Business and Architecture Considerations for Interoperable Consent Solutions

A DISCUSSION DOCUMENT

March 21, 2012
Copyright © 2012 Canada Health Infoway

This document may be reproduced or transmitted; however, no alterations, deletions or substitutions may be made to the text without the prior written consent of Canada Health Infoway (Infoway). Portions of this document that are used or quoted are to cite Infoway as the source.
Note to readers

Readers should keep in mind the following when reviewing this document:

1. This document is a reflection of consultation with stakeholders (see Appendix A for a list of stakeholders) on consent management solutions. It is not an endorsement by stakeholders or Canada Health Infoway of any particular approach or approaches to consent management solutions; rather it is a thoughtful discussion of the issues related to consent management solution development and deployment.

2. The clinical/workload implications associated with the development or deployment of a consent management solution are important but outside the scope of this project.

3. It must also be stressed that this report is not a primer on either privacy or consent management issues. It assumes a level of understanding of these topics.
Executive Summary

In response to interest expressed by its stakeholders, Canada Health Infoway embarked on the Consent Management Project in December 2010. This project is intended help jurisdictions meet their various legislative and policy requirements regarding consent by providing them with information related to consent management solution choices, planning and implementation.

This document is the key project deliverable. With the generous help of a Working Group that included representation from six jurisdictions, this project was able to gain a solid understanding of consent solutions in use today in several Canadian jurisdictions and to explore policy, operational, technical and system design issues that factor into any discussion of a consent management solution for the EHR environment. The report was developed with extensive input from this Working Group and further informed by discussion with a broader stakeholder Advisory Group. The Advisory Group, which included representation from the clinician community, emphasized that healthcare providers should be engaged as jurisdictional consent management decision-making moves forward.

BACKGROUND

Information consent is a complex topic. The express consent of the individual is generally not required for the collection of personal health information (PHI) to provide care and treatment. In fact, the collection of this information is required to provide care. The legislative frameworks in most jurisdictions, however, permit individuals to express their wishes to limit use and/or disclosure of their personal health information for some purposes. These wishes must be documented, communicated and respected throughout the individual’s interaction with the health system, in both paper and electronic systems. The exercise of these wishes however, is constrained by jurisdictional and organizational rules.

Consent directives, a term used to refer to the expression of an individual’s wishes, may include direction to permit, withhold, withdraw, change or revoke consent to collect, use or disclose personal health information. While relatively few consent directives are in place at this time, consent management functionality is a legislated requirement and must be part of electronic health record (EHR) systems.

Jurisdictions are at different stages in the development and implementation of the various components that make up their EHR systems. Many jurisdictions began the build of their EHR system by deploying a single clinical domain repository with its own consent solution based on the technical capability available at the time. Successive domains were released in a similar manner. The various point of service (POS) solutions within the jurisdictions were also implemented at different times and with different consent functionality. As result,
jursdictions are now faced with complex consent management environments, most of which are not interoperable.

BUSINESS CONSIDERATIONS AND REQUIREMENTS

This paper discusses topics which are of particular importance when considering consent management solutions within this complex environment, and it identifies common business and architectural requirements that need to be included in any generic consent management solution.

For example, the paper discusses the granularity of information that is masked by a consent management solution. Currently, if an individual wishes to mask certain information, typically the entire record in the clinical domain is masked or rendered inaccessible. Due to a number of factors discussed in the paper, this is viewed at this time to be the most effective and safest means for ensuring that the individual’s wishes are respected. It is recognized however, that masking only that information that is of concern to a patient, rather than masking all of the person’s health information, or all laboratory tests or other large masses of information, gives the individual more privacy choices. Since policies in this area may change over time, a consent management solution will require flexibility to ensure that it can accommodate the current situation as well as potential future changes.

Integration of a consent management solution (CMS) with other jurisdictional systems such as identity management systems, provider registries and client registries, is another topic that is explored. A related and more complex consideration is the integration of consent management in various EHR and POS systems which may each include different CMS functionality.

Other business considerations addressed in the paper relate to the following topics:

- Consent directive storage, management and enforcement
- Overrides
- Inter-jurisdictional movement of data
- Communications
- Future proofing
- Ownership
- Governance

The paper sets out 28 high level business requirements that reflect needs identified by the participating jurisdictions in the following areas:
• Access and authorization to consent management solution
• Solution configuration
• Data capture, storage, retrieval and enforcement of directives
• Reporting and analytics
• Maintenance of historical data and archiving
• Notification and alerts
• Conflict identification/ resolution
• Overrides
• Logging
• Viewing of data

These business requirements provide a concrete sense of what a consent management solution needs to be able to support. They guided the development of the rest of this document, and they may be useful to individual jurisdictions as they consider acquiring or developing consent management solutions.

ARCHITECTURE CONSIDERATIONS AND REQUIREMENTS

In the architecture sections of this document, architectural options and considerations for a solution are presented with the goal of facilitating the design or acquisition and deployment of interoperable CMSs.

Three generic consent solution deployment models inspired by the Infoway Privacy and Security Conceptual Architecture, current CMS deployments and new deployment model trends, are set out and their key features described. Each model assumes a common set of CMS capabilities for the capture, storage, management of consent policies and enforcement of consent directives. The models are:

1. Central consent management
   • This model features a centralized consent repository
   • It has a centralized CMS functionality within the Health Information Access Layer (HIAL) operating within a Services Oriented Architecture (SOA)
   • A CMS web interface supports the capture and management of directives

2. Consent management as part of a clinical domain repository
   • Currently this is the most common deployment model reported across jurisdictions in Canada
Each domain has a consent management solution - consent management is integrated within the clinical domain solution.

Capture, storage and enforcement of consent directives take place within the clinical domain solutions.

3. Federated consent management

- CMS components may reside in a number of locations and can work together in various ways -- multiple instances of the same CMS may be distributed across various locations or the various functions of a comprehensive solution may be dispersed.
- If consent transactions take place in a number of Consent Repositories dispersed across the jurisdiction, the repositories synchronize consent directives and consent management rules. Enforcement may be provided by a single common HIAL or synchronized multiple regional HIALs.
- If domain-specific CMSs are federated into an overall jurisdictional solution, the enforcement and management of directives may occur within the clinical domain CMS.

