FIDs could also vary. For example:

- **FID Deployment Model 1: Centrally Administered Universal FID -** It would be possible to create a central FID system that would facilitate the matching of patient/person records across EHRis. The central FID system would, when provided with an ECID from an authorised user, return all of the patient's/person's PHI from all EHRis that may be relevant to the request. Such a system would require that an FID be created for each patient/person that has received healthcare or treatment in more than one jurisdiction and for whom there is a need to access his/her PHI across jurisdictions. The FID would exist only in the FID central management system and would not be shared with jurisdictions. This FID central management system would oversee the creation of FIDs and the matching of ECIDs under FIDs. Such a system would allow for identity domains to offload the operations of an interoperable FID to a central location.

  Model 1 has the advantage in that its centralised management of FID allows for the consistent application and administration of FIDs as well as increasing the likelihood that the FID component of the Identity Protection Service would be robustly designed and implemented.

  Model 1 also has some disadvantages; given that the provision of healthcare is primarily a provincial/territorial responsibility, the operations of a centralised FID system may prove difficult to operationalise. Also, this model requires the outsourcing of responsibility for intra-jurisdiction linking of personal identifiers to a third party, which may not be supported by privacy legislation.

---

[75] An FID would not necessarily need to be created every time a patient/person seeks healthcare in a new province as would be the case that any time a patient/person seeks medical care and treatment a care provider would not always require a patient's entire medical history (as might be the case with a patient/person with a sprained ankle).

[76] The Identity Protection Service will need to support probabilistic as well as deterministic matching of ECIDs. In some cases a patient's identity may not readily be able to be ascertained. In such cases limited subsets of information should be made available to validate a patient's person's identity. In the case of emergency healthcare providers may need to be provided with emergency override capabilities. Such overrides would need to be audited on a near real time basis to control against unauthorised use.

- **FID Deployment Model 2: Jurisdictionally Administered Universal FID -** A second deployment model would require that an FID be created for each patient/person that has received healthcare or treatment in more than one jurisdiction and for whom there was a need to access PHI across jurisdictions. This single FID would be shared between all jurisdictions where a patient/person is assigned an ECID.

  This deployment model has an advantage over Model 1 that it could be administered at the EHRi identity domain level. This approach would require one interoperable FID for all identity domains. This standardised approach would have the benefit of simplicity.

  Model 2's distributed administration of FIDs would be much more complex in practice than the centralised approach of Model 1. This model would have the potential to make FIDs a national healthcare identifier (if FIDs were not deleted once the need to know the PHI no longer existed), which is undesirable from a privacy perspective.

- **FID Deployment Model 3: Jurisdictionally Administered Relationship-based FID -** A third deployment model would create an FID between each identity domain where the patient/person had an assigned ECID – i.e. if a patient had received care in Alberta, Manitoba and Quebec, in Alberta he/she would have three FIDs – one for the Alberta/Manitoba ECIDs, one for the Manitoba/Quebec ECIDs and one for the Alberta/Quebec ECIDs. This approach would have the benefit that EHRi would not have to broadcast an FID to all other EHRi in order to determine if a patient/person has in fact been assigned an ECID in anther jurisdiction, as in Model 2, which may also be susceptible to unauthorised requests for/access to PHI, Whereas, in this model requests for PHI would only be sent to those identity domains where an individual had been assigned an ECID.

  Model 3 would be beneficial from a privacy perspective in that the identifier would not be national in nature – an FID in this model would never identify a patient/person in more than two identity domains. This approach would require each jurisdiction to standardise FIDs with each other jurisdiction. This model might be deployed in an interoperable and standardised manner, but might also be deployed on an identity domain to identity domain basis, which would make the system much more complex to implement and administer than Models 1 or 2.

Infoway believes that all three of the above discussed models would effectively work to protect an individual's PHI and emphasises that the underlying requirement of all three models is common standards for FIDs and the importance of deleting FIDs on a regular basis. Furthermore, Infoway appreciates that for FIDs to be of maximum benefit from a privacy perspective, PHI would need to be stored only in the EHRi where it was collected and not replicated in accessing EHRis and POS systems connected to those EHRis, but this may not be possible in the immediate future due to constraints imposed by legacy health information systems, but could be achieved in the interim through the use of a clinical portal based deployment model.

As a practical matter however, model 1 is unlikely to be implemented, if only because of the multi-jurisdictional nature of healthcare delivery in Canada and the pragmatic difficulty of obtaining agreement on central administration of FIDs across 14 jurisdictions. Model 2 is not as privacy protective as Model 3 but likely no more difficult to implement than model 3. For these reasons, Infoway recommends model 3.

7.7.5 Implications for Client Registries

In the context of the EHRi, the identity protection service is a common service provided by the EHRi that exist as a broker between a jurisdictional client registry and jurisdictional domain repositories. The identity protection service is therefore inextricably linked with the deployment of client registries and should be developed in conjunction with client registries where they do not already exist.

7.7.6 Pseudonymisation Service

The functionality described in the above identity protection service could be further leveraged to facilitate research and public health surveillance with pseudonymous PHI. Such pseudonymous data would allow for longitudinal studies. The service would be made available to public health officials and

researchers, as authorised by research ethics boards and provincial health data protection legislation, to carry out their research using pseudonymous PHI via the EHRi. The service would provide algorithms to generate meaningless but unique identifiers from a patients'/persons' ECID and that could be used to access the patient's/person's non-identifiable PHI. Such a key would expire after a pre-specified period of time and could be designed to provide access only to specific data elements germane to the research being undertaken. Like all users accessing the EHRi, researchers accessing the pseudonymisation service would be uniquely identified and information pertaining to their access to non-identifiable PHI would be logged and could be audited. Researcher would not be able to modify, delete or otherwise manipulate the non-identifiable PHI they access in the EHRi.

7.7.7 Availability Requirements

If the Identity Protection service is used to protect store PHI by linking between identifying information and non-identifying information, then the availability of the service is as least as high as the availability requirements for the data protected.

Where the Identity Protection service is used to provide Pseudo IDs, the availability requirements are low – pseudo ID generation is needed for research data requests and could be delayed for days if necessary.

7.7.8 Policy Enforcement

Policy enforcement for the identity protection service will always occur in the EHRi common services.

7.7.9 Process Flow

The Process flow for Identity Protection is as follows:

1. An EHRi user requests PHI for a patient/person using his/her public identifier (typically a health insurance, medical services plan or healthcare number)
2. The EHRi requests an ECID related to the provided public identifier.
    a) If no ECID exists for the patient/person (i.e., if no data for the patient/person has already been stored in the EHRi), one is created; otherwise the ECID is returned to the identity protection service.
    b) If the patient/person has an existing ECID within the EHRi, the PHI stored under the ECID in the EHR data repository and domain repositories are returned.
3. If PHI is required from another EHRi the identity protection service would do a lookup for any FIDs relating to the patient's/person's ECID.
4. The EHRi does a lookup to determine if the patient/person already has a FID that is stored in other EHRis. If such an FID exists, the ECID retrieved or created in step 2 would be associated with this FID.
5. If no FID is located in steps 4 or 5 an FID is created following which a lookup for other ECIDs relating to the patient/person is initiated and stores the new FID with the ECID in each jurisdiction where the patient/person has PHI stored.
6. The FID sent to other applicable jurisdictions in order to retrieve PHI.
7. The identity protection service matches the FID to the corresponding ECID that is then used to retrieve the patient's/person's PHI, which is returned with the corresponding FID. EHRis would not return their ECIDs to the EHRi requesting PHI.
8. PHI retrieved in steps 3 and 8 (if applicable) are returned to the requesting EHRi user.

7.7.10 Requisites

- The Identity protection services has mappings for all patient/person IDs on EHR data and domain repositories

- IPS may also be extended to the client registry and other repositories
- In order for PHI to be accessible where the identity protection service is deployed, access to PHI must be through the EHRi common services.

7.7.11 Service Components

Privacy protection has two service components:

- A.5.1 Resolve ECID and FID for patients/persons
- A.5.2 Manage ECIDs and FIDs for patients/persons
- A.5.3 Pseudonymise Data

These components are further described in Appendix A.

7.8 Anonymisation in the Desired Future State

7.8.1 Overview

An anonymisation service takes PHI (i.e., data that includes fields which name or unambiguously describing an identifiable individual), removes all personal identifiers, and then either aggregates it or performs other statistical transforms.

Whereas pseudonymisation provides data on specific (pseudonymously identified) patients/persons (e.g., data field 1 for patient X, data field 1 for patient Y, data field 1 for patient Z, …), the anonymisation service will always provide data derived from multiple patients/persons (e.g.: mean and standard deviation of data field 1 across a sample size of 26 patients aged 45 to 50). Anonymisation is a complex process that is difficult to perform on PHI in a secure and privacy protective manner. The following issues must be carefully considered to ensure that anonymisation services operate securely and effectively:

- the mechanisms for processing PHI data fields to achieve anonymisation. This included both the deletion of nominative fields as well as the processing of fields such as birth date or postal code to replace the content of such fields by mapping field content to a narrow range of values such as broad age categories (in the case of birth date) or broad geographic areas where many individuals live (in the case of postal codes.
- assessment of the risk of identification through inference[77];
- techniques and methodologies for mitigating risk of re-identification in small samples
- trusted third party involvement in anonymisation;
- controlled re-identification practices where policy permits (or legislation requires) such practices.

[77] Such an assessment is usually done by calculating the so-called cell size of each record in the resulting anonymised or pseudonymised data set.

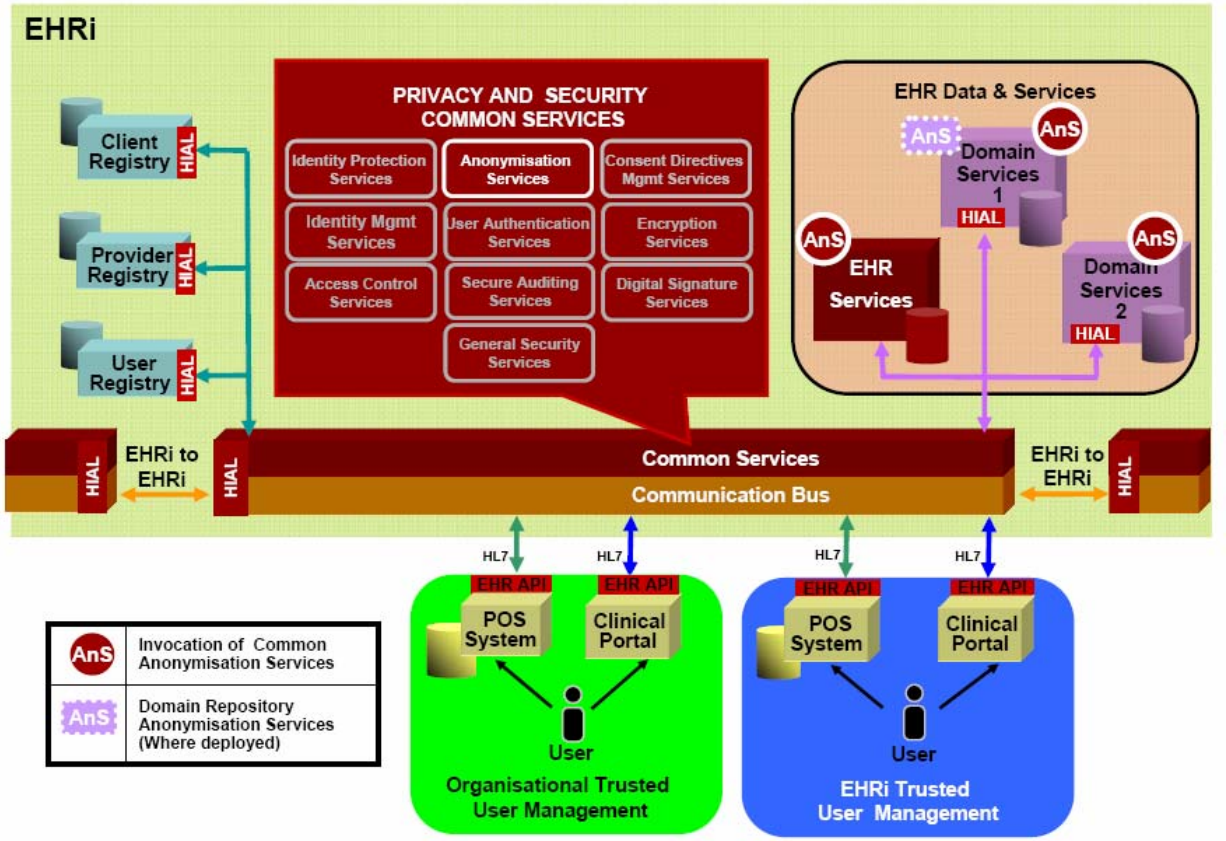

Figure 16: Anonymisation in the Desired Future State

7.8.2 Rationale

It is a fundamental privacy principle that personal information be anonymised to the greatest extent possible to serve the purpose for which it will be used or disclosed (i.e. identifiable information should not be used when anonymous information will serve the purpose). Both anonymisation and pseudonymisation (see section 7.7.6 above) are used to enhance patient/person privacy for the purpose of secondary uses and disclosures of PHI, such as clinical data, in public health monitoring and assessment, in confidential patient-safety reporting, and for comparative quality indicator reporting.

7.8.3 Availability Requirements

The anonymisation service has low availability requirements, as it is used strictly for research and administration. Hence, service requests can be delayed for days if necessary (though this of course would be undesirable).

7.8.4 Policy Enforcement

The need for an anonymisation service is applicable to all data stored in the EHRi. Therefore, from a policy compliance/enforcement perspective the service should be centrally available and accessed via the EHRi common services.

The rules for what constitutes anonymous versus identifiable PHI is a matter of jurisdictional policy.

7.8.5 Process Flow

The process flow for the anonymisation service will vary depending on jurisdictional implementations of the EHRi and how jurisdictions decide to provide access to the EHRi for the purpose of research.

The Process flow for the anonymisation service is as follows:

1. An authorised EHRi user (e.g., a researcher conducting healthcare related research that has been approved by an Ethics Review Board or a healthcare administrator obtaining statistical data for approved studies in healthcare utilisation) requests anonymised PHI from a set of EHRs that meet certain search criteria.
2. The EHRi searches for and obtains a set of applicable records.
3. The anonymisation service removes all identifying information from the record set.
4. The anonymisation service aggregates the data, ensuring that each resulting aggregate meets minimum requirements for cell size[78].
5. The aggregated data is returned to the user.

7.8.6 Requisites

- Anonymisation service will be access via the common services provided by the EHRi.
- This service will be used by and shared by several domains
- IPS may also be extended to CR and other repositories
- User is authenticated/validated and authorised to perform requested function

7.8.7 Service Components

Anonymisation has one service components:

- A.6.1 Anonymise Data

This service component is described further in Appendix A.

7.9 Encryption Service in the Desired Future State

7.9.1 Overview

Only properly applied cryptography can rigorously protect the confidentiality of data both in transit and in storage. Basic safeguards required by PHI protection legislation in multiple jurisdictions[79] encourage the

[78] Such minimum requirements may depend in part on the statistical techniques employed, but a typical minimum cell size is five aggregated entities.

[79] Examples include the following:
Alberta's Health Information Act (R.S.A. 2000, c. H-5, s. 60) states that custodians must take reasonable steps to protect against any reasonably anticipated threat or hazard to security or integrity or loss of the health information, or unauthorised use, disclosure, modification or access.
Ontario's Personal Health Information Protection Act (S.O. 2004, c. 3, s. 12) states: "A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorised use or disclosure and to ensure that the records containing the information are protected against unauthorised copying, modification or disposal".
Saskatchewan's Health Information Protection Act, (c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 16) states that custodians must establish policies and

application of encryption technology. To be effective, encryption must be based upon openly available industry standard encryption algorithms: proprietary algorithms that are not broadly accessible by the cryptographic community are unacceptable and in any event, proprietary schemes frustrate interoperability. The selection of specific encryption algorithms and key lengths that the EHRi will support are beyond the scope of conceptual architecture[80].There is accepted Canadian and international standards on the use of encryption in healthcare and they should be followed.

Strong cryptographic algorithms and lengthy keys are useless if the storage of those keys is protected by weak encryption and/or password systems that are amenable to a dictionary attack. Protection of keys is therefore a prime concern in any architecture employing encryption.

Healthcare can be a highly mobile endeavour; to the extent that they are used, public/private encryption key pairs must be capable of being easily transferred by their owner from one computer or personal computing device to another.

The encryption service described below provides for the protection of PHI in transit (message encryption), in active use (database encryption), and in long-term archival storage (data storage encryption)[81].

---

procedures to maintain administrative, technical, and physical safeguards.
Manitoba's *Personal Health Information Regulation*, (Man. Reg. 245/97, s. 2) requires trustees must establish and comply with written policies and procedures to ensure the security of personal health information, including provisions for the recording of security breaches

[80] As a practical matter, the minimum acceptable key length for any symmetric encryption algorithm is 128 bits and the minimum acceptable key length for any public key encryption algorithm other than elliptic curve crypto-algorithms is 2048 bits (elliptic curve encryption algorithms, if adopted in the future, could have a minimum acceptable key length of as few as 512 bits). Only a Threat and Risk Assessment can adequately determine a minimum adequate key length for a given use and context.

[81] Stored data can be encrypted at the application layer, at the storage layer, or at the database layer:

- Application-layer encryption allows enterprises to selectively encrypt granular data within application logic. This can provide a strong security framework if designed correctly to leverage standard cryptographic application program interfaces (APIs). If deployed correctly, application-layer encryption can protect data against storage attacks, theft of storage media, application layer compromises, and database attacks. But application-layer encryption is difficult to deploy and very difficult to deploy correctly: off-the shelf applications cannot be retro-fitted with cryptographic API procedure calls; encryption can "break" stored procedures within a database that encapsulate business logic; data values and field sizes change when data is encrypted; there is no inherent ability to enforce consistent security policies across the enterprise; and application-layer encryption still leaves the problem of how to protect encryption keys.
- Data storage encryption encrypts data when it enters (and decrypt it when it leaves) the storage subsystem, either at the file layer or at the sector (or data block) level. This type of encryption is well suited for encrypting files, storage blocks, and tape media. Unlike application-layer security, data storage encryption can separate (at least to some extent) security policy from data management, but it also has serious limitations. Most importantly, it only protects against a narrow range of threats, namely media theft and storage system attacks. Current data storage techniques only provide block-level encryption; they do not provide the ability to encrypt data at the field level. These limitations stem from the fact that the encryption devices do not know what they are encrypting; i.e., they treat the data to be encrypted as an undifferentiated block. Consequently, access to the encrypted file is all or nothing, since one can encrypt an entire database with data storage encryption (so-called *whole database encryption*), but not specific records or fields housed within the database. Whole database encryption is limited to ensuring that a stolen copy of the database cannot be browsed to obtain information (such browsing of

Figure 17 below shows where the EHRi encryption services are applied:

1. protecting data in transit:
    - in HL7v3 message traffic from POS systems and clinical portal to the EHRi: HL7v3 messages will be encoded in XML. While acknowledging that detailed studies of intensive use are not yet available, the P&S conceptual architecture currently recommends the use of XMLEnc to encrypt all HL7v3 message traffic from POS systems to the EHRi or from web browsers accessing clinical portals to the portal.
    - in messages across the EHRi communication bus (e.g.: to or from a domain repository or registry),
    - in message traffic from one EHRi to another (say, across a jurisdictional boundary);
2. protecting data in active storage:
    - within domain repository databases (domain repositories may have their own encryption services, shown on the diagram as a mauve rectangle);
    - within the EHRi data repository;
    - within registries,
    - where applicable, within POS systems (POS systems may have their own encryption systems for data storage, although this is currently uncommon);
3. protecting data at rest:
    - within EHRi backups,
    - within EHRi data archives,
    - within POS system backups (POS systems may have their own encryption systems for data backups or may rely on operating system file encryption capabilities or the encryption capabilities of dedicated data backup software).

---

unencrypted databases from popular systems such as Microsoft SQL Server, Oracle, or Sybase can be easily done with a simple text editor).