The CMS must interconnect with other parts of the EHR infrastructure such as the HIAL, and Client, Location and Provider Registries, and therefore, communication interfaces must be built and configured between these systems and the CMS. Standards are required for a CMS to communicate with these other systems. A high level review was conducted of standards in Canada and other jurisdictions and identified several approaches that could serve as potential candidates. The paper also identifies 22 functional architectural requirements applicable to a CMS notwithstanding the deployment model or consent model used by a jurisdiction. It also explores the interrelationship between the CMS and the various external systems with which it must interface and sets out architectural considerations related to each.

SUMMARY

As stated above, information consent is a complex topic. It involves the legislated rights of individuals to express wishes respecting their personal health information. It also involves a jurisdiction’s policy framework; governance structure; operational processes; current and future state EHR architecture; and choices around level of granularity, masking and overrides.

As more and more EHR components are implemented and subsequently integrated into the interoperable EHR, the existing domain based solutions which were built to meet the needs
of specific projects may become increasingly difficult to manage and sustain. For this reason, this project sees value in consistency between consent management solutions. It was recognized that a common set of requirements which accommodate the wide range of jurisdictional needs could help achieve interoperability at the jurisdictional level and in the longer term, across jurisdictions.

This document identifies certain challenges to deploy a CMS from a business, technical and architectural perspective. In the process of producing this report, however, there has been remarkable convergence amongst project participants regarding the nature of the consent management challenges to be solved and the approaches to solving them.

From a high level technical and architectural perspective, based on the information reviewed to date, the technological means exist for jurisdictions to acquire, or design and develop a CMS. Several vendors of CMS solutions were consulted during the course of this project and indicated that their current products meet the majority of the business requirements identified in this report. That being said, a common set of flexible specifications would facilitate interoperability. Such commonality could also make Canada a more attractive customer in the global marketplace for consent solutions.

As jurisdictions evolve their approach to consent management, the development of a transition plan or roadmap can help assess impacts, risks, as well as business and architectural considerations. This can assist in the determination of how best to incrementally implement, or transition between, one CMS deployment model and another.

Several jurisdictions have identified consent management as a top priority to meet their respective legislative obligations. It is our hope that this report will provide the foundation, so that as jurisdictions accept this challenge, they will have a sense of the scope and the steps required to move forward.
Table of contents

Note to readers................................................................. 3
Executive Summary........................................................... 4
    Background ..................................................................... 4
    Business considerations and requirements ....................... 5
    Architecture considerations and requirements ................ 6
    Summary ....................................................................... 7
1. Introduction....................................................................... 11
    Consent Management Project background ....................... 11
    Guiding Principles .......................................................... 13
    Project Assumptions ........................................................ 14
    Purpose of this Document ............................................... 14
    Terminology .................................................................. 15
2. Overview of current jurisdictional consent solutions .......... 16
    Legislative Overview ...................................................... 16
    Consent Management Solutions Overview ....................... 17
    High Level Overview By Jurisdiction (Presented Alphabetically) ........................................................................... 17
    overview of consent management Outside of Canada .......... 23
    Consent directives in other industries ............................... 23
3. Business considerations.................................................. 25
    Granularity and Masking .................................................. 25
    Storage Of Consent Directives ......................................... 28
    Consent Directive Enforcement ......................................... 29
    Managing consent directives ............................................ 30
    Overrides ....................................................................... 30
    Integration ..................................................................... 31
    Inter-jurisdictionAL movement of data .............................. 33
    Importance of communication ......................................... 34
    Future proofing ................................................................ 34
    Ownership .................................................................... 35
    Framework for managing consent (governance) ................. 36
4. Health System Use............................................................ 38
    Business considerations .................................................. 39
5. Consumer Health Solutions .............................................. 40
    Business considerations .................................................. 40
6. Business requirements for a consent management solution ................................................................................. 42
7. Architecture: An introduction .......................................... 51
    Projects that Have informed the CMS Architecture Considerations ........................................................................... 51
8. Architectural deployment models and considerations ........ 53
    Centralized Consent Management Deployment Model ........ 54
    Domain-based Consent Management Deployment Model .... 56
    Federated Consent Management Solution Deployment Model ................................................................. 58
    CMS deployment model comparison ................................ 62
    CMS integration to point of service applications ................ 70
    Consideration for a design/deployment roadmap ................ 72
9. Consent Management Design Requirements ....................... 74
    Architectural .................................................................... 74
    Consent Management Standards ..................................... 74
    Operational ..................................................................... 74
10. Functional Requirements of a Consent Management Solution ................................................................................. 77
11. CMS Architectural Considerations ................................................................. 80
    Health Information Access Layer (HIAL) ....................................................... 80
    Client Registry (CR) ....................................................................................... 81
    Provider Registry (PR) .................................................................................... 82
    Location Registry (LR) .................................................................................... 83
    Identity and access management (IDAM) .......................................................... 84
    Audit .................................................................................................................. 85
    Co-Existence of multiple consent models ....................................................... 85

12. Concluding statements .................................................................................... 87

Appendix A: Acknowledgements and list of Steering Committee, Working Group and Project Advisory Group Members ......................................................... 88

Appendix B: Glossary ............................................................................................ 92

Appendix C: The Process Lifecycle of a Consent Directive .................................... 101
    Capture .............................................................................................................. 101
    Create .............................................................................................................. 102
    Read ............................................................................................................... 103
    Update .......................................................................................................... 104
    Deactivate ..................................................................................................... 104
    Overrides ....................................................................................................... 105

Appendix D: International References ................................................................ 106

Appendix E: Related Initiatives ........................................................................... 110
    Privacy and EHR Information Flows in Canada: Common Understandings of the Pan Canadian Health Information Privacy (HIP) Group .................................. 110
    iEHR Technical Project I (TECH I) .................................................................. 110
    iEHR Technical Project II (TECH II) ............................................................... 111
    Privacy and Security Conceptual Architecture .................................................. 111
    Electronic Health Record Solution (EHRS) Blueprint ......................................... 111

Appendix F: Inventory of existing standards ......................................................... 112
    Message Based Standards .............................................................................. 112
    Clinical Document Architecture (CDA) ............................................................ 112
    Extendible Access Control Markup Language (XACML) ............................... 112
1. Introduction

The right of an individual to express their wishes with respect to their personal health information (PHI) is an element of most jurisdictions’ health information privacy or eHealth legislation. While individuals avail themselves of this right on a relatively infrequent basis, these instructions must be documented, communicated and respected throughout the individual’s interaction with the health system. Consent directives may be applicable at any point in the individual’s interaction with the health care system.

Some jurisdictions have already made headway in implementing consent management features in their electronic health record (EHR) applications. For the most part, based on input from participants in this project, these solutions currently have limited functionality and are not interoperable across EHR system components within a jurisdiction, or from one jurisdiction to another. Given the complexity and expected future integration of information systems within and across jurisdictions, the introduction of automated consent management solutions (CMS) merits consideration.1

CONSENT MANAGEMENT PROJECT BACKGROUND

In early summer 2010, jurisdictions were informally canvassed with respect to their interest in a consent management project. Representatives expressed interest indicating that as system integration becomes a reality; inter-jurisdictional movement of information becomes more frequent; personal health records and public sector consumer health platforms begin to be used; and health system use of information increases; the ability to manage consent wishes would become increasingly important.

In December 2010, Canada Health Infoway embarked on the Consent Management Project to explore business and architectural considerations of a technical consent management solution. Jurisdictions that are still in formative stages welcome this work as they move into consent solution development. Those jurisdictions already working on consent solutions are interested in sharing their work and view a national effort as potentially useful in informing their future releases and interoperability.

Objectives

The intent of the project is to provide jurisdictions with information that will help them make decisions related to the consent management solution they plan to implement within their boundaries.

---

1 See glossary in Appendix B for definitions of consent management, consent management solutions, and consent directives.
The specific objectives of the project are to:

- Identify pan-Canadian business and architectural requirements for consent management that can be used as appropriate, to promote consistency and reusability.
- Enable the jurisdictions to meet their various legislative/policy requirements regarding individual consent for collecting, using and disclosing personal health information to support direct patient care or health system use.
- Create deliverables that are flexible and forward looking enough to accommodate business requirements that may arise as systems are integrated and evolve over the next five years.

**Approach**

A project Working Group – which included representatives from the Health Information Privacy Group and other health care areas – served as the key mechanism for stakeholder engagement in the project. It and the Project Advisory Group – which included representation from a broader group of healthcare system stakeholders – were created to provide input, expertise and validation of the work. A list of members of these groups can be found in Appendix A.

**Project scope**

**In scope for this project:**

- The business and technical requirements related to an individual’s instructions for the collection, use and disclosure of their personal health information in EHR and POS systems for patient care, health system use (HSU) and applicable consumer health solutions (CHS).
- The CMS, interfaces and connection points to supporting EHR systems and common services, mechanisms for the exchange of consent directives, and architectural, design and deployment options for the CMS.

**Out of scope for this project:**

- Consent for treatment (e.g. surgery).
- Influencing, modifying, or standardizing privacy legislation and policies within the jurisdictions. This project is neutral to the legislation and policies of the jurisdictions.
- Reviewing privacy-related policies and/or legislation in the jurisdictions. (Project stakeholders will provide this expertise via the stakeholder engagement process.)
• Defining who, where, when, or how jurisdictions are to collect, manage or enforce consent directives. The clinical/workload implications associated with development or deployment of a consent management solution are important but outside the scope of this project.

• The management of paper-based consent directives other than recognizing the interface between paper and electronic processes in this area.

• Reviews and recommendations for the best technology to store consent, for accessing the system or validating an individual (for example, through the use of smart cards or biometrics.)

• Policies around management of the consent system, including identity authentication and management.

• Vendor product certification testing.

• Business processes related to management of consent directives.

• Review or progress of any project deliverable through any of the Standards Collaborative pan-Canadian Standards Product Lifecycle decision points to establish a pan-Canadian Standard, or any of the associated responsibilities or activities such as providing a specification for Infoway Maintenance Services.

GUIDING PRINCIPLES

The following guiding principles inform this paper:

• Interoperability of consent management solutions among various health information systems is an objective in the longer term;

• The persistence of consent or disclosure directives across the health information ecosystem is a desirable long-term goal as it would minimize complexity for both individuals as well as health care providers and administrators; and

• The principles expressed in the paper, ‘Privacy and EHR Information Flows in Canada: Common Understandings of the Pan-Canadian Health Information Privacy Group’ (referred to as the ‘Common Understandings’ paper in the remainder of this document) have been used as a basis for this project and have been reflected in the approaches described in this project.²

² “Privacy and EHR information flows in Canada: Common Understandings of The Pan-Canadian Health Information Privacy Group”, Canada Health Infoway, June, 2010
PROJECT ASSUMPTIONS

The analysis and guidance presented in this paper are based on the following assumptions:

- Jurisdiction-specific legislation as well as regulation and/or policy at the jurisdictional, regional or local level will direct the circumstances under which a consent/disclosure directive\(^3\) may be placed;
- Consent directives are placed at the direction of an individual;
- Rules respecting who is eligible to place a directive vary by jurisdiction;
- An individual need not be receiving care in order to place a consent or disclosure directive;
- When an individual is incapable of placing a consent directive (e.g. under-aged children and those with certain health issues), depending on the jurisdiction’s legislation, regulation or policy, a substitute decision maker or other authorized individual may place a consent or disclosure directive on their behalf;
- Various health information systems at point of service and those which are part of the jurisdictional EHR may handle consent directives differently and therefore a consent directive placed in one system may not be able to be interpreted and enforced in another;
- Individuals will not necessarily have knowledge of, nor an understanding of the differences between health information systems (point of service systems, provincial/territorial or federal systems) and therefore may assume that once a consent directive is placed in one system, it will flow across systems;
- Health care providers have an understanding of the differences between health information systems and of their accountabilities particularly as they relate to consent/disclosure directives for the system that they are using;
- Jurisdictions will have processes in place for identity management and authentication. Both are important building blocks for the implementation of consent management solutions; and
- Jurisdictional privacy, access, audit and breach policies are in place at the appropriate levels within the jurisdiction.