- Database encryption encrypts data as it is written to (and decrypts data as it is read from) a database. By doing so, database encryption protects data while it is in use by the database system, as well as while it is in storage. Ideally it is deployed at the column level within a database table (and hence is sometimes referred to as co*lumn encryption)* to encrypt individual columns in a data table so that they can only be seen by authorised users or user groups. This allows columns (fields) of data to be restricted to only those users with selected roles; this procedure therefore links column encryption directly to role based access control. When coupled with database security and access controls, database encryption provides a secure means of preventing unauthorised access to PHI. Database encryption protects the data both within the database management system and also within the storage media.

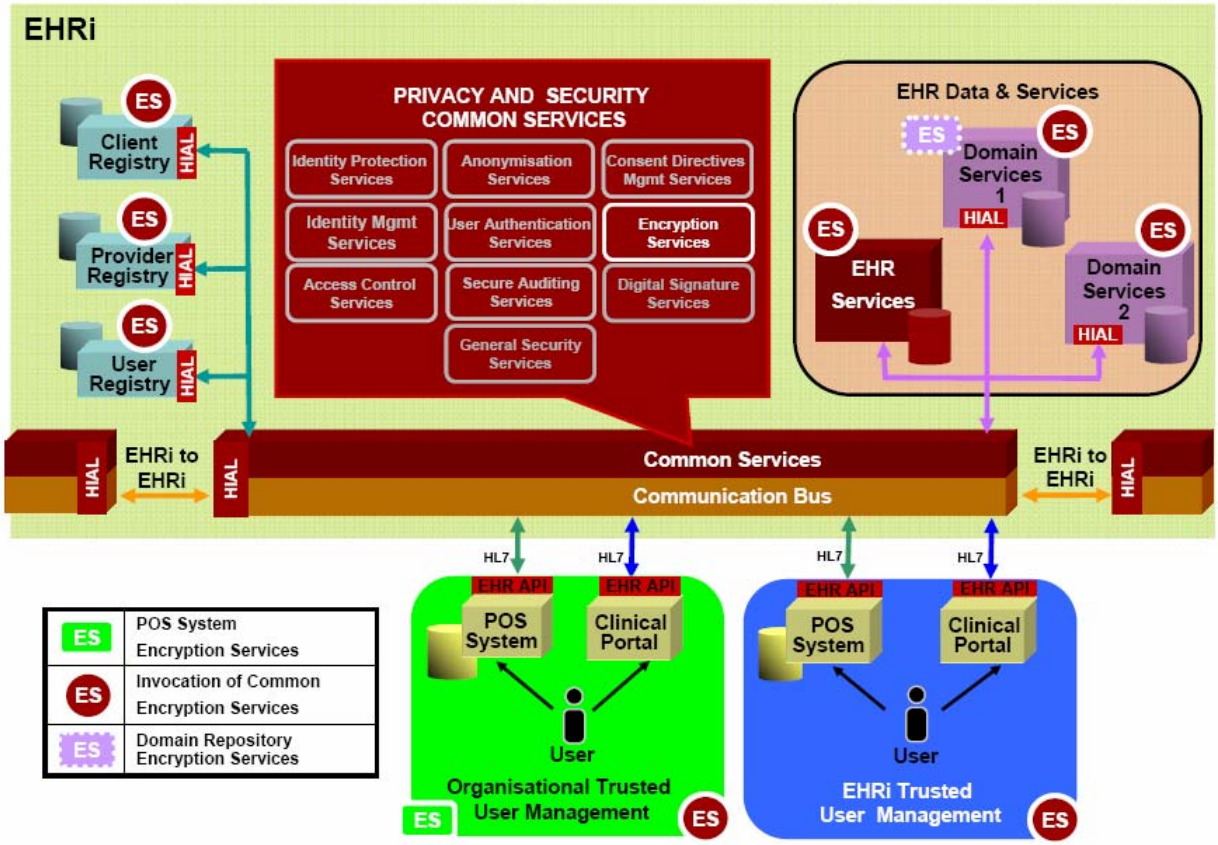

Figure 17: Encryption Services in the Desired Future State

7.9.2 Rationale:

Use of message encryption is now a common and accepted way of ensuring that the confidentiality and integrity[82] of messages is preserved. Encryption of PHI while in transit across networks ensures that it is not susceptible to eavesdropping or tampering and all major health information networks in Canada (SHIN[83], RTSS[84], BC Healthnet, Smart Systems for Health, etc.) provide for encrypted transmission of PHI and a secure EHRi must do so as well.

While encryption protocols at the network layer can be used for the maintenance of message security, there are also reasons not to rely solely on network layer encryption. For one, the increasing use of wireless and mobile computing in healthcare may leave serious security gaps if network security only protects information during transmission from server to server. For another, it is difficult to ensure that message traffic remains encrypted end-to-end in an environment where little control can be effectively wielded over POS systems and their deployments unless encryption occurs at the application layer.

[82] Most encryption schemes currently used to encrypt messages also ensure that the contents of the message cannot be altered in transit; although encryption alone does not prevent messages from being deleted or diverted by a malicious third party prior to their arrival at their final intended destination.
[83] Saskatchewan Health Information Network (SHIN). SHIN now exists as an agency of the Health Information Solutions Centre at Saskatchewan Health.
[84] Réseau de Transport Sociaux Sanitaire, Québec.

Message Integrity can also be guaranteed by encryption insofar as encrypted messages cannot be altered (although they can be deleted and hence message integrity must be considered distinctly from guarantee of message delivery).

Currently, database encryption technology is less commonly used in healthcare to protect PHI (in large measure because of the cost of the software and the high performance hardware needed to support it), although the effect of health information protection legislation in the US[85] has recently caused an increase in the number of installations of database encryption to protect EHR data. Database encryption will undoubtedly become more commonplace in healthcare as prices of both the hardware and the software needed to implement it continue to decrease and the cost of providing adequate physical security for data stores continues to increase.

Data storage encryption is most commonly seen in data backup and archiving systems. The use of data storage encryption to protect PHI is increasing in response to the ever more widespread use of mobile devices containing stored repositories of PHI. The very long lifetime of archived PHI necessitates careful management and implementation of data storage encryption in archived media. An effective strategy for storage-level encryption of PHI is essential if its benefits are to accrue to implementations of the EHRi.

7.9.3 Approaches to the Encryption of Messages

As mentioned above, the EHRi is founded on a messaging and services oriented architecture.

Multiple deployment models are possible:

- **Message Encryption Deployment Model 1: encrypt the XML message with XMLEnc**
  HL7 Inc. (and its Canadian affiliate, HL7 Canada) recommends XML as the preferred message encoding scheme for all HL7 version 3 messages. Encoding of HL7 messages with XML therefore permits the use of the XMLEnc standard to provide robust message encryption at the application layer.[86]

  Use of XMLEnc has several advantages:

  - it has all the advantages of application layer security in providing end-to-end security;
  - it is a W3C standard and its uptake by vendors is increasing rapidly;
  - it cleanly interacts with other W3C XML standards such as SOAP, SAML, and XMLDSig.

  The primary disadvantage of XMLEnc is that, like HL7v3 itself, it is not yet in widespread use. The user of XMLEnc in the desired future state depends therefore on whether it has a promising future. An assessment of that future is still somewhat a matter for conjecture. The situation for XMLEnc is not dissimilar to the situation for HL7v3 itself: it shows great promise but little intensive use by currently implemented and operational systems. Of all the recommendations in this document, the use of XMLEnc to encode HL7 needs to be revisited in the near future, as more information on practical implementations becomes available.

- **Message Encryption Deployment Model 2: encrypt the XML message with a "bespoke" encryption wrapper**
  Each XML message is a file and like any file, can be encrypted at the application layer in a variety ways; for example, by using the PKCS suite of standards.

[85] The US Health Insurance Portability and Accountability Act (HIPAA) contains provisions for the protection of data stored electronically. This American legislation is vague on specifics, however, and regulations under HIPAA do not mandate specific cryptographic technologies. As database encryption is one of the technologies that meets all of HIPAA's requirements for secure storage, it has garnered considerable interest within American healthcare organisations within the last two years.

[86] Application layer refers to level 7 in the 7 layered OSI model for network interconnection (see References section at the end of this document). The application layer supports application and end-user processes and everything at this layer is application-specific.

In additional to having the advantages of application layer security, alternative approaches to encrypting XML have the primary advantage that some of these approaches to file encryption are "tried and true".

The primary disadvantage of this approach is that it can considerably complicate the handling of HL7v3 by middleware, which will then have to have the encryption applied or removed from the message by other software processes.

- **Message encryption deployment model 3: encrypt the XML message at the transport layer** TLS (the successor of SSL) is an obvious example of transport layer encryption of text. There are many other approaches, including the use of VPN connections between POS systems and the EHRi

  TLS has the advantage that it is easily implemented for access to clinical portals by web browsers. It has the disadvantage that its use by POS systems in a message based environment would be problematic. VPNs by contrast could be used in a POS environment, but would be exasperating for users to deal with when accessing clinical portals with a browser.

  Any use of transport layer technologies (or indeed any layer other than the application layer) has some significant disadvantages. Only application layer encryption can protect messages from end-to-end; i.e., from originator (e.g.: a provider's desktop running a POS system client or a web browser connected to a clinical portal) to the server handling the request. As the message system envisioned by Infoway for connections to the EHRi is store-and-forward in nature (even if the storage period is very brief[87]), application layer encryption is the only way that the confidentiality of PHI can be relentlessly maintained. To ensure a secure and privacy enhanced EHRi, message level encryption[88] would be considered a best practice at the very least, if not an absolute requirement.

Infoway currently recommends encryption deployment model 1 (use of XMLEnc as the means by which message encryption takes place).

7.9.4 The Role of VPN Technology

VPN technology would most likely be used to authenticate connectivity end points and ensure confidentiality of message traffic between server systems within the EHRi. Examples include:

- PHI exchanges between EHRi within or across jurisdictions and where determined to be required between domain repositories, registries and EHRi common services.
- VPN technology would not be relied upon to play a role in authenticating and determining authorisation of EHRi service requests between POS systems and the EHRi.

Instantiations of the EHRi common services and its common services do not yet exist. Infoway recognises that VPN technology is currently used to secure message traffic and ensure (to some level) the confidentiality of PHI while in transit between POS systems and domain repositories or registry services. As a practical matter, transport layer security mechanisms such as VPN technology will co-exist with the progressive deployment of application level encryption as a services based architecture is deployed with the initial EHRi common services instantiations. In this interim state, VPN technology may be used, despite this technology failing to provide the same level of end-to-end protection that can be provided by XMLEnc.

[87] Brevity is a relative term and even very brief storage in a message queue still opens an avenue of attack for hackers if the queued messages are in clear text. The avenue becomes broad indeed if a breakdown in processing causes messages to back up in the queue.

[88] By message level encryption, we mean the use of cryptography at the application layer in order to ensure confidentiality and integrity of the message from the originator to the destination system in such a way as to ensure that the destination system can be assured that the originator of the message is authenticated and authorized, and that the message content cannot have been altered in transit.

7.9.5 Availability Requirements

The Encryption Service must remain continuously operational (i.e., with no scheduled downtime and robust resistance to equipment outage or denial of service attack), as without it, message traffic between the EHRi and POS systems or clinical portals cannot be encrypted or decrypted. As all such traffic will be encrypted, the Encryption Service must be available or the EHRi itself will essentially be offline. The availability requirements for encryption must therefore be at least a high as the availability requirements for any other EHRi common service.

7.9.6 Policy Enforcement

Policy enforcement is greatly simplified in that the EHRi common services will only accept message traffic that has been encrypted. Policy enforcement would happen at the EHRi common services level of the EHRi.

7.9.7 Process Flow

The process for encryption is as follows:

1. User requests, via a POS system or clinical portal, PHI from the EHRi
2. The POS encrypts the access request message to the EHRi or the user communicates the access request via a web browser to the clinical portal within an encrypted transport layer secured session and the portal server constructs and then encrypts the access request message to the EHRi.
3. The EHRi decrypts the message
4. The EHRi creates (where necessary) appropriate messages to other systems (e.g. domain repositories) and encrypts each of them
5. Each of the systems decrypts the message, interprets and fulfills the request.
6. The systems return the requested data to the EHRi in encrypted form.
7. The EHRi decrypts the returned information and consolidates it for the user.
8. The EHRi encrypts the consolidated data and transmits the data to the POS system or clinical repository
9. The POS system or clinical repository decrypts the received message and formats it for display to the user.

7.9.8 Requisites

- The POS and EHRI share the requisite encryption keys (public, private or symmetric) to exchange encrypted message traffic.

7.9.9 Service Components

The following encryption service components are described in Appendix A:

- A.7.1 Key Management
- A.7.2 Database Encryption
- A.7.3 Data Storage Encryption

7.10 Digital Signatures in the Desired Future State

7.10.1 Overview

Digital signatures will very likely be a requirement for any system that electronically delivers prescriptions from prescribers to pharmacists electronically (i.e., that replaces paper-based prescriptions with electronic documents or message-based transactions).[89] To the extent that an implementation of the EHRi supports such a capability, it must also support digital signatures for prescribers.

While e-prescribing is therefore an obvious use of digital signatures, they have other potential uses in healthcare. There are many other less common situations where the signature of a physician is required upon an e-form. Some jurisdictions require that an authorised healthcare provider sign each lab test requisitions. Some forms (example for reportable diseases) must also be signed by providers. Death certificates also require signature. Certain internal processes also benefit from the use of digital signatures (e.g. signing security asserts by means of approaches such as SAML). Finally, secure timestamps and digital notary services also require the use of digital signatures. Whatever their use, digital signatures also provide a powerful data integrity mechanism as digitally signed data cannot be tampered with or altered without invalidating the signature.

Like encryption, digital signatures must be based upon openly available and industry standard encryption algorithms. As with encryption, the minimum acceptable key length for any public key digital signature algorithm cannot be less than 2048 bits (except for elliptic curve digital signature algorithms, which if adopted in the future could have a minimum acceptable key length of as few as 512 bits).

Like encryption keys, digital signature keys must be rigorously protected. Key protection (both within the EHRi common services and within the possession of users who are potential signatories) is therefore a prime concern in any architecture employing digital signatures. This in turn leads to potential issues of interoperability among digital signature software implementations, unless a standard for private key protection is adopted.

Digital signature keys must be capable of being easily transferred by their owner from one computer to another.

A digital signature is a technical mechanism that allows a health care professional to sign a digital document (e-mail, electronic health record, etc.) in much the same way that they would apply a signature to paper, with the assurance that that the signature cannot be forged and neither the document nor the signature can be altered without rendering the signature obviously invalid. The legal force of the digital signature depends on the jurisdiction and (in part) on the type of document signed. To the extent that the EHRi allows the digital delivery of e-prescriptions from prescribing healthcare providers (e.g., physicians) to dispensing healthcare provider (e.g., pharmacists) there will be a need for

---

[89] 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*
>
> *if the prescription is given verbally, the pharmacist has taken reasonable precaution to satisfy himself that the person giving the prescription is a practitioner.*

By contrast, Title 21 Code of US Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures mandates that the US Food and Drug Administration (FDA) establish the criteria under which electronic records and electronic signatures are considered as equivalent to paper records and handwritten signatures executed on paper.

the EHRi to support digital signatures.[90] This in turn will require, on a technical level, the recognition of valid Certification Authorities and the capacity to check for certificate revocation. It will also require consistent policies and procedures for issuing digital certificates that meet the high standards of digital certificate issuance demanded of e-prescribing. Issuing digital certificates to e-prescribers and other EHRi users is a non-trivial undertaking. It involves five essential steps:

1. Register participating health care professionals (after verifying their identities) and assign each a so-called distinguished name that will link their identity to their digital signature.
2. Ensure that each prospective certificate holder signs an agreement explaining in plain language the responsibilities of certificate holders to ensure that their digital signature capabilities are not abused.
3. Enable each registered Certificate Holder to generate a digital signature key pair.
4. Ensure that any private digital signature keys generated remain protected so that only the certificate holder can use them.
5. Publish each Certificate Holder's distinguished name and/or other identification and its matching signature verification key in a document called a "digital certificate." This document is rendered forgery-proof by being signed with the digital signature of a "Certification Authority" entrusted with certifying such electronic documents. The certification process must also allow certificates to be revoked if this becomes necessary (for example, if a certificate was fraudulently obtained). To this end, a list of revoked certificates is also published and signed by the Certification Authority.

Digital signature certificates can be issued to health professionals, administrators, support staff, and (under limited circumstances) to communicating devices such as servers. Before digital signature certificates can be issued to individuals to be used for health care purposes such as signing prescriptions, a clear policy is needed on how individuals will be identified prior to receiving digital signature certificates[91]. Detailed procedures are also essential to minimise the risks and the inconvenience associated with issuing, renewing, or revoking digital signature certificates. The following policies and procedures are therefore needed to operationalise digital signature services:

a) a certificate policy for the secure issuance, renewal and revocation of digital signature certificates that answers a variety of questions, such as what limitations of liability will exist[92];

b) a certificate profile detailing precisely what the digital signature certificates are to contain (e.g.: is the name of the certificate holder to be included? an email addresses for the certificate holder? information on the certificate holder's healthcare role(s)?);

c) a registration policy specifying under what circumstances a digital signature certificate is to be issued and to whom[93];

---

[90] Digital delivery in this context means the use of the EHR as apposed to the use of fax machines or the printing of printing of prescriptions entered electronically.

[91] The identity of individuals must be securely verified before they receive digital signature certificates. Establishing and registering an individual's identity for the purposes of signing confidential health care information is a very different process from registering health professionals for other purposes such as billing or administration, as the risks involved are different. For example, if an individual is incorrectly identified when added to a payroll database, the worst that may happen is that they will receive payments to which they are not entitled—the risks are therefore easily quantified in dollars and cents. If an individual is incorrectly identified when issued a digital certificate for the purpose of signing personal health information such as prescriptions, the risks are difficult to quantify.

[92] A comprehensive guide to the appropriate structure and scope of a certificate policy can be found in IETF/RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

d) a certificate holder agreement (to be signed by the recipient of a digital signature certificate) explaining in plain language the responsibilities of certificate holders to ensure that their signature(s) are not abused.

Putting these policies and procedures into operation in turn requires digital signature services to accomplish the following tasks:

a) secure digital signature key creation and digital signature certificate issuance,

b) digital signature key renewal, and

c) secure certificate revocation.

The three services listed above are typically performed by a Certification Authority (CA) as illustrated in Figure 18 below.

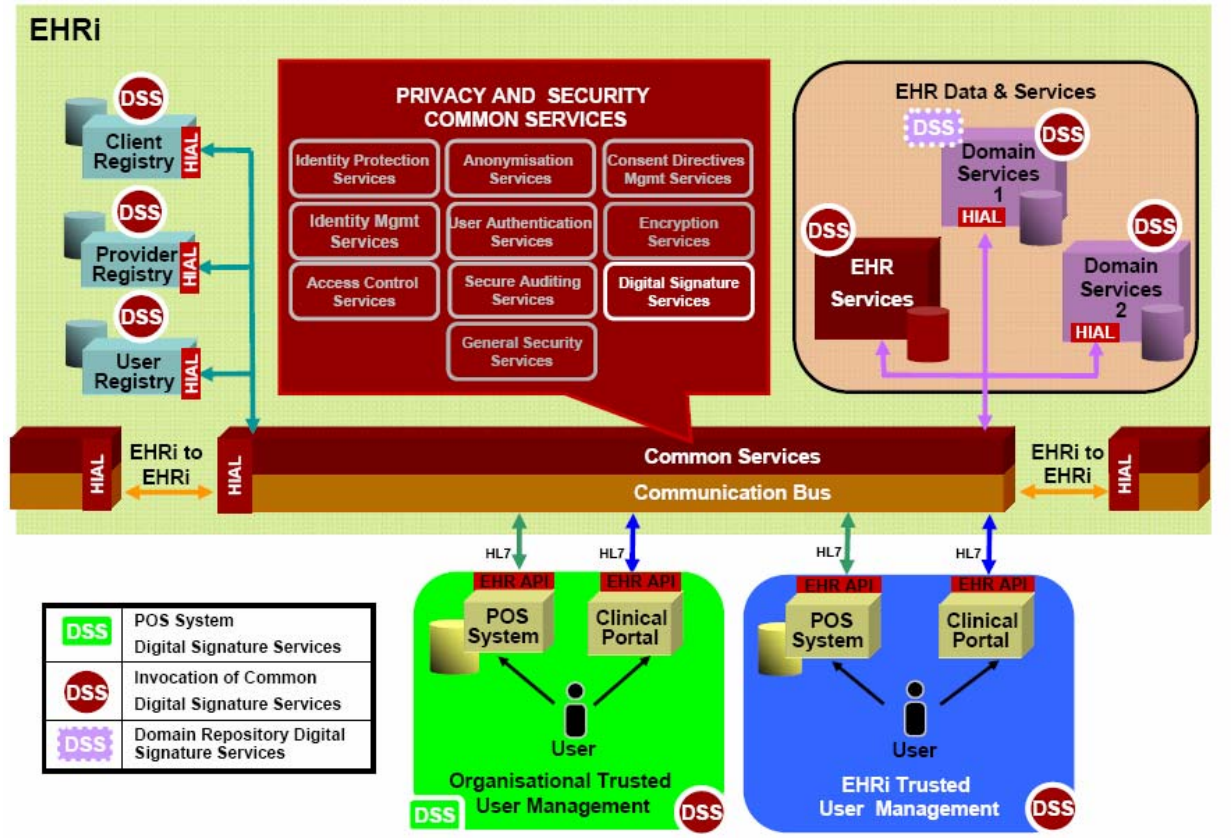

Figure 18: Digital Signature in the Desired Future State

[93] A registration policy for digital signature certificates describes how the administrative aspects of identification and registration of potential certificate holders can be delegated to a competent Registration Authority (RA). The RA oversees all aspects of registration services and operations within its domain. The RA can be an individual (acting as a registrar) or in very large implementations with intent to register many and various types of certificate holder, the RA can be a small committee providing oversight.

7.10.2 Rationale

As mentioned above, digital signatures are required if any of the following paper-based documents are to be replaced by entirely digital alternatives:

1. e-prescribing;
2. physician signatures on forms:
    a) lab test requisitions (to the extent that some jurisdictions require that an authorised healthcare provider sign each requisition),
    b) reporting of reportable diseases
    c) death certificates

Certain internal processes also benefit from the use of digital signatures (e.g. signing security asserts by means of approaches such as SAML).

Providing the EHRi with a digital signature capability will also have a significant impact on the design of the infostructure's privacy and security related functions and will enable the implementation of security features such as time stamping, notarisation, strong guarantees of data integrity, and non-repudiation (i.e., the greatly diminished ability of a signatory to later disavow data to which the signatory's digital signature has been affixed).

7.10.3 Availability Requirements

Digital signature certificate creation is a low availability function, as in many case, the generation of new digital certificates for users can be delays for days if necessary. Digital signature revocation checking is a moderately high availability service that should not be unavailable for more than approximately four hours. Digital signature generation (i.e., the application of a signature to an e-document) is done locally by the user and so places no availability requirements on the EHRi. Re-signing by a digital notary for the purposes of archiving has very low availability requirements, as this function can be delayed for significant periods of time.

7.10.4 Policy Enforcement

There are elements of policy enforcement of the digital signature service within the POS Services and domain repositories, but the main logic will exist within the EHRi common services.

7.10.5 Process Flow

The process flow for **obtaining** a digital signature certificate is as follows:

1. A registered user requests a certificate.
2. The certificate issuer (conceptually a Certification Authority, but implementation details may vary) confirms the identity of the applicant.
3. The requesting user's software or agent generates a digital signature key pair and securely communicates the signature verification key to the certificate issuer.
4. The certificate issuer generates and signs a digital certificate for the requester that contains the requester's signature verification key to a unique identifier for the requester.
5. The certificate issuer conveys the digital signature certificate to the requester.

None of the steps above need involve the EHRi, as a certificate issuer may be (will be?) a third party service provider.

The process flow for **applying** a digital signature is as follows:

1. The user, via a POS system, assembles an electronic document (such as an e-prescription or an HL7 message) for signature.

2. The POS system makes calls to a local cryptographic application program interface (crypto-API) to sign the e-document in a way that complies with the (yet unstated) EHRi standards for digital signatures.
3. The EHRi receives and where appropriate, stores the signed e-document or message.

The EHRi is not actively involved in the process of applying the digital signature, other than to store it where necessary, when it is attached to data to be stored in an EHR repository.

The process flow for **confirming** a digital signature is as follows:

1. The user invokes cryptographic software examines a signed e-document and confirms that the digital signature has not been tampered with (i.e., that a message authentication code computed from the current content of the document matches the one "decrypted" by the signature verification key contained in a digital certificate).
2. The user confirms that the digital certificate is still valid by invoking cryptographic software that either checks a certificate revocation list or that relies on an online certificate status checking protocol to ensure that the certificate has not been revoked by the certificate issuer.

The EHRi need not be involved in the provision of certificate status checking, as this may be performed by a third party certificate issuer.

The process flow for long-term **archiving** of a digitally signed e-document is as follows:

1. A Threat and Risk Assessment is periodically done to assess the robustness of extant digital signatures (e.g.: digital signatures applied using a certain algorithm with keys of a certain length and that were applied more than five years old) and recommendations are made on risk mitigation via re-signing by a digital notary to protect the original signature.
2. E-documents in storage are periodically reviewed (annually, say) to identify those digital signatures at risk.
3. E-documents in storage whose signatures are at risk are re-signed and time stamped by a digital notary.

Archiving is a process that will involve the EHRi in the application of digital signatures, either directly as a signatory, or as a requestor of signing services from a third party digital notary.

7.10.6 Requisites

- There is a certificate issuer capable of confirming the identities of prospective certificate holders, ensuring that these prospective users are bound by certain rules for the protection of their signing keys, and then generating certificates for those users and ensuring that these users.
- The certificate issuer maintains the status of each certificate; specifically, whether or not it has been revoked.
- Each certificate holder must have (or have access to) trusted software that can act as a cryptographic agent to generate and apply a digital on the user's behalf.

7.10.7 Service Components

The following digital signature service components are described in Appendix A:

- A.8.1 Digital Signature Certificate Management
- A.8.2 Digitally sign data
- A.8.3 Verify digital signature
- A.8.4 Digital Time Stamp and Digital Notary Service

7.11 Secure Auditing in the Desired Future State

7.11.1 Overview

The ability to audit transactions and events taking place within the EHRi is fundamental to meeting the P&S requirements. The ability to report on the system(s), user(s), provider(s), patients/persons, and health data involved in each EHRi transaction serves a fundamental privacy principle. It is also critical to meet other operational needs such as system administration and transaction monitoring. A service auditing service records significant privacy and security related events. The service renders the record tamper-proof.

A secure audit service is the basic EHR system component responsible for creating and managing details of system and application events. Audit records should contain the necessary information to answer the following questions:

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

The secure audit log service will create a secure audit record each time a user:

a) accesses, creates or updates PHI of a patient/person via the EHRi[94];

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.

The secure audit log service will also keep a log of message transmissions involving PHI (the log need only contain the time, origin and destination of the message, not its content.);

Logging of persistent failed attempts at authentication is a key components of intrusion detection and an essential feature of systems that robustly defend their user authentication protocols.

The desired future state of the secure auditing service is illustrated in Figure 19 below.

[94] See section 7.11 for a discussion of P&S secure audit services. See also Appendix 1 for a discussion of the privacy and security requirements related to auditing.

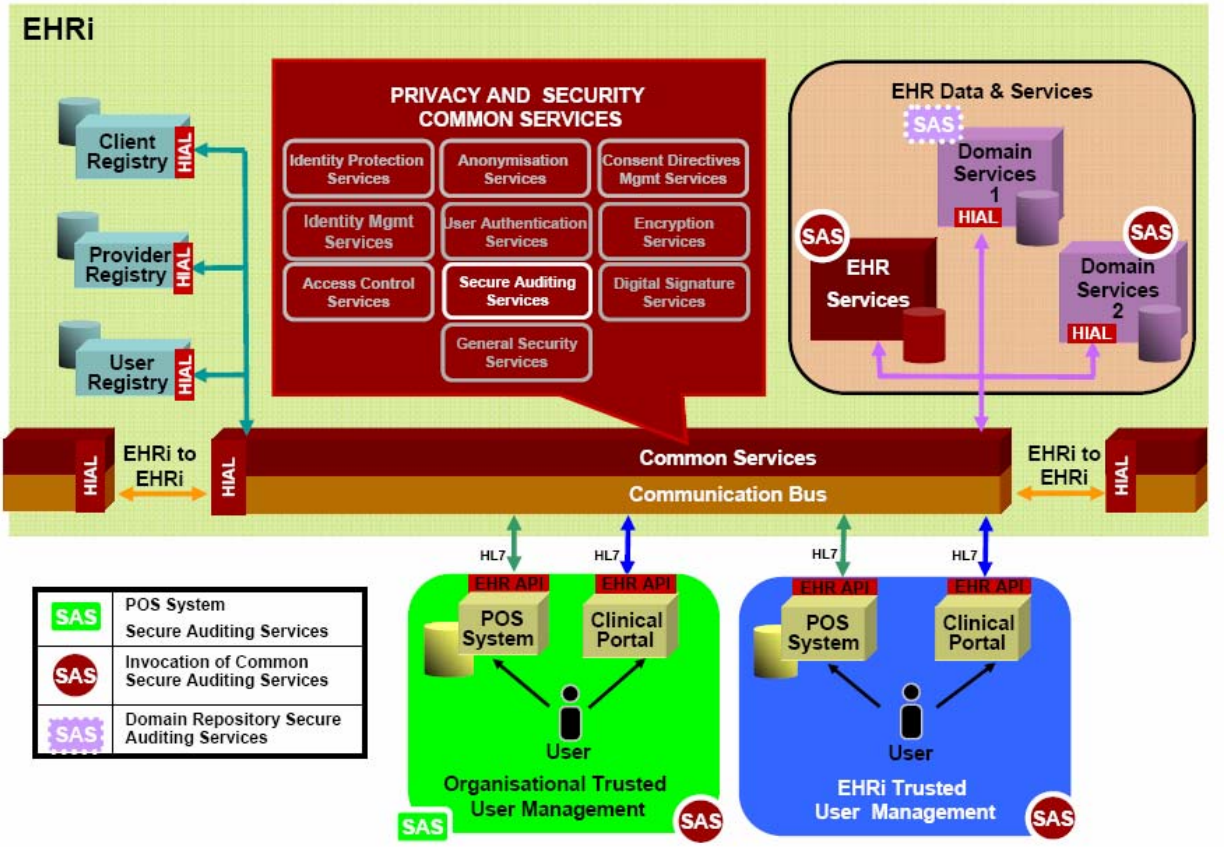

Figure 19: Secure Auditing Service in the Desired Future State

7.11.2 Rationale:

Some Canadian health privacy legislation requires healthcare providers to maintain records of successful or unsuccessful attempts to gain access to records, and attempts to add to, delete or modify the information,[95] including the time when the information was accessed and by whom.[96]

7.11.3 Availability Requirements

The auditing service must be continuously available, as otherwise an essential component in privacy protection will be missing – perhaps when it is needed most. The availability requirements for this service are therefore as high as the availability requirements for EHR data.

7.11.4 Policy Enforcement

The process flow for secure auditing will follow in a later version of the P&S architecture.

7.11.5 Process Flow

The Process

1. User requests EHRi to provide access history for a patient/person

[95] Manitoba, *Personal Health Information Act, 1997*.
[96] Ontario, *Medicine Act 1991*

2. The EHRi obtains the ECID for the patient/person and uses it as a parameter to access the audit logs
3. The audit log service will use the IPS to get a protected identity for the patient/person and then uses it to get the requested data.

7.11.6 Requisites

- The audit log is secured against unauthorised access and data may be encrypted as required (not shown encrypted in this diagram)
- User is authenticated/validated and authorised to perform requested function

7.11.7 Service Components

Appendix A described the following secure audit service components:

- A.9.1 Securely Log Events

1. A.9.2 Analyse logs and detect intrusions.

7.12 General Security Services

7.12.1 Network Security

Network security is ultimately a jurisdictional responsibility. Provincial and territorial health information networks vary widely in their capabilities and extent: some provinces do not have dedicated health information networks; some have networks that are fully operational but currently underutilised; others have networks which many of the province's health care providers actively make use of on an ongoing basis. The network architectures also vary widely: one jurisdiction's network makes exclusive use of dedicated network points of presence; another jurisdiction makes use (in part) of public carriers and the Internet. Some jurisdictions include within their network perimeters fully secured data servers in their own secured data centres. Others rely on servers located in hospitals and other institutions to provide the bulk of the data storage and processing capability of the network. Little in the way of overarching commonalities emerges from this picture. For this reason alone, the P&S conceptual architecture for the EHRi cannot rely in any consistent way on security at the network layer.

There are other reasons not to rely on network protocols for the maintenance of message security. For one, the increasing use of wireless and mobile computing in healthcare may leave serious security gaps if network security only protects information during transmission from server to server. For another, it is difficult to ensure that message traffic remains encrypted end-to-end in an environment where little control can be effectively wielded over POS systems and their deployments unless encryption occurs at the application layer.

For all the reasons stated above, the P&S architecture does *not* depend upon network security services or protocols to maintain the confidentiality or integrity of PHI traversing any network to which the EHRi is connected. Specifically, the P&S services are designed to be network architecture independent; i.e. they do not depend for their application security on decisions made at the network layer (i.e., at layer 3 or lower in the seven layer Open Systems Interconnection network protocol model[97]). Therefore, network security will not be further discussed in this document.

7.12.2 Availability Services

Many facilities must be brought to bear on the problem of maintaining EHRi operation round-the-clock. Emergency access to data essentially prevents planned downtime for many components of the EHRi,

[97] ISO/IEC 10731, *Information technology -- Open Systems Interconnection -- Basic Reference Model -- Conventions for the definition of OSI services*

which must remain operational continuously. Many of the details of these facilities are deeply connected to the specific hardware configurations deployed (e.g., failover, storage area networks, RAID storage, etc.). While not discussed at length in this conceptual architecture, failover, disaster recovery, etc. are important components of any robust implementation of the EHRi. They are also discussed in the forthcoming revision of Infoway's *EHR Blueprint*. One availability service merits special comment and it is discussed in the next subsection.

7.12.3 Secure backup/restoration of data

Servers for large domain repositories and virtually all instantiations of the EHRi data repository will rely upon continuous backup facilities to ensure uninterrupted failover.

The use of encryption or Identity Protection Services is essential to the secure backup of EHRi data containing PHI. Restoration of such data during disaster recovery or system roll-back requires secure key management protocols be in place that ensure continuous availability while at the same time ensuring that copies of EHRi data containing PHI are never stored in clear text.

7.12.4 Intrusion Detection and Prevention Services

Like network security services, intrusion detection and intrusion prevention are not dealt with at length in this document as they have few characteristics that are peculiar to the healthcare sector. See Appendix A.9.2 for a discussion of analysing logs to detect intrusion.

7.12.5 Scan for and protect against malware

Malware protection is an important component of any infostructure that connects servers to open networks (and even a VPN in such a user environment as large and heterogeneous as is frequently encountered in healthcare must be considered open). One of the assumptions listed in section 1.4 (Assumption 7) is that malware security will run on all EHRi servers.

7.12.6 Data archiving

Health data must be retained for many years. Health record archiving guidelines are available from the Canadian Health Records Institute but no national standard exists for electronic record retention of PHI. Further policy development in this area is needed if archiving is to be implemented consistently across instantiations of the EHRi.

The long periods of time during which archived data must be maintained also raised the issue of digital signature renewal. No current digital signature technology can be expected to last for decades. To the extent that digital signatures are applied to records in the EHRi, stored with the record, and either maintained online or archived for extended periods of time, a digital notary service will be necessary to periodically[98] attest to the validity of these digital signatures.

7.12.7 Secure data destruction

Several serious privacy breaches over the last five years have been traced to copies of data that were not properly destroyed before equipment or media containing the data was sold or scrapped. Some Canadian jurisdictions have enacted laws to prevent such occurrences: for example, legal requirements

[98] Just how often such periodic attestation must take place is a function of the digital signature algorithms and key lengths used and the current state of cryptographic research. In essence, a digital signature must be subsequently countersigned by a notary using a more robust digital signature before such time as the original digital signature can be called into question. For example, digital signatures made with a 1024 bit RSA digital signature should now be countersigned by a notary using a more robust signature key (e.g. a 2048 bit RSA digital signature) lest rapid advances in the use of cryptanalytic tools running in parallel on many desktop computers place the integrity of the original signature in doubt.

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”.

Simple utilities exists to securely wipe data from rewriteable media such as computer hard disks and their use must be rigorously enforced and secure methods for destruction of non-rewriteable media must be followed.

8 Other EHRi Common Services with P&S Implications

Appendix A briefly describes several EHRi common services that, while they are not P&S services, nonetheless have P&S features or special considerations. They are:

- Session management,
- Client registry services,
- Provider registry and user registry services,
- Notification services,
- Messaging Services, and
- Mapping Services.

All of the above are described in detail in the forthcoming revision to the Infoway *EHRS Blueprint*. P&S implications for these services are briefly described in the subsections that follow.

8.1 Policy Management Service

A policy management service works as a uniform way to access, modify and coordinate the privacy and security related business rules operationalised by the P&S services and other common EHRi services. P&S services that rely upon the policy management service are:

- User Identity Management Services,
- Access Control Services (access control policy),
- Consent Directives Management Services, and.
- Identity Protection Services (issuance of FIDs and resolution of ECIDs).

As policies are developed (see section 10.3 for a list of the policies and procedures that must be developed before the architecture can be fully implemented), the Policy Management Service must be able to encode and then enforce the operational aspects of these policies. To be effective, policies must be codified and interpreted and where necessary, mapped from one jurisdiction or set of jurisdictions to another. Important architectural questions remain about how this is best handled within the Policy Management Service and a full resolution of the outstanding issues will remain unanswered until more policy development takes place. For example, a policy framework for consent metadata has not yet been developed. In the absence of such a framework, the encoding of consent rules into the Policy Management Service will remain ad-hoc.

Several goals must be achieved before policy enforcement can be automated by a policy management service:

1. Jurisdictional policies must be harmonised, at least to the extent that they can be placed within a coherent conceptual framework. For example, while consent policy varies widely among jurisdictions, a conceptual data model for consent directives will allow information about consent directives to be meaningfully transmitted from one jurisdiction to another.
2. Rules must be captured and codified in data structures that allow the policy management service to operationalise these rules.
3. When rules change, the EHRi must, for audit purposes, be capable of reconstructing exactly which rules were in place and operationalised at any given point in time.

Inter-jurisdictional flow of PHI requires additional processing to ensure effective policy enforcement. An additional goal must be achieved before policy negotiation can be automated:

4. A common vocabulary must exist within which policy terms can be unambiguously defined for the purposes of implementing policies and instantiating them in procedures. For example, if the

meaning of "implied consent" varies operationally from one jurisdiction implementing the EHRi to another, consent policy rules that operationalise aspects of consent directives management dealing with implied consent can't work during inter-jurisdictional transfers of PHI.

Some simplifying assumptions can be made to ease the implementation of the policy management service and make its operations tractable. The most important simplifying assumption is the following:

Assumption 22 Data containing consent directives may flow from one jurisdiction to another but policy related data does not.

For example, the EHRi implemented in jurisdiction "A" will apply all of A's policy rules for the enforcement of consent directives. It may even have additional policy rules specifically for the case where PHI is disclosed to jurisdiction "B". Jurisdiction "A" will also attach consent directives to the data (where applicable) and transfer them to jurisdiction "B" along with the PHI. Jurisdiction "B" may even have special policy rules for PHI received from another jurisdiction. But jurisdiction "A" will never transmit its policy rules to jurisdiction "B", nor expect jurisdiction "B" to process these foreign rules.

This assumption eliminates the requirement for policy mappings or a policy mapping component, at least for the purposes of operationalising the P&S conceptual architecture. Nevertheless, the need remains for data structures that support interoperability (for example, a common sharable data structure for consent directives).

8.2 Session Management Service

Every user accessing the EHRi will be authenticated and logged in to a secure session. Session Management services will be responsible for maintaining the authenticated user identity post-login by means of a session token. Service component include those that open, close and terminate user sessions.

8.3 EHR Services

In addition to protecting the contents of client registries, the P&S services must call upon client registries to provide an essential service: the marking of patients/persons whose privacy and security are at elevated risk. This in turn is required to operationalise Security Requirement 49 "Analysing Audit Logs for Patients/Persons At Elevated Risk. See "Mark EHR of patient/person at elevated privacy risk" in Appendix A.