PURPOSE OF THIS DOCUMENT

This document is a key project deliverable. It is intended for all those considering or involved in making decisions regarding electronic consent management systems. It identifies and describes the business considerations and the business requirements for a flexible consent

\(^3\) Note – the terms consent and disclosure directives are defined in the glossary – the two terms are used interchangeably and are explained in further detail on page 17.
management solution. While it sets out a number of architectural considerations, it is not a high-level design document for implementing a consent management solution.

Another purpose of this document is to serve as a vehicle for jurisdictional stakeholder engagement, feedback and validation.

The document is NOT meant to be a comprehensive description of every jurisdiction’s current and planned future consent practices. Rather, based on input from a number of Canadian jurisdictions, it illustrates the wide range of consent practices and requirements that need to be taken into consideration when considering technical approaches to consent management in an interoperable environment.

TERMINOLOGY

For ease of understanding, Appendix B provides a collection of definitions of terms.
2. Overview of current jurisdictional consent solutions

LEGISLATIVE OVERVIEW

Informational consent, or the ability of an individual to exercise a certain level of control over their personal health information (PHI), is addressed in a variety of ways in privacy and other legislation across Canada. The express consent of the individual is generally not required for the collection of personal health information for the provision of care and treatment. In fact, the collection of this information is required to provide care. The legislative frameworks in most jurisdictions, however, permit individuals to express their wishes to limit use and/or disclosure of their personal health information for some purposes. Consideration needs to be given to the individual’s wishes; however, jurisdictional and organizational rules drive the extent to which these wishes may be exercised.

‘Consent directive’ is one term used to refer to an individual’s explicit instructions limiting the use or disclosure of their personal health information as permitted by legislation, regulation or policy. Some jurisdictions use other terms to refer to this e.g., ‘disclosure directives’ or ‘expressed wishes’. Consent directives may include direction to permit, withhold, withdraw, change or revoke consent to collect, use or disclose personal health information.

While most jurisdictions have enacted health care specific privacy legislation and some also have enacted e-health specific statutes, health care providers and organizations may be subject to additional pieces of jurisdictional legislation that also address consent. For example, there may be legislation and associated regulations which dictate information management practices of hospitals. Additionally, regulated health professionals may also have privacy codes which guide their behavior and could have implications for the application of consent directives.

Another important feature of the consent provisions in legislation is that they generally do not address details related to implementation such as the level of detail (granularity) to which the consent applies to or how information systems are to be configured to support consent requirements. Consequently there may be variations in how consent is operationalized even within a jurisdiction.
CONSENT MANAGEMENT SOLUTIONS OVERVIEW

Many jurisdictions began building their EHR systems by deploying a single clinical domain repository\(^4\) with a consent solution specific to the needs of the domain and technical capability at the time. Successive domains were released with consent functionality that suited the domain needs and available technical functionality. Within these same jurisdictions there may also be POS solutions with differing consent functionality. As a result, jurisdictions are faced with complex consent management environments, most of which are not interoperable with other consent solutions and clinical domain repositories. Further, jurisdictions are at different stages of development and implementation and therefore require consent management solutions that reflect their unique circumstances.

Process Overview

Just as there are differences between jurisdictions in their approach to consent, there are also differences in the way consent directive options are made known to the public and how the consent instructions are captured, documented, entered into information systems and managed. This is the lifecycle of a consent directive.

The cycle begins with individuals being made aware of the option to apply a consent directive. Individuals then make their wishes known to a party who can ‘capture’ and process them. This involves entering them into a consent management system or ‘creating’ the directive. Once entered into the system the system will ‘read’ the directives when an access request is made. Changes or ‘updates’ to the directives can be made and finally, the directive can be deactivated. The stages of the lifecycle including ‘capture’, ‘create’ ‘read’, ‘update’ and ‘deactivate’ are described in further detail in Appendix C: The Process Lifecycle of a Consent Directive.

HIGH LEVEL OVERVIEW BY JURISDICTION (PRESENTED ALPHABETICALLY)

This section is intended to provide a high level overview of the current state of a jurisdiction’s consent management solutions both from process and technical perspectives. It is based on input from six jurisdictions represented on the Consent Management Project Working Group. There may be other approaches to consent management in Canada that are therefore not reflected in this section. In reviewing these descriptions it must be kept in mind that consent management processes in the EHR environment are still relatively new services and the processes are still evolving.

Alberta

Information and forms for placing consent directives can be found at doctors’ offices, the ministry of health website or through a central phone number. Capturing the data is a manual process and record management is done within the ministry of health. Consent storage is within the Health Information Access Layer (HIAL). Consent directives can be

\(^4\) EHR information domain repositories include but are not limited to laboratory, drugs, diagnostic imaging.
placed at the domain or discipline (e.g. physician documentation) level by global masking. Data is not masked at the source. This means that all information – demographic and clinical – is collected and stored in source systems. When an individual requests masking, it is done at the provincial viewer level which hides clinical information but demographic information remains visible. Alberta is looking into enabling finer granularity.

**British Columbia**

In BC individuals can get information and forms on making or revoking disclosure directives either through a provincial toll free call centre or through a provincial website. Staff at the call center is available to answer questions around how disclosure directives work. For individuals who want to know the clinical implications of making a disclosure directive a registered nurse is available to provide guidance. Disclosure directives are placed on each applicable domain and these directives are stored within a repository in the HIAL. Domain data is masked at the global level with a keyword to unmask. The ministry administers the keyword database. BC legislation contemplates having a patient portal to enable individuals to manage their own directives; however, before this can be done a solution to individual identity management must be found and implemented.

**Manitoba**

In Manitoba, information and forms for placing consent directives for eChart Manitoba can be found on an eChart website, through brochures and forms at points of care, or requested through a related toll free phone number. All public facing phones at the Manitoba eHealth offices and within the ministry of health have scripted information to explain the process for placing or removing a consent directive and the effect. Consent directives are placed and managed centrally, and only the Disclosure Directive Manager and the backup to that position have access to the system. The Disclosure Directive is stored in the provincial Client Registry, which is a source of demographic information for eChart Manitoba. A Disclosure Directive results in global masking of clinical information – demographic information cannot be masked. In communications with the public, global masking is described as “hiding” the information. A message will indicate that information is in the system but is not available to the user. Each override triggers an alert to a privacy officer.

**Newfoundland and Labrador**

In Newfoundland and Labrador, information flows into the EHR without an individual’s consent. At this time, the Pharmacy Network is the only component of the EHR offering consent management. Masking is global so that when a consent directive is placed, only demographic information and a notice that clinical information is unavailable are displayed. The pharmacist/professional always has the ability to override the mask in an emergency.

To place a consent directive an individual contacts the Service Desk of the Centre for Health Information which forwards requests to the Pharmacy Network Program within the Centre for Health Information. A pharmacist representing the program contacts the individual and
explains the consequences of masking. Should the individual still wish to place a mask on their profile, the pharmacist forwards a Pharmacy Network Password Management Form. The completed form and proof of identification is submitted and then compared against information found in the Client Registry. Once identity is verified, the individual is contacted to establish a password and three security questions, which can be used in future to confirm the individual’s identity. To remove the mask, the same process is repeated.

Currently, consent management occurs in the domain but there are plans to move it to the HIAL to support consent in other EHR domains. There are no plans to change the level of granularity associated with EHR consent in the foreseeable future.

All EHR data, including masked information, flows into the EHR Data Warehouse. The Data Warehouse is used to support health system uses and disclosures, many of which can occur without an individual’s consent.

**Ontario**

Ontario currently has two provincial electronic systems in place, including laboratory and drug information. Personal health information is captured in each of the systems based on implied consent. Each system has its own approach for processing and administering consent directives. Currently consent directives are managed at the POS and also through a centralized call centre. Other non-provincial systems also have their own consent directives processes, which are not standardized across the province.

For the Ontario Laboratory Information System (OLIS), patients can restrict access to lab information associated with one specific test request and result or all test requisitions and results. If patients choose to restrict access, only the health professional who ordered the tests and the health professionals who are identified to be copied on the results, will be able to access the test results through OLIS.

For the Ontario Drug Benefits (ODB) program, patients have the ability to withdraw fully, where the Ministry will not disclose information related to the patient’s drug claims history. The patient can also choose a partial withdrawal of consent, where only the information on a specific drug can be masked. The Ministry will not disclose information related to those masked medications.

For both OLIS and ODB, overrides of consent directives are only permitted with the consent of the patient or substitute decision maker. In cases of overrides, the patients are automatically notified through a letter stating when, where and by whom, the override occurred.

For the Baseline Diabetes Database Initiative (BDDI) individuals can withdraw their consent from having their personal health information included in the Diabetes Testing Report. Those individuals who have withdrawn their consent will not be included in BDDI.
Depending upon the program, consent directives may be placed at the provider, organization, requisition and drug levels. As a result of the various levels of granularity within these systems, an individual may have multiple consent directives in place. In all three systems, patients can reinstate their consent.

The Ministry is working jointly with its agency, eHealth Ontario, to develop a Consent Management Framework that will guide the development of a province-wide consent management solution and be applicable across all domains in the EHR system.

**Saskatchewan**

Information and a form for placing consent directives in Saskatchewan are available through an eHealth privacy service which includes a toll-free number, website, and email address. The service currently resides in the Drug Plan and Extended Benefits Branch of the Ministry of Health but is transitioning to eHealth Saskatchewan and should be completed in October 2011. Communication information and scripts to explain the implications of applying a consent directive are available to providers, the eHealth privacy service, and patients. Requests are made through the eHealth privacy service. Once a consent directive has been activated, confirmation is sent to the individual. Consent directives are stored in the domain for the drug domain, a separate application for PACS, and in the HIAL for the lab domain. Consent directives are placed at the domain level, one per domain, and data is masked globally. No decisions have been made regarding future granularity requirements.
Comparing jurisdiction consent management implementations

Generally, the approach to managing consent directives is fairly consistent across the six provinces informing this document. There is some variation, however, which is summarized below:

Approaches to capturing consent directives:

- Five of the jurisdictions involved in the project have a centralized approach for capturing a consent directive. Websites and call/service centers provide individuals with access to forms and information about consent directives including the implications of placing one. Only one jurisdiction has a strictly decentralized approach as a result of the manner in which domains have been implemented.

- In most situations, contributing jurisdictions require that individuals complete a form containing demographic information and provide identification in order for a consent directive to be placed. Information captured on the form varies by jurisdiction and in one case, by system. One jurisdiction accepts verbal consent for application of a directive and another may accept verbal instructions if the individual has a disability and is unable to complete a form.

- Multiple disclosure directives may be in place for the same individual. A separate form may be required for each domain/system, although some jurisdictions are moving towards the development and use of a single form.

Approaches to verifying the information captured on the consent directive form:

- Most jurisdictions reported verifying information provided by individuals. This is done by comparing information provided by the individual on a paper-based form to information already contained in a provincial health care information system. In two jurisdictions, the Client Registry is the information system used to compare data.

- In one jurisdiction, the administrator sends a letter with a code and telephone number to the individual who has requested the placement of a consent directive. The individual must call the number and provide the code for the directive to be activated.

- To date, no automated reconciliation of multiple consent directives has been implemented.

Approaches to creating a consent directive:

- In five jurisdictions, individuals submit the completed form to an organization or entity with the responsibility to receive and process directives. In the sixth, in some circumstances, a telephone call is placed and the consent instructions and authority to activate the consent directive is received verbally.

- Once a completed form is verified, the individual responsible for administering the system creates the directive in the appropriate system.
• Creating a consent directive by entering information into a system is generally a manual process. Paper forms are retained in at least three jurisdictions. In two jurisdictions the forms are scanned into the system.

• In the creation of consent directives, two jurisdictions make use of keywords to unmask (override data). Keywords, which may only be a single character in length, must be established when the consent directive is created.

• Three of the jurisdictions have implemented global masking, in other words – individuals are permitted to restrict either all personal health information with the exception of their demographic information, or to restrict nothing.

• Four jurisdictions create consent directives at the clinical domain repository level. One of the four jurisdictions that creates domain level directives does so by discipline (e.g. cancer care, direct primary care), and another does so by provider (named clinician). One jurisdiction uses varied approaches to applying consent directives in multiple domains.