8.4 Provider Registry and User Registry Services

The provider registry and user registry[99] will contain information on providers and users that will need to be protected and this information is included in the information assets whose confidentiality, integrity and availability must be protected (see section 0). The confidentiality of this information should not be underestimated, as information such as email address of healthcare providers, telephone numbers, and practice addresses would have considerable value to marketers. A large-scale disclosure of such information would constitute a major security failure.

Like other common services of the EHRi, the P&S services will rely upon the user registry to resolve user IDs.

[99] The question of whether these are two separate registries or combined into one is briefly discussed in section 7.2.3.

8.5 Notification Services

Notification of privacy officers and security officers of certain specific events is an essential feature of the P&S conceptual architecture. The general Notification Services are required to operationalise the following:

1. **Notify on override of consent directives**, used to notify an organisational privacy officer that a patient consent directive has been overridden; for example, to disclose data in a medical emergency (see section 7.6.11); and
2. **Notify on security event occurrence**, used to notify a security officer of a security breach; for example, an intrusion detection alert.

8.6 Messaging Services

The EHRi messaging service will be responsible for processing all messages sent to or from the EHRi. This service will need to be tightly coupled with the encryption service to ensure that all message traffic is encrypted at the message level.

8.7 Mapping Services

General mapping services are provided by the EHRS Blueprint. The P&S conceptual architecture requires mapping services at several points:

1. in the mapping of organisational user roles to EHRi user roles (see 7.5.3);
2. in the mapping of consent directives between/among jurisdictions (see section 7.6.7); and
3. in the mapping of ECIDs between jurisdictions via FIDs.

The latter (item 3) is not expected to be implemented with a mapping service, but rather with the secure and privacy protective mechanisms of the Identity Protection Service (see section 7.7).

9 Deploying the P&S Conceptual Architecture: Interim States

9.1 Introduction

This document has so far examined the desired future state of the P&S conceptual architecture; i.e., what it will look like when fully built and deployed. But what will it look like in the next 24 months? In other words, what will its interim state be in mid 2007?

The question has three aspects:

1. **interim states of deployment of the EHRi**
   Questions to consider include how access via clinical portal and access via POS system will impact deployment to users and how this will affect the type of trusted user management that most needs to be deployed first.
2. **interim states of the architecture as a whole**
   Questions include which services are most critical and which services must be implemented first.
3. **interim state of each of the ten P&S service**
   As described in section 7, some of these services have different approaches for deployment and some a quicker to deploy than others.

Infoway is currently engaged in a major project to update its EHRS Blueprint. At that time, interim states of deployment of the EHRi will be carefully considered for all EHRi services, including those P&S services described in this document.

10 Governance of the EHRi

10.1 Overview

Why does an interoperable EHR require governance? Governance is needed because healthcare custodians won't use an EHRi unless they have assurance that their custodial responsibilities are not be compromised in the process. Without such assurance there will be no trust in the system by its users. Without such trust, user will not make widespread and effective use of the EHRi. Without widespread use, the EHRi will be in constant danger of degenerating into a regrettable waste of time and resources.

Effective governance of an interoperable EHR rests on several core components:

- clear articulation of trust and accountability,
- setting of minimum standards,
- conformance criteria and compliance measurement, and
- frameworks and detailed policies and procedures.

As discussed in the Requirements document, Infoway is keenly aware that it has no mandate to participate in the governance of EHRi operations or to develop operational policy or to assess compliance. This document continues to evolve within a collaborative framework of consultations with Canadian health informatics experts and with healthcare representatives of Canada's federal, provincial and territorial jurisdictions and professions and it is expected that broad consensus on the P&S conceptual architecture will be achieved. Nevertheless, the question of exactly how the secure and privacy protective design, implementation and ongoing operation of the EHRi is achieved is ultimately a question to be resolved by whatever information governance structure is put in place to guide the deployment of the EHRi across Canada and the future inter-jurisdictional flow of information that the EHRi will facilitate. Many EHRi governance issues are unresolved at the time of this writing. In stating that resolution of governance issues is outside the scope of this document, the authors in no way wish to diminish the important task of resolving these important issues.

The reader's attention is drawn to two governance issues that pertain to this document's contents:

1. One of the assumptions made in this document has significant implications for governance; i.e. Assumption 14 **Every implementation of the EHRi will store PHI under the governance of the implementing jurisdiction(s).** This has implications not only for inter-jurisdictional transfers of information, but for the maintenance of sovereignty over information held in custody. Concerns surrounding the US Patriot Act continue to concern healthcare custodians and at least one jurisdiction (BC) has reacted decisively to this perceived challenge to patient privacy and responsible custodianship.
2. While the emphasis in this document is on protecting the privacy of patients/persons, the privacy of healthcare providers is no less important. As noted in 0, confidential information obtained during the registration process includes personal information and must be protected as such. More generally, health care providers must be confident that information collected for the purposes of treatment and care will not be used secondarily to monitor the practice habits of individual (identifiable) healthcare providers without their express consent. To do otherwise invites a cessation in use of the EHRi by healthcare providers.

10.2 Development of Governance Models and a Governance Framework

Issues surrounding transfer of PHI across interoperable systems need to be addressed. Even within a jurisdiction, governance models would need to be established to address intra-jurisdictional transfers of PHI from one institution to another. Many questions remain outstanding. What are the rules for cross-border data exchange? What are the roles for cross-organisational data exchange? What are the

minimum criteria for effective data sharing agreements? How is custodianship addressed and custodian responsibilities maintained when data flows from one jurisdiction to another or from one organisation to an interoperable EHR? How are disputes fairly and efficiently resolved? Such questions require much discussion and policy resolution. During jurisdictional workshops, participants clearly articulated the need to develop consensus on what governance models would be most effective. They also wanted a clear framework within which questions about governance and policy could be answered. This framework and these governance models will be needed to support the deployment of the technical architecture.

Considerable uncertainty remains among jurisdictional representatives as to the custodial responsibilities of healthcare custodians, especially as they relate to inter-jurisdictional disclosures of PHI, Clarity is essential if healthcare custodians are to use the EHRi with trust and assurance that their custodial responsibilities will not be compromised in the process.

While these governance issues are far beyond the scope of an architectural document, the development and implementation of the EHRi depend critically upon these governance issues being adequately addressed. Governance itself is outside the scope of Infoway's mandate, yet there remains a possible future role for Infoway in facilitating further inter-jurisdictional discussions on governance, especially as such discussions relate to privacy, security, and the EHRi.

However governance issues may be resolved in the future, jurisdictional representatives have clearly indicated that effective governance is critical to ensuring the confidence of healthcare providers and the general public in the safety, integrity and trustworthiness of electronic health records.

10.3 Development of Policies and Procedures

Effective operation of the P&S conceptual architecture will not be possible as described in this document without development of the following policies and procedures (the following is not an exhaustive list):

1. an access control policy that determines, for each user role and in each jurisdiction, the EHRi services that the user can make use of and the EHRi data fields which the use can access or update (see section 7.5.3);
2. a mapping, where applicable, of organisational user roles to EHRi user roles for all organisational roles supported by a jurisdiction's implementation of trusted organisational user management (see sections 7.2 and 7.5.3);
3. a mapping of roles and access privileges from one jurisdiction's EHRi to another's for all jurisdictions permitting access requests (under strictly controlled circumstances) from users in another jurisdiction (see section 7.5.3);
4. a policy for the withholding or revocation of consent, including a definitive description of permissible consent directives and the circumstances under which they can be effected or overridden (see section 7.6.7); and
5. a policy on the mapping of ECIDs between jurisdictions via FIDs (see section 7.7.4).
6. a policy on what constitutes adequate levels of authentication and a threat and risk assessment of the combinations authentication factors that will provide equivalent ways of achieving this level of authentication (see section 7.4.3).
7. a nationally adopted and jurisdictionally supported and applied consent messaging schema.

The ACIET framework is a useful starting point for the further development of policy for the effective operation of an EHRi, as it encapsulates some significant policy analysis and a broad agreement among many Canadian jurisdictions (excepting Saskatchewan and Quebec).

Over the long term, the EHRi will also need detailed recommendations on minimum standards for digital archiving.

11 Privacy and Security Standards

The right standards adopted at the right time can make an important contribution to the development of the EHRi and to its efficient ongoing operation. They will do so by applying critical design constraints: standards chosen appropriately conserve designers' time and effort by providing a stable foundation of pre-defined capabilities and processes that do not need to be re-invented. Instead of designing the privacy and security features of the EHRi from scratch, architects are free to turn their attention to the design of higher-level, value-added functionality, while letting the standards inform the design of the basics.

Designing the EHRi in this way does more than just save time and effort. Good standards allow systems to interoperate seamlessly. Good standards encapsulate a great deal of knowledge and experience – some of it hard-won – and make it available to the architects of new systems. These standards make virtual private networks possible. They protect the privacy of individuals without limiting their freedom of choice or compromising their security. Some make their way into laws and regulations. There are many more P&S standards that, while arguably not great standards, are still serviceable and worthy of serious consideration. These standards are addressed in "EHR Privacy and Security Standards Review"

Three types of standard are considered in this document:

1. best-practices standards that specify in detail how an activity should be carried out;
2. evaluative standards that specify either a minimum level below which performance is considered unacceptable, or a desired level at which performance is regarded as effective or as meriting certification; and
3. technical standards that specify in detail how information technology protocols work.

It is the last type of standard that has a direct impact on the P&S conceptual architecture. Three such standards are noteworthy:

1. Extensible Access Control Mark-up Language (XACML),
2. Security Assertion Mark-up Language (SAML),
3. the Extensible Mark-up Language Encryption standard (XMLEnc), and
4. the Extensible Mark-up Language Digital Signature standard (XMLDSig).

These and others are discussed in detail in the Standards document and recommendations made about their appropriate use.

12 Implications for Vendors of POS Systems

Without the cooperation of vendors to modify and implement POS systems to interact with the EHRi, the EHRi will not come close to reaching its potential. Infoway is committed to working closely with vendors to ensure that this conceptual architecture is both comprehensive and capable of being effectively implemented. Infoway expects jurisdictions to refer to this architecture when planning and designing interoperable EHRs and thus vendors can expect aspects of this architecture to be referred to in RFPs. Therefore understanding of this architecture for vendors of solutions in the Canadian healthcare marketplace is essential and Infoway would like them to integrate this architecture into their discussions with jurisdictions.

The vendor web cast of May 25, 2005 generated much useful written feedback. Among the many comments received:

- when PHI is disclosed from one jurisdiction to another, which jurisdiction's rules apply? (the disclosing jurisdiction's rule apply – see Assumption 13 on page 3);
- concern was expressed about the need for effective use training as an essential ingredient in any successful implementation of a security architecture – see the Requirements document for further discussion of user training requirements;
- vendors commented on the potential of using digital signatures in the process flow of user identity management and also speculated about its potential use in securing audit logs;
- vendors suggested that healthcare professionals can create accounts for their assistants thus eliminating the need for each professional to give his/her own access code / password to somebody else (see the enhanced discussion of delegated registration of users in section 7.3.4);
- concerns have been expressed about "role explosion" – the potential for role based access control to become burdensome because of an excessive number of roles (see section 7.5.3 for further discussion of professional, EHRi roles and POS system roles);
- support for a "responsible senior healthcare provider" in relation to each patient/person health profile was seen as an important enabler in at least one jurisdiction (see section 7.5.5);
- respect for custodial responsibility is seen as essential for gaining the trust of healthcare providers, which in turn is essential for uptake of EHRi services (see section 10.2);
- concerns were expressed about the clarification of rules regarding access by healthcare providers with specific roles and how these access privileges map to those of other jurisdictions during inter-jurisdictional access (see the discussion of the need for access control policy in 10.3);
- vendors want to ensure that the content of audit logs is specified; that access rules as to who can access an audit logs are clearly spelled out, that governance issues relating to inter-jurisdictional audit are clearly specified; and that compliance criteria are developed for auditors;
- concern was expressed about the variability of interpretations that exist in (some versions of) HL7 and the need for unambiguous guidelines where such ambiguities exist;
- the categorisation of data for the purposes of consent is an essential constituent of fine-grained consent directives (i.e., those that not merely opt out of the entire EHR) and vendors want such categorisation to be specified;
- further clarity is needed in the general specification of when data is a copy, when it is a "master", and when duplicated data is updated (as they are not specific to the P&S architecture, such data replication issues will be addressed in the forthcoming revision of the EHRS Blueprint); and
- standards are needed for the storage of consent directives and for their interoperable exchange;
- some misunderstandings arose about the need for risk assessment (essential in any implementation – as this is a conceptual architecture, it does not lend itself to a detailed Threat and Risk Assessment, but implementation of the services described herein are certainly

amenable to such an assessment and indeed this is an essential component of a secure and robust implementation.

The May 25, 2005 vendor web cast was only one of many opportunities for vendors to influence thinking around the EHR architecture. In addition to feedback obtained during and after this web cast, Infoway welcomes additional comments and suggestions from POS system vendors.

Appendix A Detailed Description of P&S Services

A.1 User Identity Management Services

Service Components:

- A.1.1 Register EHRi user
- A.1.2 Manage User Identity

A.1.1 Register EHRi user

Description:

An EHRi user is any person or system that can access EHR information. This includes physicians, patients, substitute decision makers, system and user administrators etc.

The "register user service" is used to register a user. This is a called service which means that other services would be calling this service to register a user. This service may physically exist as part of the services implemented in a user registry. The parameters required to be passed to this service are dependant on the interface provided by the component that implements this service, namely the user registry.

Used by:

Applications that need to register users.

Uses:

This is a called service that exposes a public interface. What it calls or uses to fulfill its responsibilities is not visible.

Required Inputs:

- First name
- Middle initial
- Last name
- Address (various fields)
- User ID
- Password
- Location/Facility ID

Response:

- Success or Failure.

Rationale:

All organisations connecting to the EHRi must have a formal user registration process to which potential users of systems connecting to the EHRi are subjected.

These user registration procedures must ensure that the level of user identification that is provided is consistent with the degree of assurance required, given the value of the information assets and the functions that will be available to the user and the potential for abuse inherent in the functions accessed by the user.

Every healthcare provider accessing an EHR must be registered and that registration must include capture of the user's identity. Without being registered, a user will not be able to access

any data from the EHR. The registration of the user forms the basis of authentication and authorisation systems.

A.1.2 Manage User Identity

Description:

This service component provides foundational services for other higher-level services such as user registration, authentication, authorisation etc. The following services are part of the manage user identity service component:

- Generate unique identifiers for users:

  This service is used to generate a unique user ID during the user registration process.

- Lookup user ID for a user

  Given alternative identifiers such as first name, last name, driver's license, health card number etc., this service will provide the (unique) user ID. This can then be used to access functions and data in the EHR.

- Suspend/revoke user access

  Flags the user ID to revoke user access to the system

Used by:

- A.1.1 Register EHRi user
- Any application or service that needs to look up user ID to fulfill other business requests

Uses:

- A.9.1 Securely Log Events

Required Inputs:

- None (for generate unique user ID)
- Alternative IDs such as first name, last name etc. (for lookup user ID for a user)
- User ID (for revoking user access)

Response:

- User ID (for generate unique user ID and Lookup user ID)
- Success/ Failure (Revoke user access)

Rationale:

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

The EHRi and all systems connected to the EHRi must also support the suspension or revocation of user access to the EHRi in a timely manner; i.e. they must immediately prevent the newly disenfranchised user from logging on. This requirement ensures that user access to PHI can immediately and systematically be suspended. This is a distinct process from the quotidian updating or deletion of a given access privilege for a user; the latter is an administrative function of assigning user access privileges, not suspending *all* access by preventing the user from logging on. The exercise of such extraordinary measures would only be undertaken in the case of suspected identity fraud, malicious use or similar such circumstances. The latter allows responsible individuals to rapidly terminate the access privileges of one or more registered users of the EHRi. The suspension or revocation of user

access privileges need not be pejorative; there are many reasons why a user's access privileges should be revoked. Medical leave of absence is a typical example. The revoking user will supply a reason for revocation and the suspension/revocation event will be logged, as well as the reason for suspension or revocation.

A.2 User Authentication Services

Service Components:

- A.2.1 Authenticate user
- A.2.2 Generate Authentication Token

A.2.1 Authenticate user

Description:

This service component validates a user's identity. This service is called the first time a user accesses the EHR. Depending on the authentication mechanism used, the service will receive a user ID, password, PIN, token or other such identifier, which will be used to validate the user. If the user is valid, the service will return an access token. The "authenticate user" service then calls the services in the session management service to store the token as part of its collection for the duration of the session. An example of a token is a cryptographically protected binary encoded string that the user can then use to access EHR functions during the session without having to re-login.

When an already authenticated user makes a system request, the requested service will call the "authenticate user" service, passing it the access token retrieved from the session service. It will then check if the authentication token is valid, based on the timestamp and the time-to-live properties. If the time to live is less than the assigned threshold, the 'authenticate user' service will call the "generate authentication token" service to refresh the timestamp. If the authentication token is expired, the service will raise an exception notice indicating that the user needs to login again with the appropriate credentials.

Used by:

- Any business service that requires users to be validated before providing access to function and data
- Administrative applications that need to authenticate users

Uses:

- A.2.2 Generate Authentication Token
- A.11.1 Session Management Service
- A.9.1 Securely Log Events

Required Inputs:

- User ID
- Password and other authentication identifiers
- Access Token

Response:

- Access Token
- Success or Failure

Rationale:

Every user needing access to the EHR must be authenticated. This service component provides this needed validation of the user's identity.

A.2.2 Generate Authentication Token

Description:

This service component is part of the services contained in the user authentication services. This service is called by the "authenticate user" service component and it generates an access token. An access token is a cryptographically protected, binary-encoded string containing minimal user information, a timestamp, time-to-live data, etc. This service can also be used to regenerate an expiring token. When the time to live property value is below a pre-configured setting, the authentication service calls the generate authentication token service component passing it a valid but soon to expire access token. The service component regenerates and returns the access token to the authenticate user service.

Used by:

- A.2.1 Authenticate user
- A.9.1 Securely Log Events

Required Inputs:

- User ID
- Access Token (for regenerating expiring tokens)

Response:

- Encrypted Access Token

Rationale:

In a distributed application, a user needs to be validated every time a request is made to the system. One way to do this is to get the user to login before every request. This is not practical. The access token generated by this service component is used by the system to validate the user for subsequent requests made within the duration of a given session. The encrypted token and the time-to-live property provide the necessary protection against unauthorised users trying to access the system.

A.3 Access Control Service

Service Components:

- A.3.1 Manage access control related business rules
- A.3.2 Manage user's role
- A.3.3 Manage association between user and work group
- A.3.4 Manage association between user and patient/person
- A.3.5 Authorise user

A.3.1 Manage access control related business rules

Description:

The *Manage Access Control-Related Business Rules* service component is the central rules management and coordination tool for access control related business rules. This service component will translate the access control policy into an automated set of business rules that can be applied on a real time basis to the determination of access privileges for users.

This is also the service component administrators would use to administer each of the following:

- jurisdictional list of available user roles,
- mappings from one jurisdictional set of roles to another, and
- mappings of user roles to EHRi services.

Used by:

Administrators of access control policy.

Uses:

A.9.1 Securely Log Events

Required Inputs:

- EHRi user ID,
- Action to be performed (create, read, update or delete business rule)
- Relevant data (new or updated role, new or updated services available to the role, etc.)

Response:

Success or failure.

Rationale:

This service component will enable central management and coordination of access control policy. Without such a centralised policy management service component, the many service components related to user privilege management would not operate in a coordinated and comprehensive manner.

A.3.2 Manage user's role

Description:

Access to data and functions in an EHR is provided based on the user's identity and role, as well as on related criteria such as location and institutional affiliation. Roles play an important role in support of an authorisation model.[100]

This service component allows an administrator to assign one or more roles to a user and also allows such assignments to be changed as required over time. These roles are predefined and are created using service components in the access control service. The service will first check to ensure the user ID and the role to be assigned are both valid and will otherwise raise an appropriate exception error.

Used by:

- Administrators of user access privileges.

Uses:

- Manage User Identity
- Securely Log Events

Required Inputs:

- User ID of user whose role is being assigned or changed,

[100] Authorisation is the confirmation that an authenticated principal (a user, a computer, a device, etc.) has permission to perform an operation.