Approaches to **storing** a consent directive:

• In two jurisdictions consent directives are stored in a dedicated consent repository in the HIAL. In jurisdictions that apply the consent directive at the HIAL or EHR level, as opposed to at the domain level, the directive only applies to the EHR system and not to the domain.

• In three jurisdictions consent directives are stored in the domain. These jurisdictions are considering storing consent directives in a HIAL.

• One jurisdiction stores consent directives in the Client Registry.

Approach to **reading** a consent directive:

• In the one jurisdiction where multiple consent directives for an individual may be in place because they are captured per domain, there is no automated process for ensuring no conflict between them.

Approaches to **updating** a consent directive:

• Five of six jurisdictions reported that changes can be made to a consent directive by completing a form or calling a central number to request the change. In two jurisdictions, the only change that can be made is to deactivate the consent directive.

Approaches to **overriding** a consent directive:

• All jurisdictions have override provisions.

• The reason for the override must be entered into the information system in two jurisdictions.
• The duration of an override varies by jurisdiction, application and situation. One jurisdiction requires the provider to indicate the duration that the override will be in effect. One jurisdiction allows for a four-hour temporary override for an application.

• In some jurisdictions, the system automatically notifies an administrator, privacy officer or other role of the override event.

• One jurisdiction sends acknowledgement letters to individuals to inform them that an override has been entered and that a health care provider accessed their electronic health records.

OVERVIEW OF CONSENT MANAGEMENT OUTSIDE OF CANADA

Internationally, the manner in which health care is delivered varies by country, as well as by regional differences in societal values and policy. Further, the electronic health record models differ from country to country. Legislative frameworks impacting privacy practices, while generally consistent with the Organization for Economic Cooperation and Development privacy principles\(^5\), also vary from country to country. These differences make it difficult to compare countries’ approaches to consent management.

Information on consent management practices in Sweden, Denmark, Netherlands, Germany, Australia, United Kingdom and closer to home, in the United States has confirmed variation in practice. Nevertheless, it would appear that other countries implementing electronic health records and associated consent directive management solutions are dealing with similar issues – what model to use, the degree of granularity that can or should be used and how to accommodate these policy decisions within the electronic health record systems being implemented.

For more information on how specific countries and international jurisdictions are implementing consent management solutions, see references noted in Appendix D.

CONSENT DIRECTIVES IN OTHER INDUSTRIES

Other industries, for example: finance, education and life sciences, also deal with personal information and are subject to privacy legislation and, in the case of finance, external regulatory bodies. These industries must also consider how best to manage confidential information and, in certain circumstances, make provisions for the management of consent for use and disclosure of that information. Education, which heavily invests in research, may come closest to reflecting the secondary uses and integration with consent management of health information. However, there are also significant differences which make it difficult to

\(^5\) Organization for Economic Co-operation and Development Privacy Principles were published in 1981 and was influential in the development of privacy law. http://oecdprivacy.org/
translate practices from these industries to health. With health care, the relationship between the individual and bodies providing care can span the duration of a lifetime whereas transactions with entities in the financial or education sector may be more limited in terms of both duration of the relationship as well as in the nature of information being shared. Therefore, at this point their experience does not seem to be directly applicable to the health care sector.
3. Business considerations

The sections below describe a variety of policy, business and operational issues related to operationalizing, applying, storing, and managing consent directives. The issues outlined are those that would be of relevance primarily to implementers or decision/policy-makers. It is not meant to be a comprehensive list, as it is recognized that additional issues may be identified through jurisdictional privacy impact assessments (PIA); threat and risk assessments and other planning processes.

GRANULARITY AND MASKING

Granularity is a particularly challenging topic with policy, process and technical implications. Granularity refers to the level of detail in a consent directive that an individual may request. For example, starting with the most coarse-grained and moving to the finer-grained, a directive could apply to:

- All PHI: Meaning all PHI stored in the EHR
- PHI by Domain Repository: Meaning all PHI stored in one or more domain repositories (e.g. entire drug profile)
- PHI by Facility: Meaning all PHI by facility (e.g. this is a common request of staff within a healthcare facility)
- PHI by Role: Meaning all PHI by EHR User role (e.g. social workers may not be authorized to use or disclose information)
- PHI by EHR User: Meaning all PHI by EHR User identity (e.g. a specific doctor or nurse cannot use or disclose information)
- By Data element: Meaning a specific record or data field in the EHR or type of health information (e.g. HIV test results cannot be used or disclosed)

Other examples of fine granularity:

- Include only (e.g. limit access to a provider/location only and exclude all others)
- Ability to hide specified documents (e.g. limit access to all psychological reports)
- Restrict by use (e.g. information can be used but not disclosed or cannot be used for research)
- Restrict to certain time period (e.g. consent revoked or available for a specified time only)
- Restrict by type of diagnosis or disease (e.g. masking all references to specific sensitive conditions)
The typical ways to prevent access to personal health information include masking and keywords. Other approaches to preventing access may include rendering the information unavailable by removing a link to the record, manually removing individuals from the database or concealing the existence of a record. Note that if these other approaches are used, they prevent the information from being accessed, even in the case of an emergency. These are exceptional, manual procedures and therefore, are outside the scope of this project. Jurisdictions considering including these approaches will require a strong communication strategy to ensure individuals understand this implication.

In most jurisdictions at this time, if an individual wishes to render their information inaccessible, the entire record in a domain is rendered inaccessible. This approach has been adopted as it is viewed, at this time, as the safest option for both the individual and care providers and the option that is the most effective at ensuring the individual’s wishes are in fact respected.

Clinicians indicate that there may be potential patient safety issues in reviewing a record which does not include potentially relevant clinical information. It is also difficult to assure individuals that their wishes are being respected when the information they are trying to restrict may be discerned from other data in the system. For example, to restrict the diagnosis of HIV it would be necessary to not only restrict the diagnosis but also specific lab results from the lab repository, as well as information that may reside in the drug repository. Moreover, system administrators and developers report that the only means of removing the information is by physically redacting all information potentially related to the information the individual wishes to restrict and it is difficult to ensure that all relevant information is removed.