- Role being added or deleted
- Action to be performed (add or delete role)

Response:

- Success or Failure

Rationale:

Ethical and legal privacy requirements, as well as the consent directives of each patient/person, govern access to the patient/person's EHR. The EHRi must ensure that legitimate (i.e., authenticated) users access only those records that they entitled to access in the course of their work. Users may have access restrictions based upon their role (e.g. a podiatrist may not be able to access mental health data), their work group (e.g., whether they are staff of a particular clinic or hospital), their relationship to a patient/person (i.e., whether or not they are a part of a patient/person's care team), and the specific consent directives of the patient/person. The system may restrict the information that a user is allowed to retrieve based upon their role (e.g., a medical receptionist may only be able to retrieve or update demographic information and emergency contacts). The "assign role(s) to user" service component creates the association of a user with authorised roles.

A.3.3 Manage association between user and work group

Description:

This service component allows user access control administrators (typically local administrators) to assign a user to one or more work groups (such as clinical teams) to determine which records the user can access. Group-based access control allows users to be assigned to working groups such as primary care clinics, hospital emergency departments, and community based health and social care teams. Users can then rapidly be given access to all the records of patients in the care of that team.

Used by:

Local administrators who assign users to work groups for the purposes of access control.

Uses:

A.9.1 Securely Log Events

Required Inputs:

- EHRi user ID,
- User ID of user whose association is being assigned or changed,
- Action to be performed (add or delete association with group).

Response:

Success or failure.

Rationale:

Group-based access control facilitates the rapid administration of access control for users who move frequently from one team to another (for example, based on assignment to hospital care teams). As noted above, such groups are typically administered locally (within a hospital, say), but the ability of the EHRi to support group-based access control will greatly enhance the security and utility of EHRi access control in situations such as primary care where the access of users to patient records is largely dependent on whether there is a professional association between the user and a primary care physician associated with the patient's record – i.e., whether the user is a staff member of the practice.

A.3.4 Manage association between user and patient/person

Description:

This service allows users with a pre-existing relationship to a patient/person's EHR (a family physician, say) to grant access to other users who have no previously established relationship to that patient/person's EHR (a specialist, say).

Used by:

EHRi users who have access to a given patient/person's record, who wish to confer access to another EHRi user, and who (by virtue of their role) have the ability to do so.

Uses:

- A.9.1 Securely Log Events

Required Inputs:

- EHRi user ID of user granting access,
- User ID of user whose association is being assigned or changed,
- EHRi patient ID of patient/person who is the subject of the access being assigned,
- Action to be performed (add or delete association with role).

Response:

Success or failure.

Rationale:

This service component is needed in those situations where a user who has full access to a record (a responsible physician, say) must rapidly grant access to a user who has never had a previous legitimate relationship with the patient (a specialist, say). The patient may not be present or even conscious when this access control decision is made. Explicitly managing such associations between providers and patients/persons 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.

A.3.5 Authorise user

Description:

Authorisation of users attempting to access an EHRi service (including reading or updating portions of a given patient/person's EHR) is an essential privacy and security protective feature of the EHRi. Only authorised users can access an EHR or avail themselves of an EHRi service. Authorisation of a user includes processing of all of the following:

- the user's assigned role(s) (role based access control),
- where applicable, associations between the user as a healthcare provider and other providers (group-based access control),
- where applicable, associations between the user as a healthcare provider and the patient/person whose EHR is being accessed (discretionary access control), and
- consent directives of the patient (determined via the "Validate consent" service component).

Used by:

- all EHRi services prior to granting access to a user

Uses:

- A.4.3 Validate consent

Required Inputs:

- User ID of user to be authorised
- Record ID of patient/person whose record is being accessed (where relevant)
- Service ID of service being accessed (e.g. read access to a patient/person's EHR)

Response:

Success or failure.

Rationale:

Authorisation of users is a fundamental requirement of controlling access to services and records accessible from the EHRi, as not all users will be qualified to access all EHRi services and not all will be qualified to access the EHRs of all patients/persons.

A.4 Consent Directives Management Service

Service Components:

- A.4.1 Manage Consent-Related Business Rules
- A.4.2 Manage Patient/Person Consent Directive
- A.4.3 Validate consent
- A.4.4 Map consent (between and among jurisdictions)
- A.4.5 Override Consent
- A.4.6 Patient/person access control service
- A.4.7 Log Consent Directives and Their Application

A.4.1 Manage Consent-Related Business Rules

Description:

This service component allows users to handle PHI in an EHR environment in accordance with consent-related business rules specific to organisations and jurisdictions. For example, application of consent-related rules might automatically prohibit the *disclosure* of any PHI for care and treatment purposes in an EHR environment if a patient/person has indicated that such information cannot be *used* for care and treatment purposes. Similarly, managed consent rules might also permit “lock boxes” or masked PHI to be accessed in an EHR environment in accordance with specific consent-related business rules (e.g. for emergencies or in the case of mandatory reporting of communicable diseases).

Used by:

This service component manages the rules used by the *Manage Patient/Person Consent Directive* service whenever a patient/person grants, withholds or revokes consent. The rules are also used by services that insert, update and retrieve PHI in order to apply the patient/person’s consent directives or to override these directives in specific, limited circumstances.

Uses:

This service component uses the Consent Directive Repository to retrieve and apply consent rules. This service will use the Securely Log Events service when consent rules are applied.

Required Inputs:

Required inputs will vary depending on the purpose for which the service is used and the manner in which it is deployed in each organisation/jurisdiction. Typical inputs include:

- EHRi user ID,
- EHRi user role name,
- client ID (i.e., ID of patient/person),
- application ID (i.e., ID of POS system or EHRi component making the request for PHI),
- domain ID,
- jurisdiction ID
- EHR Data and other PHI
- Consent Directive

Response:

Response will vary depending on the purpose for which the service is used; the purpose for which the service is used will vary by organisational/jurisdictional requirements and deployment.

Rationale:

There are a number of enterprise-wide consent-related business rules, normally documented in an organisation's privacy policies, which the EHRi may be able to automate. By automating these rules, this service component ensures that PHI receives appropriate protection in an EHR environment while reducing the time and effort required to process an individual patient/person's privacy-related requests. This service component is also required to operationalise Privacy Requirements 3, 12 and 13.[101]

A.4.2 Manage Patient/Person Consent Directive

Description:

This service component allows patients/persons to grant, withhold or withdraw their consent for the collection, use or disclosure of PHI in accordance with applicable privacy legislation and policies. The granting, withholding or withdrawal of consent in these circumstances is known as a "consent directive". An individual may have multiple consent directives in an EHR environment and these directives may also change over time. Authorised substitute decision makers may also issue consent directives on behalf of patients/persons. Consent directives may relate to specific EHRi users, data elements, diagnoses, and diagnosis-related information (e.g., HIV tests results and related medications). Information pertaining to a patient/person's consent directives is contained in a Consent Directives Repository.

Used by:

This service component is used by authorised EHRi users on behalf of a patient/person or his or her authorised substitute decision maker. Authorised EHRi users may use this service component directly or they may use it through a POS system.

Uses:

Information concerning a patient/person's consent directives will be stored in a Consent Directives Repository. Depending on the nature of the consent directive, the service component may use the provider registry and/or user registry, the patient/person's EHR, or domain repositories, in order to facilitate the consent directive. This service component also uses "Log Consent Directives and Their Application" (see section A.4.7).

Required Inputs:

[101] See Canada Health Infoway, *Electronic Health Record Privacy and Requirements,* 2004.

- EHRi user ID,
- EHRi user role ID,
- client ID (i.e., ID of patient/person),
- substitute decision maker ID (where applicable)
- facility ID,
- jurisdiction ID
- Consent Directive (grant, withhold, withdraw)
- EHRi User ID, EHR Data or other PHI for which patient/person wished to grant, withhold or withdraw consent for access, modification or disclosure.

Response:

Operational status (success or failure of attempted update).

Rationale:

This service component is required to operationalise Privacy Requirements 8, 10, 11, 12, 14 and 15.[102]

A.4.3 Validate consent

Description:

Validation of consent is an essential component of authorising users prior to accessing a patient/person's EHR. This service component will determine whether consent has been withheld or revoked before information is provided by the EHRi to the requesting application and EHRi user (via the "Authorise user" service component). The determination of the status of a patient/person's consent will be performed by consulting a consent repository for entries associated with that patient/person. In the event a negative consent repository is used (i.e., containing only entries for patients/persons who have withheld or revoked consent), each entry shall represent an individuals wishes to withhold or revoke consent for use and/or disclosure of PHI.

Used by:

- A.3.5 Authorise user
- A.4.2 Manage Patient/Person Consent Directive

Uses:

- A.4.7 Log Consent Directives and Their Application

Required Inputs:

- EHRi user ID,
- EHRi user role ID,
- client ID (i.e., ID of patient/person),
- Facility ID (i.e., ID of facility making the request),
- domain ID,

[102] See Canada Health Infoway, *Electronic Health Record Privacy and Requirements,* 2004, pages 30-31.

- jurisdiction ID

Response:

True/False (i.e., consent is interpreted as given or not)

Interoperability Requirements:

Harmonisation of consent directives between and among jurisdictions

Rationale:

A consent validation service is required to operationalise Privacy Requirements 11 and 12[103].

A.4.4 Map consent (between and among jurisdictions)

Description:

This service component will translate consent rules from one jurisdiction or organisation so that authorised users accessing the EHRi from another jurisdiction or organisation can clearly understand and apply such rules to their own uses and disclosures of an individual's PHI. In the current (primarily paper-based) healthcare sector, data sharing agreements between jurisdictions or organisations within a single jurisdiction typically outline how jurisdictions or organisations (e.g. the signatories to the data sharing agreement) should interpret and apply specific consent rules contained in various legislation and policies. This service component would automate this process, based upon written policies and data sharing agreements.

Used by:

This service would only be called upon when data is to be transmitted between jurisdictions, or potentially between organisations, that have different consent rules. Service components such as *Validate consent* (see section A.4.3), would call this service component in such circumstances.

Uses:

This service would use its own mapping table to translate consent rules. The rules would then be applied by other services components, such as *Validate consent.*

Required Inputs:

Consent information from the location currently storing or accessing PHI, in cases where consent models in two locations differ.

Response:

Where the accessing location provides consent rules to this service component, the service component will return consent rules from the storing location. Where the storing location provides consent rules to this service component, the component will return the corresponding consent rules for the accessing location.[104]

Interoperability Requirements:

Harmonisation of consent directives between and among jurisdictions

---

[103] See Canada Health Infoway, *Electronic Health Record Privacy and Requirements,* 2004, pages 30-31.

[104] Such a bidirectional consent mapping would occur in a situation where a patient/person had placed his or her PHI in a lock box, which requires the patient/person's consent or a healthcare emergency to override it. This rule would need to be applied and conveyed to the accessing location, which could then either accept it or override the lockbox (see *section Appendix AA.4.6* below).

Rationale:

Different jurisdictions may have different legislative responsibilities as well as inter and intra jurisdictional interpretation of consent terminology. In order for a patient/person's consent directives to be applied in a consistent manner, jurisdictions must consistently define and/or map consent terminology and related rules. In addition, this service component is required to operationalise Privacy Requirements 10, 11 and 12.

A.4.5 Override Consent

Description:

This service component allows authorised healthcare providers to override a patient/person's consent directives in medical emergencies in accordance with applicable privacy legislation and policies. The service determines whether consent can be overridden in the circumstances specified. It is an essential feature of overriding consent that the event be logged and that a duly authorised privacy officer be informed of the override to ensure the override is justifiable and that privacy policy has not been abrogated.

Used by:

Services that insert, update and retrieve PHI.

Uses:

- A.4.7 Log Consent Directives and Their Application

Required Inputs:

- EHRi user ID,
- EHRi user role ID,
- client ID (i.e., ID of patient/person),
- application ID (i.e., ID of POS system or EHRi component making the request),
- facility ID,
- jurisdiction ID
- type of access (e.g.; read, update, etc.)
- purpose (e.g.; emergency access)

Response:

True/False (i.e., consent is overridden or not)

Rationale:

Established practice in all Canadian jurisdictions and explicit legislative authority in Ontario mandate that medical information is to be accessed during medical emergencies where either the patient/person under treatment cannot provide explicit consent directives or where time is of the essence.

A.4.6 Patient/person access control service

Description:

Patients/persons may wish to restrict access to specific components of their EHR. A prime example is the prescription drug profile. (Access control by patients/persons to their prescription drug profiles is already effectively operationalised in the BC Pharmanet system). This information would then only be accessible to pharmacists and other authorised users to whom the individual has provided his or her permission in the form of an access code. A patient/person may permit a healthcare provider with general access to his or her entire

prescription drug profile, or the access may be restricted by subject, a date range, or other variables as established by the patient/person.

Used by:

All services attempting to access, modify or disclose a patient/person's prescription drug profile would use this service component, but only when the patient/person had placed access controls on his or her prescription drug profile.

Uses:

Client Registry

Directive/access control data store

Required Inputs:

Activation of Access Control Inputs: Patient/person identity, elements to which the patient/person would like to control access, and any other rules related to the access control (e.g. global access once delegation of responsibility occurs; access is restricted to 24 hours duration; or, restriction of access to particular individuals designated by the patient/person).

Transactional: the patient/person identifier, EHRi user identifier, prescription drug information requested, access code (where code is required for access)

Response:

Activation: Access control directive implemented (yes/no)

Exception: Could not place access control on specified information

Rationale:

As mentioned above, this service has been implemented successfully in British Columbia's Pharmanet provincial pharmaceutical information system. Unfortunately, the access control system was only implemented following several high profile privacy breaches. This service component is related to the *Manage Patient/Person Consent Directive* service component (e.g. locking or masking) described above, but provides additional privacy by allowing only the patient/person to override the access restrictions in order to provide access to his or her record. Lockboxes typically allow authorised clinicians to override a patient/person's consent directive when *they* believe it is reasonably necessary.

A.4.7 Log Consent Directives and Their Application

Description:

This service component will record when access to PHI has been denied (i.e., when an EHRi user has requested access to specific PHI and the requested information has been withheld because consent directives prohibit the information's disclosure). The determination of the status of a patient/person's consent will be performed by consulting a consent repository for entries associated with that patient/person. In the event a negative consent repository is used (i.e., containing only entries for patients/persons who have withheld or revoked consent), each entry shall represent an individual's wishes to withhold or revoke consent for use and/or disclosure of PHI.

Used by:

- A.4.1 Manage Consent-Related Business Rules
- A.4.3 Validate consent
- A.4.5 Override Consent

Uses:

- Securely Log Events

Required Inputs:

- EHRi user ID,
- EHRi user role ID,
- client ID (i.e., ID of patient/person),
- facility ID (i.e., ID of the facility from which the EHRi user is making the request),
- facility ID,
- jurisdiction ID
- type of log entry:
    - consent-related rule addition, update or deletion;
    - patient/person consent directive addition, update or revocation; or
    - consent validation result (when negative)
- new or updated data values.

Response:

True/False (indicating success of logging operation)

Rationale:

The privacy principles of "openness" and "challenging compliance" necessitate that where consent is overridden, a log entry must be made. In addition, an individual accountable for compliance with organisational privacy policy must be made aware of the existence and nature of the overriding event.

A.5 Identity Protection Service

Service Components:

- A.5.1 Resolve ECID and FID for patients/persons
- A.5.2 Manage ECIDs and FIDs for patients/persons
- A.5.3 Pseudonymise Data

A.5.1 Resolve ECID and FID for patients/persons

Description:

Upon receiving an authorised request for PHI, this service component would resolve the identity of the patient/person to an ECID. Patients/persons will typically be identified by a public identifier (e.g. a health insurance, medical service plan or health card number) that would correlate to one ECID in each identity domain containing PHI about the patient/person. Upon receiving a public identifier the service would match this identifier to an ECID that can then be used to retrieve PHI within an identity domain. The service would also be able to acquire patients'/persons' FIDs where a link between their ECID and FID had been created with the Manage ECIDs and FIDs for patients/persons service described below. Lastly, this service would facilitate the returning of PHI in or between identity domains upon receiving an authorised request for PHI containing an ECID or an FID linked to an ECID. FIDs would be used by the service in much the same manner as the public identifier, i.e. the FID would be resolved to an ECID that could then be used to retrieve PHI Both the FID and the ECID would only be used within the EHRi or disclosed between EHRis (the latter only applies to FIDs). Neither would be returned or otherwise made available to EHRi users requesting PHI. Data in transit to and from the linking tables must be encrypted.

Used by:

This service may be used by any component of the EHRi where PHI is stored. The P&S services likely to use this service are:

- A.4 Consent Directives Management Service
- A.5.3 Pseudonymise Data
- A.9.1 Securely Log Events

Lastly, this service would also be used by the "Manage ECIDs and FIDs for patients/persons" that would use this service to retrieve ECIDs in support of inter-jurisdictional disclosures of PHI.

Uses:

A.7 Encryption Services

Required Inputs:

Patient/person public identifier and/or FID

Response:

Patient/person ECID identifier. (The Patient's/Person's ECID could be used by the EHRi common services to retrieve PHI stored under the ECID)

Rationale:
Maintaining the integrity of ECID requires by definition that those identifiers remain internal to the identity domain. Sharing an ECID between one jurisdiction's EHRi and another's creates serious problems for the maintenance of referential integrity. This service will protect eliminate this risk to referential integrity.

A.5.2 Manage ECIDs and FIDs for patients/persons

Description:

This service component manages the identity protection service's identifier linking/deletion process. If the "Resolve ECID and FID for patients/persons" service is not able to resolve an individual's public identifier to an ECID (i.e., if no PHI for the patient/person had been previously stored in the EHRi), this service will create an ECID and would link the ECID to the patient's/person's provided public identifier. Subsequently, if additional PHI from the patient's/person's health profile is required for the delivery of healthcare this service will attempt to locate an FID associated with the patient/person. If no FID can be located for the patient/person one will be created and an attempt will be made via a probabilistic and deterministic matching process to locate any ECIDs related to the patient/person stored in other identity domains. These ECIDs will be linked under the patient's/person's FID. Also, this service would allow for the deletion of FIDs when the link between PHI in different identity domains is no long required as well allow for the deletion or modification of ECIDs, as may be required (e.g. duplicate ECIDs exist or when an ECID is compromised). Data in transit to and from the linking tables must be encrypted.

Used by:

This service may be used by any component of the EHRi where PHI is stored. The P&S services likely to use this service are:

- A.4 Consent Directives Management Service
- A.9 Secure Audit Logging Services

Uses:

- A.5.2 Manage ECIDs and FIDs for patients/persons
- A.7.4 Message Encryption

This service component may also use the "Secure Audit Logging Services".

Required Inputs:

Patient/person public identifier

Patient/person ECID and/or FID

Other patient/person identifying information to assist in resolving the patient's/person's identity within or between jurisdictions

Operation to be performed (create or modify ECID or FID)

Response:

Patient/person ECID and/or FID

Requested PHI operation confirmation or denial

Where PHI has been requested, requested PHI or notification of denial-of-access

Rationale:

Health data protection legislation commonly prohibits organisations from using information that would reveal a patient's/person's identity when other information will serve the purpose. This service component will work to ensure that the EHRi supports and facilitates this requirement by providing information that uniquely identifies a patient/person to authorised care providers without unnecessarily storing or transmitting personal identifiers through the EHRi. Storing and transmitting PHI separately from information that uniquely identifies a patient/person will protect individual privacy and mitigate the risk of a privacy breach.

A.5.3 Pseudonymise Data

Overview:

Patients/persons must be protected from inadvertent disclosure of any unencrypted identifying data, e.g. name, health card number, address, phone number etc. Risk of disclosure increases when PHI is used in situations where data stripped of identifying information could suffice (e.g. in planning, administration, and some forms of research).

Attempting to prevent this disclosure by striping identifiers such as name or health number from an EHR can be problematic. This can result in the records becoming truly anonymous, with no possible way to link the diverse records of a single patient/person. By carefully identifying each patient/person with a unique pseudonym, all the longitudinal records for "patient X" can still be interrelated.

The action of identifying an individual as "patient X" is an example of pseudonymous identification. The word "pseudonymous" refers to the fact that while the underlying identity of the patient is forever hidden behind a pseudonym, that pseudonym is unique. Therefore, all clinical records for any patient/person stored pseudonymous form will remain related. By contrast, were the records truly anonymous, there would be no way to cross-reference all the records for a single patient/person.

Pseudonymous identification has several strategic advantages:

1. Health researchers can have greater access to clinical data without compromising the privacy and confidentiality of patients/persons.
2. Hospital, institutional and health ministry planners can have greater access to health care data without compromising the privacy and confidentiality of patients/persons.
3. Healthcare providers can arrange for anonymous testing for their patients.

Description:

This service takes structured PHI and does the following:

1. remove nominative fields (e.g.: name, street address, phone number)
2. remove unstructured data (e.g.: descriptive clinical notes in text based form, as such notes may contain comments that effectively identify the data subject);
3. map quasi-nominative fields such as birth date or postal code to replace the content of such fields by mapping field content to a narrow range of values; e.g.: by mapping the postal code H3A 3G4 (Infoway's) to a geographic code for the Montréal urban community;
4. perform a cell-size count to ensure that a minimum number of patients/persons also have EHRs that would produce the same pseudonymised data;
5. assign unique but meaningless identifiers to each patient/person record such that:
   a) the same patient/person will receive the same unique but meaningless identifier in the future (hence allowing for longitudinal studies);
   b) the same patient/person will receive different unique but meaningless identifiers in pseudonymisation requests from unrelated users or institutions (hence preventing constructive inference by combining data sets in an unauthorised fashion).

Used by:

- Secondary users of healthcare data (healthcare researchers and administrators)

Uses:

- A.4.3 Validate consent
- A.4.7 Log Consent Directives and Their Application
- A.3.5 Authorise user
- A.9.1 Securely Log Events
- A.1 User Identity Management Services

Required Inputs:

Pseudonymous identifier

ECID

Specification of the data set to be pseudonymised (i.e., which records, which fields)

Identifier of the institution or individual requesting pseudonymisation – this will affect the assignment of pseudonyms so that the same institution or individual submitting a future request for a pseudonymised data set that includes records for patients/persons in the current data set will receive data with matching pseudonyms.

Response:

Pseudononymised data set

Rationale:

As noted above, both anonymisation and pseudonymisation are used to enhance patient/person privacy in secondary research use of clinical data, in patient identification during clinical trials, in public health monitoring and assessment, in confidential patient-safety reporting, and for comparative quality indicator reporting. The complexity of anonymisation and the need for trusted third party involvement in all currently feasible schemes for pseudonymisation make this an essential privacy service for the EHRS to provide.

A.6 Anonymisation Service

Service Components:

- A.6.1 Anonymise Data

A.6.1 Anonymise Data

Description:

This service takes structured PHI and does the following:

2. removes nominative fields (e.g.: name, street address, phone number)
3. removes unstructured data (e.g.: descriptive clinical notes in text based form, as such notes may contain comments that effectively identify the data subject);
4. maps quasi-nominative fields such as birth date or postal code to replace the content of such fields by mapping field content to a narrow range of values; e.g.: by mapping the postal code H3A 3G4 (Infoway's) to a geographic code for the Montréal urban community;
5. performs a cell-size count to ensure that a minimum number of patients/persons also have EHRs that would produce the same anonymised data[105].

Used by:

- Secondary users of healthcare data (healthcare researchers and administrators)

Uses:

- A.4.3 Validate consent
- A.4.7 Log Consent Directives and Their Application
- A.3.5 Authorise user
- A.5 Identity Protection Service
- A.9.1 Securely Log Events

Required Inputs:

Anonymisation requested

Specification of the data set to be anonymised (i.e., which records, which fields)

Response:

Anonymised data set

Rationale:

As noted above, anonymisation is used to enhance patient/person privacy in secondary research use of clinical data, in patient identification during clinical trials, in public health monitoring and assessment, in confidential patient-safety reporting, and for comparative quality indicator reporting.

[105] Ensuring a sufficiently high cell size count is the accepted statistical method of ensuring that the combinations of field values that result from an attempted anonymisation do not identify a patient/person because of the unique or nearly unique combination of values represented by the data. For example, while a data set consisting solely of gender, height and weight for each patient in a research group, unusual sets of data values may still identify patients because of the scarcity of that set of values in the general population; e.g.: women over 2.4 metres or men under 1.5 metres. What constitutes an "unusual" set of data values can only be effectively determined by examining how many other EHRs would also produce the same set of data values (i.e., how many patients/persons would be included in this so-called "cell"). A cell size of fewer than five individuals is generally considered unacceptable when one is attempting to protect the identities of the patient/persons whose records would be included in the cell.

The complexity of anonymisation and the need for trusted third party involvement in most currently feasible schemes for pseudonymisation make this an essential privacy service for the EHRS to provide.

A.7 Encryption Services

Service Components:

- A.7.1 Key Management
- A.7.2 Database Encryption
- A.7.3 Data Storage Encryption

A.7.1 Key Management

Description:

Although message encryption at the transport layer or network layer[106] typically uses symmetric session-based keys that are randomly generated and distributed using standardised protocols such as Diffie-Hellman, encryption keys for data storage must be generated and safely maintained for extended periods. This requires a full suite of key management protocols. These standardised protocols[107] for key management enable tasks such as the following to be performed:

- key generation,
- secure key distribution,
- secure storage of keys within a cryptographically sealed environment,
- key renewal,
- key recovery (where applicable), and
- key revocation.

Used by:

Administrators who must maintain encrypted databases, encrypted data backups, or encrypted data in long-term (archival) storage.

Uses:

Key management services do not rely upon other privacy or security service components.

Required Inputs:

- user ID,
- operation to be performed [key generation, key renewal, key recovery, key backup (where applicable)],
- key identifier (for key renewal, recovery or backup).

Response:

[106] The so-called "transport layer" is one of the seven layers in the widely adopted Open Systems Interconnect (OSI) model of network operations (the OSI layers consist of the physical layer, data-link layer, network layer, transport layer, session layer, presentation layer, and application layer). The transport layer is also one of the four layers implemented within the Internet.

[107] Security standards, including key management standards, are the subject of Electronic *Health Record Standards for Privacy and Security,* Canada Health Infoway, 2005 (forthcoming).

- secure key delivery (where applicable),
- secure key recovery (where applicable),
- updated key revocation list (where applicable), and
- operation status (success or failure).

Rationale:

It is essential to include the ability to securely generate and manage keys within the EHRi. This can be achieved by providing consistent and well-implemented key management capabilities and by effectively automating administrative key management tasks. These task include key generation, key revocation, and automated and secure mechanisms for key renewal, key replication, and (where applicable) key backup.

Key generation and secure key management are fraught with potential for error[108] and cryptographic security must be effectively and efficiently embedded in the operations of the EHRi.

A.7.2 Database Encryption

Description:

This service component encrypts and decrypts fields (columns) and records (rows) within database tables and is used to protect PHI and other security critical system data in active use within the EHRi.

Used by:

Data repositories within the EHRi containing PHI and other security critical system data organised into databases.

Uses:

Storage encryption services do not rely upon other privacy or security service components.

Required Inputs:

- user ID,
- operation to be performed (encryption of data to be inserted or updated; decryption of data to be accessed),
- database access co-ordinates (row and column identifier(s) for data accessed),
- where applicable, data to be inserted or updated,
- encryption key(s).

Response:

- database operation (insertion, update, or access),
- Operational status (success or failure).

[108] Over the years, many well intentioned but technically incorrect implementations of encryption technology have had deleterious effects on systems that included such implementations. Examples include errors in pseudo-random number generation during key generation by Netscape in early implementations of SSL and the misapplication of encryption algorithms in the design of the Wired Equivalency Protocol (WEP) for wireless networks.

Rationale:

Database encryption protects data while it is in use by the database system, as well as while it is in storage. It allows access to fields of data to be securely restricted to just those authorised users assigned roles that permit access to those fields; hence, securely operationalising role based access control. Database encryption effectively enables security policy to be disentangled from data management. Database encryption products also effectively handle the many key management problems that arise in the effective administration of column-level and row-level encryption. Finally, because database encryption protects the data both within the database management system and also within the storage media, it also protects against application-layer security breaches, server breaches, and media theft[109].

A.7.3 Data Storage Encryption

Description:

This service component encrypts and decrypts files and other data blocks and is used to protect data (other than databases – see above) in active storage, backup, or long-term archive.

Used by:

- A.10.2 Secure Backup/Restoration of Data,
- A.10.3 Data Archiving.

Uses:

Storage encryption services do not rely upon other privacy or security service components.

Required Inputs:

- user ID,
- operation to be performed (encryption/decryption),
- data to be encrypted or decrypted,
- encryption key(s).

Response:

- encrypted or decrypted data (files, or data blocks),
- operation status (success or failure).

Rationale:

Data storage encryption is most commonly needed for the following tasks:

a) data backup to secure the backup media

[109] Database encryption also has some limitations. When indexed columns are encrypted, database-management software will sort the encrypted strings and numeric values in the order of their encrypted hexadecimal values, which won't match the ordering of the unencrypted data. Special steps must be taken to deal with the encryption of indexed columns and these steps decrease the efficiency of database searches involving these columns. Encrypted databases also take up two to four times the amount of storage as their unencrypted counterparts because of the way in data is manipulated as part of the encryption process.

b) data archiving to secure the long-term storage of PHI

c) data storage of PHI on portable devices or media (such as laptops and handheld devices).

The use of data storage encryption to protect PHI is increasing in response to the ever more widespread use of mobile devices containing stored repositories of PHI. The very long lifetime of archived PHI necessitates careful management and implementation of data storage encryption in archived media. An effective strategy for data storage encryption of PHI is essential if its benefits are to accrue to implementations of the EHRi and attached POS systems.

A.7.4 Message Encryption

Description:

This service component provide for the protection of PHI in transit via message-based encryption (i.e., encryption of data in transit across networks and between servers). Such encryption is short-lived (for the duration of transport only) and is not to be confused with database encryption and data storage encryption (see above).

Used by:

- POS systems connecting to the EHRi,
- EHRi servers communicating with one another.

Uses:

Message encryption services do not directly rely upon other privacy or security service components.

Required Inputs:

- operation to be performed (encryption/decryption),
- message data to be encrypted or decrypted,
- encryption key(s).

Response:

- encrypted or decrypted data (files, or data blocks),
- operation status (success or failure).

Rationale:

Message encryption is a common and accepted way of ensuring that message confidentiality and integrity are preserved. Encryption of PHI while in transit across networks ensures that it is not susceptible to eavesdropping or tampering. As noted above, all jurisdictional health information networks in Canada provide for encrypted transmission of PHI and a secure EHRi must do so as well.

A.8 Digital Signature Services

Service Components:

- A.8.1 Digital Signature Certificate Management
- A.8.2 Digitally sign data
- A.8.3 Verify digital signature
- A.8.4 Digital Time Stamp and Digital Notary Service

A.8.1 Digital Signature Certificate Management

Description:

Like the encryption key management services described in section Appendix AA.7.1, digital signature keys and their attendant certificates requires a full suite of key management protocols. These standardised protocols[110] for key management enable tasks such as the following to be performed:

- secure digital signature key pair generation,
- secure transmission of the signature verification key to the CA for inclusion in the digital signature certificate,
- generation by the CA of the digital signature certificate,
- storage of signature keys within a cryptographically sealed environment,
- key and certificate renewal, and
- certificate revocation.

Used by:

EHRi users who will make use of digital signatures.

Uses:

- A.7.4 Message Encryption,
- A.9.1 Securely Log Events.

Required Inputs:

- user ID,
- operation to be performed (certificate generation, renewal, or revocation),
- key generation material (in the case of certificate generation),
- certificate identifier consisting of issuer and certificate serial number (in the case of renewal or revocation),
- reason (in the case of revocation).

Response:

Operational status (success or failure).

Rationale:

Digital signature capability is impossible to implement securely without providing key and certificate management services as described above.

A.8.2 Digitally sign data

Description:

Digital signatures are generated locally and are not, strictly speaking, service components provided by the EHRi (at least in the sense of a server or centralised application system generating and applying digital signatures to data on behalf of users). Nevertheless, interoperability and maintenance of a consistent level of trust require that digital signature

[110] Security standards, including key management standards, are the subject of Electronic *Health Record Standards for Privacy and Security,* Canada Health Infoway, 2005 (forthcoming).

capabilities, though locally deployed, must meet consistent minimum requirements in terms of signature key protection, algorithms supported, and key lengths allowed.

Data to be signed may include:

- a data file,
- a record,
- a field within a record,
- a security assertion, or
- an XML document, including an HL7 message or object rendered as an XML document.

Used by:

EHRi users who wish to apply a digital signature to a data file, record, security assertion, email message or other message.

Uses:

Implementation of digital signatures is local to the user's computer and does not rely on other privacy or security service components aside from the Digital Signature Certificate Management services need to create the signature keys and matching certificates in the first place.

Required Inputs:

As implementation of digital signatures is local to the user's computer, data for signature, and the signing key do not leave the user's local computer environment.

Response:

N/A

Rationale:

If the EHRi is to include e-prescribing, some capacity for digital signatures must be included in the EHRi. There are many other less common situations where the signature of a physician is required upon a form (for example, death certificates), and the replacement of these other paper based forms with electronic equivalents would speed handling and effective processing of the information they contain.

Providing the EHRi with a digital signature capability will also enable the implementation of secure time stamps, digital notarisation, strong guarantees of data integrity, and non-repudiation.

A.8.3 Verify digital signature

Description:

In addition to a user checking the information contained within a digital certificate affixed to a digitally signed document (to verify the name of the signatory for example, or the issuer of the certificate), a user's software may also check to ensure that the digital certificate has not been revoked prior to the generation of the signature. Certificate revocation checking consists in the user's software accessing an online resource (the location of which is specified within the certificate) to ensure that the certificate has not been revoked. Two common techniques are employed:

1. Certificate revocation list publication, and
2. Implementation of the Online Certificate Status Protocol (OCSP).

Implementations of the latter typically also provide an implementation of the former for backward compatibility with older systems.

Used by:

Recipients of digitally signed data who wish to confirm the validity of the signature.

Uses:

Signature verification services do not directly rely upon other privacy or security service components.

Required Inputs:

Certificate identifier (issuer and certificate serial number).

Response:

Revocation status of certificate.

Rationale:

Digital signature keys may be compromised through mishandling by the certificate holder (e.g., permitting another user to use one's digital signature). In such cases, the user must request of the issuing CA that the certificate be revoked. In rarer circumstances, a certificate may have been obtained through fraudulent means (although robust identification procedures of prospective certificate holders should make such fraud exceedingly difficult to commit). In such cases, a Registration Authority (RA) may request of the CA that the certificate be revoked. Whatever the reason, users who rely upon the validity of digital signatures must have some means by which to check the current status of a digital signature certificate in order to ensure that the certificate was not revoked and a compromised signature key used to fraudulently sign the document in question.

A.8.4 Digital Time Stamp and Digital Notary Service

Description:

A digital timestamp is a tool for creating digital evidence. It ensures that data has not been altered or backdated. A digital notary may be used to digitally sign and time stamp data to ensure that its state at the time of signing can be independently verified. Digital notarisation is the electronic equivalent of a human notary signing (i.e., notarising) a paper-based document.

Digital notaries may also be used to ensure the long-term validity of digital signatures. In general, the security inherent in a digital signature technology (including algorithms and key sizes) slowly degrades over a period of many years. Periodic re-signature and timestamp by a digital notary while the security of the underlying algorithm and key size are still considered robust allows the useful lifetime of digital signatures to be extended indefinitely. Standardised protocols exist for executing such digital notary services. [111]

Used by:

- Archivists seeking to ensure the long-term validity of digital signatures that are contained within archived data.
- Administrators seeking to secure the evidentiary validity of certain data.

Uses:

- A.8.2 Digitally sign data,

[111] A standard format for long-term digital signatures is provided by IETF standard RFC3126 *Long term electronic signature*, or equivalently by European standard ETSI TS 101 733.

- A.9.1 Securely Log Events.

Required Inputs:

User ID of requesting user,

Data to be time stamped.

Response:

Digitally notarised and time stamped data,

Operational status (success or failure).

Rationale:

As healthcare data may remain relevant for decades, its legal status as evidence may likewise be the subject of legal dispute decades after it is created (especially in the case of paediatric data). This is longer than current digital signature technologies can ensure the integrity of a digital signature. As noted above, the security inherent in a digital signature technology (including algorithms and key sizes) slowly degrades over a period of many years. Periodic re-signature and timestamp by a digital notary while the security of the underlying algorithm and key size are still considered robust is essential if the useful lifetime of digital signatures to be extended to meet the long lifetimes of PHI.

A.9 Secure Audit Logging Services

Service Components:

- A.9.1 Securely Log Events
- A.9.2 Analyse logs and detect intrusions

A.9.1 Securely Log Events

Description:

Each update of the EHR audit log will create a record in the EHR audit log containing the following information:

- the user ID of the accessing user;
- the role the user is exercising;
- the organisation of the accessing user (at least in those cases where an individual accesses information on behalf of more than one organisation);
- the patient ID of the data subject (patient/person);
- the function performed by the accessing user;
- a time stamp;
- 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
- in the case of changes to access restrictions directed by a substitute decision-maker, the identity of the decision-maker.

Used by:

- A.1.1 Register EHRi user
- A.1.2 Manage User Identity

- A.3.1 Manage access control related business rules
- A.3.2 Manage user's role
- A.3.3 Manage association between user and work group
- A.3.4 Manage association between user and patient/person
- A.4.7 Log Consent Directives and Their Application
- A.5.1 Resolve ECID and FID for patients/persons
- A.5.2 Manage ECIDs and FIDs for patients/persons
- A.8.1 Digital Signature Certificate Management
- A.8.4 Digital Time Stamp and Digital Notary Service
- A.11.1 Session Management Service
- A.11.3 Mark EHR of patient/person at elevated privacy risk
- A.11.4 P&S Notification Services.

Uses:

- A.8.2 Digitally sign data

Required Inputs:

- the user ID of the accessing user;
- the role the user is exercising;
- the organisation of the accessing user (at least in those cases where an individual accesses information on behalf of more than one organisation);
- the patient ID of the data subject (patient/person);
- the function performed by the accessing user;
- 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
- in the case of changes to access restrictions directed by a substitute decision-maker, the identity of the decision-maker.

Response:

Operational status (success or failure).

Rationale:

At a minimum, as noted above, some Canadian health privacy legislation requires healthcare providers to maintain records of successful or unsuccessful attempts to gain access to records, and attempts to add to, delete or modify the information, the time when the information was accessed, and by whom. Secure operation of the EHRi also requires the logging of a wide variety of security related events such as the registration of new users, changes in user registration status, user session initiation and termination, changes in privacy policy or access control policy, changes in EHR data, changes in consent directives and many other events.

A.9.2 Analyse logs and detect intrusions

Description:

Analysis includes examination of all records that have been accessed by a user, all users who have accessed a patient/person's EHR, all users who have accessed EHRS of patient/persons at elevated privacy risk, and all users with suspicious patterns of use. A distinction must be

drawn between privacy and security auditing. A CPO would not typically be qualified to review security event logs for inappropriate access attempts, nor would a CSO typically be qualified to evaluate whether or not an authorised access was inappropriate or if the unmasking of PHI was reasonably necessary. This said, the service would operate in relatively the same manner; it would simply be accessed and used differently.

A.10 General Security Services

Four general security services are only briefly described in this section. Their detailed components are not specified in part because their implementation will be inextricably tied to jurisdictional variations in EHRi operations and in part because there is nothing in the design and deployment of the services which is unique to a healthcare environment. For example, malware protection will operate within the EHRi in essentially the same way it operates in the infrastructure of any industrial sector (banking, manufacture, government, etc.). For these reasons the general security services that follow are only briefly discussing within this document.

Service Components:

- A.10.1 Scan for and protect against Malware
- A.10.2 Secure Backup/Restoration of Data
- A.10.3 Data Archiving
- A.10.4 Secure Data Destruction

A.10.1 Scan for and protect against Malware

Malware protection is an important component of any infostructure that connects servers to open networks (and even a VPN in such a user environment as large and heterogeneous as is frequently encountered in healthcare must be considered open). It is assumed that malware security will run on all EHRi servers (see Assumption 7).