At the time of writing, a research study on discerning masked data from other data in a record conducted by Dr. Khaled El Emam, Canada Research Chair in Electronic Health Information at the University of Ottawa, was nearing completion. The research design tests the ability of health care practitioners, in this case, pharmacists, to predict a masked diagnosis from longitudinal drug information and patient demographics. The early findings of this research, expected in the spring of 2012, suggest that these predictions can be accurate.

While at this time most jurisdictions have chosen to mask all domains, it is recognized that masking only that information that is of concern to a patient, rather than masking all of the person’s health information, or all laboratory tests or other large masses of information gives the individual more privacy choices. This finer granularity may also be a requirement in specific care settings such as a hospital or clinic, in certain particularly sensitive situations, and also as EHR systems become more integrated.

Some health information software (HIS, CIS, EMR) solution vendors have indicated that such fine grained consent to the field level is possible; however, at this time, the project could not
identify any such solutions in operation. Consent solution vendors that were contacted recognized that this may be a potential requirement; however, uniformly recommend a more coarse-grained approach. From their perspective, fine-grained consent presents operational challenges.

Due to the complexity of fine grained consent, it may have significant administrative, implementation, management and cost implications in an EHR environment at this time, although as already noted, fine grained consent may currently be more feasible in a hospital or other more localized system.

Jurisdictions wishing to implement a fine level of granularity in the EHR may need to consider the impact that this will have on both technology and associated processes for managing consent. Jurisdictions also need to consider, that with multiple or fine grained disclosure directives, the number of rules to be verified and applied for each access to an EHR will increase in number and potential complexity. This may have an impact on system performance.

If fine grained consent as it relates to diagnosis/condition is the chosen policy option, until the EHR can accommodate persistence between systems, someone who is knowledgeable in clinical records and data associated with specific diseases would need to be tasked with the responsibility for identifying the information that would need to be masked. Moreover, there may be a need for ongoing review of the masked elements. For example, as additional test results about an individual become available (e.g. an individual learns of a new diagnosis) and clinical knowledge evolves (e.g. new research demonstrates a link between a particular laboratory test and a certain condition) and as consent directives options become even more fine-grained (e.g. allow for drug-specific or lab-specific blocks), the question arises as to whether a review is necessary of the currently masked elements or whether individuals are to be informed of potential changes to their consent directives options. As a result, there could be risk and workload implications to this approach.

Jurisdictions may also wish to consider whether to move towards a consistent approach to granularity in their legacy, current and planned systems. There may be a strong rationale for taking different approaches in different parts of the EHR system however, managing multiple approaches is likely to be more difficult than managing a single approach, particularly as additional components / domains are added to the system.

As noted above, the current thinking is that global masking or global masking by domain is the approach most able to truly honour patient expectations at this time. Policies in this area may change over time; as such, any consent management solution will require a degree of flexibility to ensure that it can accommodate potential future changes, particularly as they relate to granularity. For example, as individuals become more aware of masking either via the EHR or in the process of setting up their own personal health record system, the public may demand finer grained consent options.
STORAGE OF CONSENT DIRECTIVES

In order for consent directives to be interoperable and available they must be stored and accessible for validation whenever PHI is accessed and regardless where consent is captured; by POS system, by EHR or by clinical data system viewers. There are two main consent directive data storage models, centralized and decentralized.

Centralized storage enables consent directive data sharing to all points of service through connectivity from a centralized repository. Consent directives stored centrally, or within connected centralized repositories such as a Client Registry, ensure that they are available to be applied whenever health information is viewed. Access to the centralized consent repository may be via a HIAL interface.

Decentralized storage maintains consent directives in multiple locations. In a decentralized system, there may be a separate approach to consent directive storage for each system. For instance storage could occur at the POS or within the clinical domain repository such as the jurisdictional laboratory repository.

In a decentralized environment, if EHR administrators wish to bring consent directives together to consolidate management or enforcement, there may be a need to create/acquire a system/engine that will find all consent directives in all of the systems, consolidate them, interpret them in a common way and enforce them. To do so, the consent directives must be codified and accessible in a common format. If they are not, a translation or mapping function would also be required.

Consent directives may also be stored in local POS applications and environments. In the event that a consent directive is captured by either an EMR or hospital information system it may, in addition to being stored in a centralized repository, be stored in the local system if it applies to locally stored PHI. The determination as to whether the captured consent directives should be stored locally is dependent on specific use cases and business requirements.

Some jurisdictions also store paper copies of consent directives. Signed papers are physically stored in a designated location. Other jurisdictions may scan and electronically store consent directive forms, with the paper version also stored. While this project does not deal with paper based systems, some jurisdictions may have a requirement for the CMS system to be able to store and transmit a copy of a scanned paper document or to be able to indicate where the paper document is stored.
Considerations:

- Consideration needs to be given to whether consent directives will be stored in one location and referenced by other systems or whether they will be replicated and stored in multiple systems. These considerations are both architectural/technical and business related.

- If a decentralized storage model is being contemplated, a common messaging standard is important to ensure the interoperability of consent directive data. This permits a consistent/uniform interpretation of directives across systems.

- As additional clinical systems are implemented it may be helpful to consider the potential benefits of a global/enterprise view.

CONSENT DIRECTIVE ENFORCEMENT

When a consent directive is in place for an individual and a request is made to access the masked information, the CMS will apply or enforce the instructions that were contained in the directive. The enforcement of a consent directive can occur in any of several locations, for example, local POS systems, clinical domain repositories or in a centralized CMS.

Considerations:

- As part of the enforcement of the consent rules, as discussed in the Common Understandings paper, it is important to include in the CMS appropriate messages to the clinician who is viewing/using the record to indicate that information is masked.

- Various documents, such as clinical summaries, could be included in the EHR. Consideration should be given to the fact that documents may include information to be masked and may come from several sources. Further, the information in the documents may not be in a structured format and therefore may not be machine readable. Enforcement of consent directives in a document with unstructured language is difficult and would require a flag in the CMS that indicates the document is subject to a consent directive. It is important to note that changes to consent directives associated with these documents may require human intervention to ensure that the flag continues to be applicable.
MANAGING CONSENT DIRECTIVES

Once captured and stored, consent directives must be managed, in other words there need to be processes in place respecting access to the consent directives, how they will be updated and monitored, and how to deal with conflicting instructions, etc.