A.10.2 Secure Backup/Restoration of Data

Servers for large domain repositories and virtually all instantiations of the EHRi data repository will rely upon continuous backup facilities to ensure uninterrupted failover. Restoration of such data during disaster recovery or system roll-back requires secure key management protocols be in place that ensure continuous availability while at the same time ensuring that copies of EHRi data containing PHI are never stored in clear text.

The application of encryption is essential to the backup of EHRi data containing PHI.

A.10.3 Data Archiving

Health data must be retained for many years. Health record archiving guidelines are available from the Canadian Health Records Institute but no national standard exists for electronic record retention of PHI. Further policy development in this area is needed if archiving is to be implemented consistently across instantiations of the EHRi.

A.10.4 Secure Data Destruction

Simple utilities exists to securely wipe data from rewriteable media such as computer hard disks and their use must be rigorously enforced and secure methods for destruction of non-rewriteable media must be followed.

A.11 Other EHRi Common Services that Have an Impact on P&S

A.11.1 Session Management Service

Description:

The session management service manages user sessions and provides necessary context to the system beyond that pertaining to a single user request. A user session may contain information relevant to the session such as an access token, an authorisation token and other information that can provide efficient and secure access to users in a distributed application.

Rationale:

Maintaining contextual information during a user session in a distributed application environment helps provide efficient access to users. It also provides mechanisms for personalisation and for better response time and increased system efficiency by obviating the need to make repeated calls to the same functions for every user request.

The session management service component is made up of the following lower level services.

- Create/Open session
  This service creates a new session or opens an existing session. The “create session” service is called the first time the user sends a request to the system. The service creates a session object with the appropriate structures. This is then used by various services to store and access application or service level information. The session is encrypted. The “open session” service is called to access contents of an existing session.
- Modify Session
  This service is used to add or delete tokens in a session. For example, the "authenticate user" service uses this service to add the access token to the session after a user is authenticated.
- Secure session
  This is an internal service that is called by the create/open and modify session services to secure the session.
- Validate session
  This service is used to validate a given session to see if it is expired and other such validation checks.
- Close/Terminate session
  This internal service is used to close or terminate a session. It can be prompted by an explicit application call or by a request made through a cleanup batch service that is executed periodically. It will delete sessions that have been inactive for a configured period of time. Logout user function is an example of an explicit application call that will result in the termination of the session. A new request from the user will require the user to login, which will then result in the creation of a new session that will be associated with the user

Used by:

- A.2 User Authentication Services
- A.3.5 Authorise user
- Any other service that needs to store context information over the lifetime of a user session

Uses:

- A.9.1 Securely Log Events

Required Inputs:

- Tokens
- Application ID
- User ID
- Session ID

Response:

- Session ID
- Session object/string
- Token

Rationale:

The services in this session management service component provide features that result in system efficiency, and that support personalisation and other benefits in a distributed environment. Such services are usually found in tightly connected systems.

A.11.2 EHR Services

A.11.3 Mark EHR of patient/person at elevated privacy risk

Description:

This service component would enable the flagging of certain patient/person's PHI as being at a heightened risk of privacy breach. The component would be invoked either at the request of the patient/person or that of an authorised EHRi user. This protective measure may be used for privacy auditing purposes, whereby flagged records would automatically be audited, or to note specific information concerning the patient/person's EHR.

Used by:

- A.9 Secure Audit Logging Services
- A.11.4 P&S Notification Services
- A.3 Access Control Service
- A.2 User Authentication Services

Uses:

- A.9 Secure Audit Logging Services
- A.11.4 P&S Notification Services
- A.11.2 EHR Services

Required Inputs:

Patient/person ID

Type of flag (notification/alert flag, audit flag)

Text of notification/alert (could be entered as free text, but it would be preferable to use drop down list)

Response:

Text of notification/alert

Rationale:

This service would be used to increase the likelihood of locating instances of inappropriate access through ensuring that audits are conducted on the EHRs of individuals whose information is especially vulnerable to inappropriate access. This vulnerability may arise, for example, from the circumstances under which these individuals receive care or from their public stature. Also, the notification/alert component of the "Mark EHR of Patient/Person at Elevated Privacy Risk" service component would ensure that an individual's information is protected by whatever means necessary, while still allowing authorised clinicians to access the information. Such a feature would be imperative in the context of spousal or child abuse, rape, attempted homicide or other violent crimes where the perpetrator might try to locate the victim for malicious purposes.

A.11.4 P&S Notification Services

Notification of privacy officers and security officers of certain specific events is an essential feature of the P&S conceptual architecture. The general Notification Services are required to operationalise the following:

1. **Notify on override of consent directives** , used to notify an organisational privacy officer that a patient consent directive has been overridden; for example, to disclose data in a medical emergency (see section 7.6.11); and
2. **Notify on security event occurrence**, used to notify a security officer of a security breach; for example, an intrusion detection alert.

This service will be further defined through the EHRS Blueprint Evolution project and will be included in the next version of the EHRS Blueprint.

A.11.5 Messaging Services

Every user accessing the EHRi will be authenticated and logged in to a secure session. Session Management services will be responsible for maintaining the authenticated user identity post-login by means of a session token.

This service will be further defined through the EHRS Blueprint Evolution project and will be included in the next version of the EHRS Blueprint.

Appendix B Mapping P&S Requirements to P&S Services

All of the technical privacy requirements and technical security requirements listed in the Requirements document have been addressed by the P&S conceptual architecture's services. The tables below list each technical requirement and the services and service components that implement the requirement.

Table 5: Technical Privacy Requirements

Technical Privacy Requirements	Implemented by these service component(s)
Requirement 6 Associating Identified Purposes with Collected PHI	• Manage Consent-Related Business Rules (section Appendix AA.4.1)
Requirement 11 Recording Consent in the EHRi	• Manage Patient/Person Consent Directive (section Appendix AA.4.2)
Requirement 12 Associating Consent Directives with PHI in the EHRi	Messaging services must ensure that consent directives are made available to the recipient when transfers of data take place (especially relevant to inter-jurisdictional transfers). This might impact HL7 messaging constructs. Some jurisdictions will associate consent with groupings of data, others with specific "locked" or masked regions of data, still others with domain related data such as a lab test. The EHRi must support multiple ways of applying consent directives.
Requirement 13 Logging the Application of Consent Directives	• Log Consent Directives and Their Application (section Appendix AA.4.7). Includes: logging denial of access, logging consent override Messaging services must also ensure that recipients are notified of the existence of blocked or masked data.
Requirement 15 Recording Identity of Substitute Decision Makers	(Services recording changes in data must be able to record the identity of a substitute decision maker) • Register EHRi user (section Appendix AA.1.1)
Requirement 19 Logging Access, Modification and Disclosure	• Log access to data • Log changes to data
Requirement 21 Retaining Records	May impact design of archiving services – is archiving an EHRi service?
Requirement 22 Accuracy	(May impact design of user interfaces if direct web based access to the EHRi is permitted) • Digitally sign data, section Appendix AA.8.2 • Verify digital signature, section Appendix AA.8.3 • Digital Time Stamp and Digital Notary Service, section Appendix AA.8.4
Requirement 25 Amending Inaccurate or Incomplete Information	Although no specific P&S service exists to facilitate this requirement, the EHRi data model will allow for the recording of patients'/persons' challenge to the accuracy of their PHI.

Table 6: Technical Security Requirements

Technical Security Requirement	Implemented by these service component(s)
Requirement 17 Terminating User Access When Terminating Employment	• Suspend/Revoke user access function of Manage User Identity
Requirement 22 Disposing of or Reusing EHRi Equipment	• Secure Data Destruction (section Appendix AA.10.4)
Requirement 29 Protecting Against Malware	• Scan for and protect against (section Appendix AA.10.1)
Requirement 30 Securely Backing Up Data	• Secure Backup/Restoration of Data (section Appendix AA.10.2) • Data Archive (section Appendix AA.10.3)
Requirement 31 Encrypting PHI During Transmission	• Message Encryption , section Appendix AA.7.4
Requirement 32 Protecting Source and Destination Integrity During Transmission of PHI	• Digitally sign data, section Appendix AA.8.2 • Verify digital signature, section Appendix AA.8.3 • Message Encryption , section Appendix AA.7.4 Issues around multiple signatures, signatures covering parts of a message.
Requirement 33 Acknowledging Receipt of Transmitted PHI	• Send Acknowledgement of message receipt
Requirement 35 Disposing of Media Containing PHI	• Secure Data Destruction (section Appendix AA.10.4)
Requirement 36 Protecting Data Storage	• Database Encryption A.7.2 • Data Storage Encryption A.7.3
Requirement 38 Logging Transactions in the EHRi	• Log EHR transaction
Requirement 39 Logging of Changes to PHI in the EHRi	• Log Changes to Data
Requirement 41 Logging EHRi Transmissions of PHI	• Log message transmission
Requirement 43 Minimum Content of Audit Logs	• Log Access to Data • Log Changes to Data • Log EHR Transaction • Log message transmission • Log Denial of Access • Log Consent Override
Requirement 45 Logging Continuously	(Will impact implementation and operations but not service spec)
Requirement 46 Analysing Audit Logs to Detect Patterns of Misuse	• Analyse log – all users with suspicious patterns of use

Technical Security Requirement	Implemented by these service component(s)
Requirement 47 Analysing Audit Logs to Disclose Every Access To A Patient/Person's EHR	• Analyse log – all users who have accessed a patient/person's EHR • Retrieve unique identifier of patient/person
Requirement 48 Analysing Audit Logs to Disclose Every Access By A User	• Analyse log – all records accessed by a user
Requirement 49 Analysing Audit Logs for Patients/Persons At Elevated Risk	• Mark EHR of patient/person at elevated privacy risk • Analyse log – all users who have accessed EHRS of patient/persons at elevated privacy risk • Retrieve unique identifier of patient/person
Requirement 1 Securing Access to EHRi Audit Logs	(will have privacy related impact on design of authorisation services)
Requirement 51 Rendering Audit Logs Immutable	-- A variety of functional approaches, including: • Digitally sign data
Requirement 55 Assigning Identifiers to Users	• Generate unique identifier for user • Retrieve unique identifier of user
Requirement 58 Granting Access to Users by Role	(Will impact design of user registration and authorisation services) • Manage user role • Determine user access privileges • Register user • Retrieve unique identifier of user
Requirement 59 Selecting A Single User Role Per Session	(Will impact the design of authentication services)
Requirement 60 Granting Access to Users in Work Groups	(Will impact design of user registration and authorisation services) • Manage association between user and work group • Determine user access privileges
Requirement 61 Work Groups Do Not Override Roles	(Will impact design of authorisation services) • Determine user access privileges
Requirement 62 Timely Revocation of Access	• Suspend/Revoke user access function of Manage User Identity
Requirement 63 Granting Access By Association	(Will impact authorisation services) • Manage association between user and patient/person o Retrieve unique identifier of user o Retrieve unique identifier of patient/person • Determine user access privileges

Technical Security Requirement	Implemented by these service component(s)
Requirement 70 Restricting Connection Times to EHRi Applications	(Will impact session management) • Open session • Close session • Timeout session
Requirement 71 Robustly Authenticating Users	• Authenticate user
Requirement 76 Assigning Identifiers to Patient/Person	• Register patient/person • Generate unique identifier for patient/person
Requirement 79 Digital Signatures for Users	(many services are needed to issue digital signature certificates – unclear what role if any the EHRi will play in providing this) • Digitally sign data • Digitally sign message • Verify digital signature
Requirement 80 Validating and Preserving Digital Signatures On PHI	• Verify digital signature
Requirement 84 Reporting Security Incidents Involving the EHRi	• Notify on override of consent directive

Appendix C – Informational Consent

Purpose

This appendix outlines the differences between the types of informational consent models found in Canadian privacy legislation and health information legislation (the latter is sometimes called "health privacy legislation" or "health data protection legislation"). This appendix is intended to provide background information on informational consent to support the reader's understanding of the proposed privacy and security (P&S) conceptual architecture outlined in this document. The reader is reminded that the P&S conceptual architecture outlined in this document does not prescribe specific technologies, vendor products, and operating system environments. In a similar vein, this appendix does *not* prescribe specific methods for implementing informational consent requirements outlined in legislation.

General Discussion on Informational Consent Models in Canadian Legislation

Informational consent refers to a patient's/person's permission for the collection, use or disclosure of his or her personal information. It should be distinguished from *consent for healthcare services or treatment*, which relates to the permission that a patient/person gives before receiving healthcare services or treatment, such as receiving nutrition counselling or physiotherapy, or before undergoing a specific healthcare procedure, such as donating blood or undergoing diagnostic tests or a surgical procedure. Health information legislation deals primarily with *informational* consent although it is often conflated with consent for healthcare services or treatment since the delivery of such services or treatment invariably requires the collection, use or disclosure of PHI.

In Canada, there are four separate health information statutes, each outlining an informational consent model that applies to most organisations and individuals which collect, use or disclose health information that identifies a patient/person. (Such information is known as "identifying health information" or "personal health information"; Infoway uses the latter term in this document, which is abbreviated to "PHI"). The four Canadian health information statutes do *not* impose privacy and security rules on the collection, use or disclosure of health information in anonymous or de-identified form, but all four statutes apply to PHI held in a variety of forms (e.g. paper, electronic, photographic and verbal). The four Canadian health information statutes are:

1. The *Personal Information Protection Act*, Alberta;
2. The *Personal Health Information Act*, Manitoba;
3. The *Health Information Protection Act*, Saskatchewan; and
4. The *Personal Health Information Protection Act,* Ontario.

All of the health information statutes listed above are predicated in some form on internationally recognised fair information principles (such as the CSA Model Code for the Protection of Personal Information). In addition, all four statutes provide a means for the independent review and resolution of complaints regarding the handling of PHI, which is typically done through the provincial Information and Privacy Commissioner (as is the case in Alberta, Saskatchewan and Ontario) or the provincial Ombudsperson (as is the case in Manitoba). (Individuals with privacy complaints about the handling of their PHI may also have the right to complain to their Information and Privacy Commissioner in British Columbia, Quebec, Prince Edward Island, Newfoundland and Labrador and all three territories as well as to an Ombudsperson in New Brunswick and a Freedom of Information and Privacy Review Officer in Nova Scotia, but this right does not exist through separate health information legislation in these jurisdictions).The statutes also give individuals a right of access to their own PHI (with limited exceptions) and a right to request corrections to their PHI. The issue of patient access to PHI is discussed in greater detail later in this appendix. In the meantime, there are important differences between the informational consent models outlined in the above legislation and other Canadian privacy laws, which are discussed below.

The Alberta and Manitoba legislation listed above rely on a "no-consent" model, which means that healthcare providers do not need to obtain an individual's permission for the collection, use or

disclosure of his or her PHI in order to deliver healthcare services and treatment to that individual, provided other conditions in the legislation are met, including the requirement for healthcare providers to inform the individual of the purposes for which his or her PHI is being collected, used and disclosed (e.g. the notice requirement).[112] The notice requirement is typically met through written notices such as posters or pamphlets. Healthcare providers in Alberta and Manitoba may still be bound by privacy provisions in other legislation, and they are also required to obtain an individual's consent for the use and disclosure of his or her PHI for activities other than those for which the information was collected and are permitted or required by law. Also, in Alberta, the *Health Information Act* initially included a requirement under section 59 that health information custodians needed to obtain express consent for any sharing of personal health information by electronic means. The provision was repealed in 2003, a year after the Act went into effect, following the receipt of several complaints from physicians and other healthcare providers who expressed serious concerns that the provision impeded care delivery and imposed an unnecessary administrative burden on their practices.

In Saskatchewan, the *Health Information Protection Act* relies on a "deemed consent" model, which means that an individual is deemed to have consented to the collection, use and disclosure of his or her PHI when he or she seeks healthcare services and treatment from healthcare providers in the province. Like the "no-consent" model, healthcare providers in Saskatchewan are required to inform individuals of the purposes for which their PHI is being collected, used and disclosed and they may also be bound by privacy provisions in other applicable legislation.[113]

The differences between a "no-consent" model and a "deemed consent" model are often a cause for confusion. A "no-consent" model means that healthcare providers do not require an individual's consent for the collection, use or disclosure of his or her PHI provided that other conditions in applicable legislation are met. A "deemed consent" model, by contrast, actually *requires* an individual's consent but deems individuals to have granted the necessary consent for the use of their PHI for the purpose of delivering healthcare services and treatment, provided other conditions in the Saskatchewan *Personal Health Information Act* are met. For this reason, a "deemed consent" model is sometimes described as a "legal fiction." From a patient's/person's point of view, however, both models manifest themselves in the same fashion – e.g. a patient/person is not asked for, nor may he or she withhold or revoke his or her permission to collect, use or disclose his or her PHI for the delivery of healthcare services and treatment, either because the patient's/person's consent is not needed (e.g. the "no-consent" model) or because consent is required and is already deemed to have been given (e.g. the "deemed consent" model).

In Ontario, healthcare providers can obtain either "express consent" or "implied consent" to collect, use or disclose an individual's PHI for the delivery of healthcare services and treatment provided that they also comply with other conditions in the *Personal Health Information Protection Act*. Some of these conditions include:

1. Implementing information practices that comply with the Act (section 10);
2. Taking reasonable steps to ensure that PHI under the custodian's custody or control is protected against theft, loss, unauthorised use or disclosure, and unauthorised copying, modification or disposal (section 12.1);
3. Notifying individuals at the first reasonable opportunity if their PHI is stolen, lost or accessed by unauthorised persons (section 12.2);
4. Designating a contact person to facilitate: the custodian's compliance with the Act; ensuring that all agents are informed of their duties under the Act; responding to inquires from the public about the custodian's information practices; responding to requests from individuals

[112] See the Alberta *Health Information Act*, R.S.A. 2000, c. H-5, s. 22(3)(a) and the Manitoba *Personal Health Information Act*, R.S.M. 1997, c. 51 – Cap. P33.5, s.15(1)(a).

[113] See the Saskatchewan *Health Information Protection Act*, c. H-0.021 as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; and 2003, c.25, s. 9.

to access or amend their PHI; and receiving complaints from the public about alleged infractions of the Act or its regulations (section 15.3); and

5. Providing a written public statement that: provides a general description of the custodian's information practices; describes how to contact the custodian's contact person outlined in section 15 of the Act; describes how an individual may request access to his or her PHI and request a correction to his or her PHI; and describes how to make a privacy complaint to the custodian and to the Ontario Information and Privacy Commissioner (section 16).

These conditions are designed to ensure that consent is "knowledgeable", regardless of whether it is expressly obtained or implied. Consent is considered knowledgeable under section 18(5) of the *Personal Health Information Protection Act* if it is reasonable in the circumstances that the individual 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 an individual: (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, alternatives 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.

Implied consent means that healthcare providers may assume that an individual consents to the collection, use or disclosure of his or her PHI for the delivery of healthcare services and treatment, provided the conditions listed above in the *Personal Health Information Protection Act* are achieved. By contrast, *express consent* (and not "expressed consent") means that an individual is expressly asked for his or her permission to collect, use or disclose his or her PHI before any information collection, use or disclosure may take place. This is often achieved through a written informational consent form that is signed by the individual. Sometimes express consent is also incorporated into existing "consent for treatment" or "consent for healthcare service" forms. Express consent can also be obtained verbally. (It is a common misperception that express consent can only be obtained in writing). With limited exceptions, an express consent model governs the collection, use and disclosure of PHI in Quebec for the delivery of healthcare services and treatment. These rules are contained in the province's public sector privacy legislation (and not in separate health information legislation).

Finally, for those jurisdictions for which there is no specific health information legislation in effect – for example, British Columbia, Quebec and the Atlantic provinces – informational consent rules for PHI vary. As noted earlier, express consent is generally required in Quebec for the collection, use and disclosure of PHI for the delivery of healthcare services and treatment, with limited exceptions. In all other jurisdictions, a "no-consent" model supported by specific notice requirements is in place. Individuals wishing to learn more about the informational consent rules in effect in these jurisdictions should consult the provincial or municipal Freedom of Information and Protection of Privacy Acts (FOIPPA) or other relevant legislation.

Appendix D – Candidate Conceptual Data Models

The two figures that follow (Figure 20 and Figure 21) show several data classes[114]:

- patient/person, including attributes such as a unique client identifier (ECID),
- Public identifier (PIDs) such as health card numbers, etc. assigned to patients/persons (where each patient/person has zero or more PIDs.
- Federated identifier (FIDs) that are assigned to patients/people for purposes such as mapping identifiers from one jurisdiction to another.
- Pseudonymous identifier (Pseudo IDs) that are a specialisation of FIDs and that are used in research to allow longitudinal study of data from an otherwise anonymous patient/person (i.e., that allow a research to gather data over time on "patient X"),
- EHRi user, including attributes (among many other not specified) such as EHRi user ID,
- regulated healthcare provider – a specialisation of EHRi users – who each have a professional role,
- POS system instance IDs,
- Organisation IDs,
- professional role; a class of possible roles that can be assigned to EHRi users for the purposes of access control,
- EHRi role; a class of possible roles that can be assigned to EHRi users for the purposes of access control (examples include physician, dentist, pharmacist, patient/person, substitute decision maker, researcher, etc.),
- EHRi role mapping: whereby a set of POS system roles is mapped into a set of EHRi roles or where a set of roles in one jurisdictional EHRi implementation is mapped to those in another jurisdiction,
- discretionary access conveyance; i.e., where one healthcare provider confers access to a specific patient/person's EHR upon another healthcare provider (see 7.5.5),
- information security policy, and
- Information security domain.

[114] The authors are indebted to Doug Williscroft and his colleagues from the BC Ministry of Health Services for an earlier version of a P&S data model on which the current diagrams are loosely based.

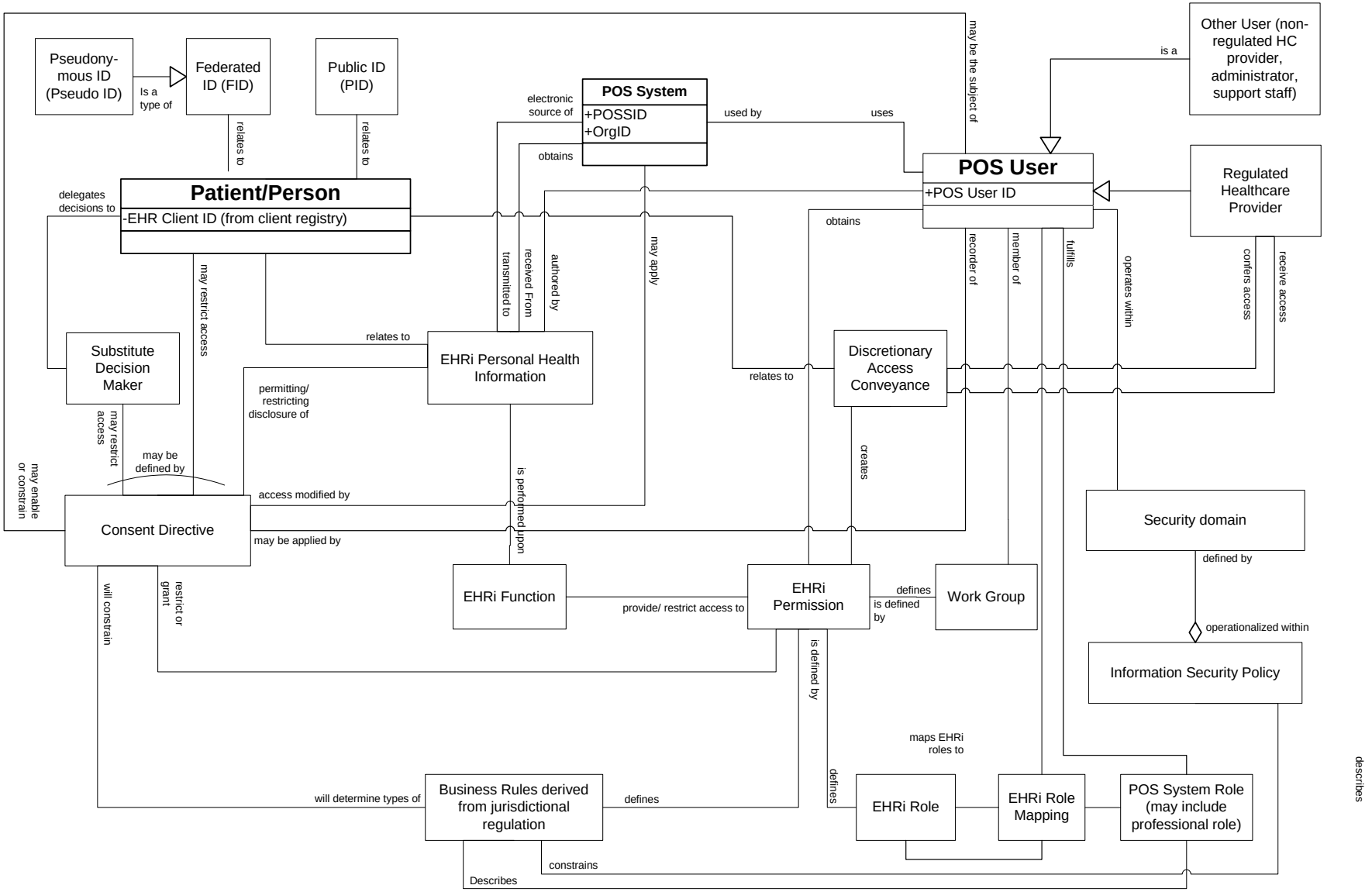

Figure 20 Conceptual Data Model for Organisation Trusted User Management

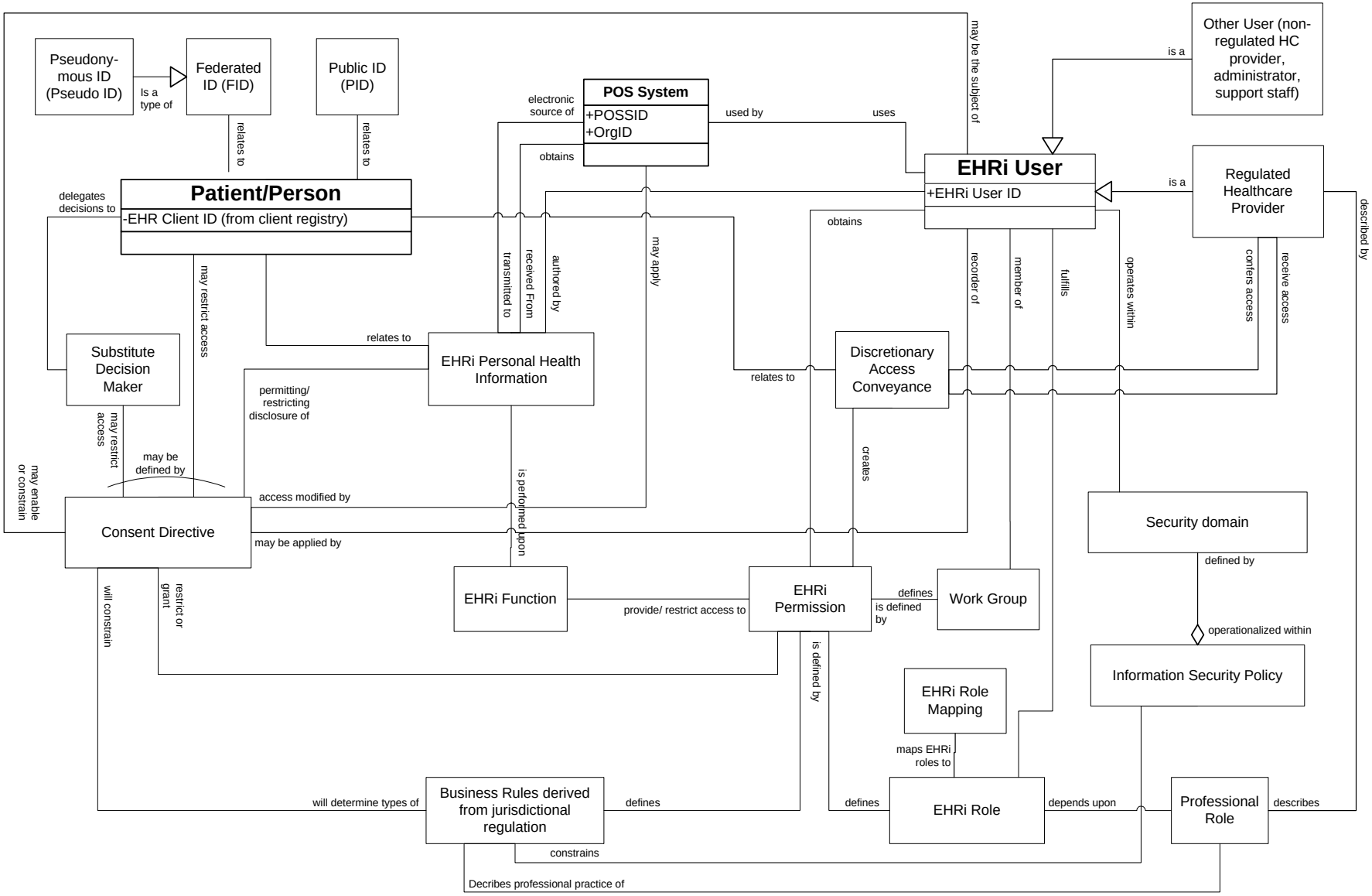

Figure 21 Conceptual Data Model for EHRi Trusted User Management

Acknowledgements

Infoway is proud to have had the opportunity to sponsor and deliver the Privacy and Security Conceptual Architcture project. Initiated in June of 2004, the project team has worked with Canadian stakeholders to engage and obtain feedback on the Privacy and Security Architecture.

Infoway would like to thank all stakeholders who participated and engaged in a collaborative spirit in the different workshops and web casts conducted in January and May 2005.

The members of the Privacy and Security Architecture team gratefully acknowledge the valuable insights and feedback of the experts and jurisdictional, providers and vendors representatives listed below.

The presence of any name in the lists that follow should not be construed as an endorsement by that individual of the content of this or any other Infoway document.

Alec Campbell
Executive Director, Privacy Policy and Assessment
Office of the Corporate Chief Information Officer, Government of Alberta

Hugh Ellis
Principal
Cinnabar Networks Inc., Ottawa

Claude Vigeant
Président
OKIOK, Laval, QC

Steven Johnston
Office of the Privacy Commissioner of Canada

David H. Flaherty
Adjunct professor in political science and consultant
University of Victoria

Dr. Kathryn J. Hannah
Adjunct Professor
Department of Community Health Sciences
Faculty of Medicine, University of Calgary

Marc-André Léger
Canada rep to SC27 and PhD student
University of Sherbrooke

Denis Protti
Professor
University of Victoria's School of Health Information Science

Don Willison
Assistant Professor, Clinical Epidemiology and Biostatistics Associate
Centre for Health Economics and Policy Analysis (CHEPA) Scientist
Centre for Evaluation of Medicines

Doug Williscroft
Electronic Service Delivery Architect

Standards and Architecture Branch
BC Ministry of Health Services

Gerry Bliss
EHR Privacy Consultant
Standards and Architecture Branch
BC Ministry of Health Services

Peter W. Durrant
Director - Aggregated Health Information Project
Director, Knowledge Integration & Development
BC Ministry of Health Services

Gregg Danderfer
A/Manager, Data Access Services
Information Resource Management
Knowledge Management and Technology Division
BC Ministry of Health Services

Brian Hamilton
Team Leader, Privacy & Security
Alberta Health & Wellness

Nick Giesinger
Director, Technical Architecture and Database Services
Health Information Solutions Centre
Saskatchewan Health

Randy Brunet
Legal counsel
Health Information Solutions Centre
Saskatchewan Health

Dave Langen
Security Officer (Architect)
Manitoba Health

Carol Appathurai
Director
Health Information Privacy and Sciences Branch
Integrated Policy and Planning Division
Ontario Ministry of Health and Long-Term Care

Michele Sanborn
Manager- Health Information Privacy Unit
Health Information Privacy and Sciences Branch
Integrated Policy and Planning Division
Ontario Ministry of Health and Long-Term Care

Pat Jeselon
Director, Liaison & Coordination
Broader Health Sector, Ontario e-Health Office
Ontario Ministry of Health and Long Term Care

Brendan Seaton
Chief Privacy & Security Officer

Ontario Smart Systems for Health Agency

Danna Dobson
Executive Director Standards Management and Business Integration
EHR Proj exec lead
Ontario Smart Systems for Health Agency

Jane Dargie
Director, Privacy
Ontario Smart Systems for Health Agency

Dr. Marion Lyver
Ontario Smart Systems for Health Agency

Gurjeet Dosanjh
Ontario Smart Systems for Health Agency

Mel Cassalino
Ontario Smart Systems for Health Agency

Mel Casalino
Privacy Consultant
Ontario E-Health Office

Fred Carter
Policy and Information Technology Analyst
Information and Privacy Commissioner / Ontario

Patrick Lo, CISSP
Vice President, Privacy, Security and Ethics
OntarioMD

Dieter Pagani
Director of ITS
Nova Scotia Department of Health

Michelle L. Gignac
Acting Manager
Information Access and Privacy Unit
Nova Scotia Department of Health

Michael Muise, CISSP
IT Security Coordinator
P.E.I. Dept of Health

Lucy McDonald
Director, Privacy and Communications
Newfoundland & Labrador Centre for Health Information

Tom King
Project Manager - Health Information Network
Newfoundland & Labrador Centre for Health Information

Marc Paradis
Business Analyst
Yukon Dept of Health & Social Services

LCol Jim Kirkland
Chief Information Officer, Federal Healthcare Partnership
Federal Healthcare Partnership

Philippe Tousignant
Senior Policy Analysist
Privacy Policy Division
Health Canada

Nicole d'Avignon
Senior Policy Analysist
Privacy Policy Division, Health Canada

Eric Ward
Legal Counsel
Privacy Policy Division, Information
Analysis and Connectivity Branch, Health Canada

Raymond D'Aoust
Assistant Commissioner
Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Denis Morency
Consultant
Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Dr. Jay G.Mercer, MD, CCFP
Physician and consultant
Canadian Medical Association
Association médicale canadienne

Bev Allen, BSP
Assistant Professor of Pharmacy
Structured Practice Experiences Coordinator
College of Pharmacy and Nutrition
University of Saskatchewan
Canadian Pharmacists Association
Association des pharmaciens du Canada

Marie Berry
Pharmacist
Canadian Pharmacists Association
Association des pharmaciens du Canada

Lori Forand, (RN, BN, MCS)
Nursing Practice Consultant, Calgary Health Region
Canadian Nurses Association
Association des infirmières et infirmiers du Canada

Dr. David Kogon
Dentist
Canadian Dental Association
Association dentaire canadienne

- **Vendor representatives**

  Suneel Bhargava
  Accenture

  Annie Thibodeau
  Coordonnatrice aux communications et événements
  AITS

  Danielle Blanchard
  Directrice générale associée
  AITS

  Steven A. Huesing
  CEO
  Canadian Healthcare Information Technology Trade Association

  Constantine Karbaliotis
  CGI

  Mark Switzer
  Executive Consultant
  CGI

  Yogen Appalraju
  Vice-President Security Solutions
  Emergis

  Derek Browne, CISSP, ISSAP
  Senior Security Consultant, CISO
  Emergis Inc.

  Bruce Rosenberg MD
  President
  Healthscreen Solutions Inc.

  Christine Callahan
  Corporate Relations
  HIPAAT Inc

  Kelly Callahan
  Special Projects
  HIPAAT Inc.

  Steven Meyer
  Chief Engineer
  HIPAAT Inc.

  Terry Callahan
  Managing Director
  HIPAAT Inc.

  Marc Bage, Ph.D., ing.
  Chercheur / Researcher

Institut international des télécommunications / International Institute of Telecommunications
Caren Adno
Vice President
ITAC

Bob McKeever
President
McKeever's Software Wizardry Limited

John Weigelt, CISSP, CISM
Chief Security Advisor
Microsoft Canada

Trevor Cook
Industry Architect – Healthcare
Microsoft Services - Canada

Carman Baggaley
Office of the Privacy Commissioner of Canada

Jean Boilard
Président
Omni-Med.com

Jean-Guy Dupuis
VP Technologies
Omni-Med.com

Michael Craig
Vice President
Orion Canada Ltd

Predrag Zivic, CISSP, CISM, ISO
COO
Scienton

David Fusari
Director, Product Architecture
Sentillion Canada

John Appleton
Director Product Management
Sentillion Canada

Cajetan Amaral
Technical Architect
Sierra Systems

Georges Lysenko
Principal
Sierra Systems

Blake Sutherland, P.Eng.
Director, Product Management
Third Brigade Inc.

Mauro Lollo
VP and CTO
UNIS LUMIN Inc.

Robert S. Miller
Technology Architect
Sun Microsystems

Sarah Graham
Regional Vice President
Sentillion Canada

Blake Sutherland, P.Eng.
Director, Product Management
Third Brigade Inc.

Bryn Jones
President
ICDL Canada

- **P&S CA Project Team**

  The Privacy and Security Conceptual Architecture project team itself deserves a lot of credit for all the hard work that was accomplished in defining a first pan Canadian validated vision of privacy and security services required for an interoperable EHR. This body of work represents a substantive investment in intellectual capital that will be of service to the Canadian health informatics community. Our special thanks go to:

  - Mr. André Boudreau, Boroan Inc.
  - Ms. Margot Brown, Director Adoption, Canada Health *Infoway*
  - Mr. Stephen D'Silva, Silvacorp Inc.
  - Mr. Ross Frazer, Sextant Software Inc.
  - Ms. Cindy Hoffman, Director of Corporate Communication, Canada Health *Infoway*
  - Mr. Don MacPherson, Anzen Consulting Ltd
  - Mrs. Mary A. Marshall, Mary A. Marshall Professional Corporation
  - Mr. Stan Ratajczak, Director IT Security and Privacy, Canada Health *Infoway*
  - Ms. Sari Schapira, Project Coordinator, Canada Health *Infoway*
  - Ms. Miyo Yamashita , Anzen Consulting Ltd.

  Our thanks go also to everyone who has provided their leadership, support, help, and feedback in the course of the project, namely;

  - Mr. Dennis Giokas, Chief Technology Officer, Canada Health *Infoway*
  - Mr. Luc Bouchard, IPM Group Director, iEHR and Infostructure programs, Canada Health *Infoway*
  - Mr. John Burns, Senior VP Investment Programs Management, Canada Health *Infoway*
  - Mr. Robert Caron, SAG Group Director, Infostructure, iEHR and Telehealth, Canada Health *Infoway*
  - Mr. Trevor Hodge, Senior VP Investment Strategy and Alliances, Canada Health *Infoway*
  - Mr. Don Sweete, National & Atlantic Alliance Executive, Canada Health *Infoway*
  - Mr. Mike Sheridan, Chief Operating Officer, Canada Health *Infoway*
  - Mr. André Laurendeau, Director Information Management and Technology, Canada Health *Infoway*
  - Mr. Jose Mussi, SAG Group Director, Clinical Programs, Canada Health *Infoway*

- Ms. Elizabeth Newscomb, User Support and Toolkit Document Coordinator, Canada Health *Infoway*
- Mr. Ron Parker, Director Architecture , Canada Health *Infoway*
- Mr. Brian Philbin, Chief Financial Officer, Canada Health *Infoway.*

References

Infoway

- Canada Health Infoway, *EHRS Blueprint: An Interoperable EHR Framework*, July 2003
- Canada Health Infoway, *Electronic Health Record Privacy and Security Use Cases,* 2004
- Canada Health Infoway, *Electronic Health Record Privacy and Security Requirements,* 2005
- Canada Health Infoway, *Electronic Health Record Privacy and Security Standards Review,* 2005

Privacy

- *Tees Confidentiality Model: Towards a Conceptual Framework for Authorisation*, J. Longstaff, et al, March 2004.

Security

- *ISO/IEC 17799 – Code of Practice for Information Security, 2005*

Policy

- *Pan-Canadian Health Information Privacy And Confidentiality Framework*, Advisor Council on Information and Emerging Technologies (ACIET), January 27, 2005 www.hc-sc.gc.ca/ohih-bsi/theme/priv/index_e.html

Other

- ISO/IEC 10731, *Information technology -- Open Systems Interconnection -- Basic Reference Model -- Conventions for the definition of OSI services*
- ISO/IEC 10731, *Information technology -- Open Systems Interconnection -- Basic Reference Model -- Conventions for the definition of OSI services*
- IETF/RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*
- e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment, Enrico Coiera, Journal of the American Informatics Association, vol. II, number 2, March/April 2004, page 129.