Considerations:

- In some jurisdictions an individual can place more than one consent directive. Conflicts between directives may need to be identified and resolved to ensure an individual’s wishes are followed. Automated processes may be available to recognize and notify administrators of potential conflicts and where and what human intervention is required.

- Consideration must be given to how consent directives will be updated as required by changes in an individual’s circumstances. Who will be permitted to access the CMS to make updates to the system? What process will be used to authorize changes in the system? Some jurisdictions may wish to allow individuals to electronically update their own consent directives as a potential future option.

- When a decentralized system for storage is used, depending on the level of technical integration, updates to consent directives may need to be applied to multiple systems.

- A decentralized approach for the management of consent directives may have implications for management functions such as auditing. When an audit is required, either for purposes of conducting an investigation or for monitoring compliance there will be a need to consider ALL the systems which manage consent so that information is pulled from all relevant systems.

- Jurisdictions may wish to consider incorporating mechanisms in the CMS to provide metrics, for example the number of directives in place, volume of change, number and nature of overrides, etc. (Note that there may be privacy issues related to certain types of reports, particularly if de-identified information could potentially be rendered identifiable.)

- Legislation, policy and other guidelines for consent may change over time, which may result in the need for changes to the rules within the CMS.

OVERRIDES

Most jurisdictions make some allowance for consent instructions to be overridden, for example in emergency situations. The approach taken to overrides can vary by system and across jurisdictions.
Jurisdictions may want to consider:

- Including in the CMS mechanisms to allow the individual to authorize an override in certain circumstances. Some jurisdictions provide a keyword to the individual for this purpose.
- Mechanisms for ensuring individuals are aware of the conditions under which their consent directives may be overridden.
- Establishing specific criteria which need to be met for an override to be allowed.
- Establishing time limits for an override.
- Specifying the range of roles that will be allowed to override a consent directive. The range needs to be large enough to ensure prompt care for an individual, but restricted enough to limit the potential for unwarranted overrides.
- Automatic notification to an administrator or privacy officer role or the individual of certain or all successful (and possibly unsuccessful) attempts to override a consent directive.
- Professional practice requirements for health care providers related to documentation of information which includes instances where health care providers have acted on information made available as the result of an override.

INTEGRATION

The CMS will need to be able to interact with other systems such as the jurisdiction’s identity management systems, provider registries and client registries. For example, within a CMS, an identity management function is required to uniquely identify administrators, providers, and potentially individuals (at some future point). While out of scope for this project, it is also acknowledged that jurisdictions may be considering information systems to support audit or breach management. To the extent that these systems are being considered, integration with the CMS may be desirable.

Because there are thousands of end-points in the health system, technical standards and a common vocabulary are important for interoperability, particularly if a decentralized approach is taken to the CMS. However as more and more components of the iEHR are implemented, jurisdictions may see value in moving towards integration of consent management solutions.

The jurisdictions represented in the Working Group noted that regardless of whether a centralized, decentralized or mixed approach is used, movement towards some consistency in consent approaches would be helpful. In addition to easing system management, consistency could also help decrease the complexity (and the attendant requirements for communications and explanation) that an individual may face in placing a consent directive.
and ensuring it can be respected in all the systems being used. However moving to a more consistent approach can present a number of challenges, for example:

- Legacy systems, including those that rely both on paper forms and electronic systems to capture and create consent directives, may continue to be used in the overall care system.

- In a POS solution, consent directives may be placed at finer levels of granularity than with the EHR, which at this point tends to apply a coarser granularity. Integration becomes an even greater challenge in situations where there are multiple consent management solutions in various POS systems and the EHR, and the solutions do not have the same level of granularity or differ on some other functionality.

- There could also be a situation in which various EHR components – a lab system, a drug system and a diagnostic imaging system – each have a different CMS.

- In some instances it may not be possible to retool the legacy systems to capture and create consent directives while in other instances some type of integration may be possible.

- A reconciliation, mapping or harmonization process may be required to resolve conflicts and ensure that information masked in one system does not become visible as it moves to another system.

- Jurisdictions will need to consider the relationship of the CMS with legacy systems to determine what integration issues they may face and how they may be addressed.

The table below, which correlates the EHR CMS to those POS that have a CMS, summarizes situations where conflicts may occur.

<table>
<thead>
<tr>
<th>CMS enabled Points of Service</th>
<th>Harmonized granularity policies and technical capacities</th>
<th>Differing granularity policies OR technical capacities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EHR</td>
<td>EHR</td>
</tr>
<tr>
<td></td>
<td>Single CMS solution</td>
<td>Multiple CMS solutions</td>
</tr>
<tr>
<td>Single CMS solution</td>
<td>Conflict unlikely</td>
<td>Conflict unlikely</td>
</tr>
<tr>
<td>Multiple CMS solutions</td>
<td>Conflict unlikely</td>
<td>Potential conflict</td>
</tr>
<tr>
<td></td>
<td>Conflict unlikely</td>
<td>Conflict likely</td>
</tr>
<tr>
<td></td>
<td>Conflict unlikely</td>
<td>Conflict likely</td>
</tr>
<tr>
<td></td>
<td>Conflict likely</td>
<td>Conflict likely</td>
</tr>
</tbody>
</table>
As jurisdictions evolve in their approach to consent management and to the degree that this evolution may include the migration of existing solutions to a more integrated future state, the development of a road map or plan may be helpful. The road map would need to include a model of the planned future state, associated use cases, the business and technical requirements, as well as steps planned to migrate the information from multiple systems into a single system. It would also need to include methods for addressing issues such as plans for moving from a less granular consent approach to a more granular one.

INTER-JURISDICTIONAL MOVEMENT OF DATA

A discussion about business considerations of managing consent directives would be incomplete without contemplating what will happen when an individual with a consent directive in place either seeks care outside of his/her home jurisdiction or moves to another jurisdiction. Inter-jurisdictional movement of data has many challenges, particularly when consent directives are in place.

This project does not anticipate that consent directives themselves or the consent directive instructions will be shared across jurisdictions or that there will be uniformity in CMSs across the country that would allow for application in second jurisdiction of a directive originating in another jurisdiction. Rather, it assumes that any consent directive instructions will be applied by the disclosing jurisdiction before a disclosure is made. In other words, as noted in the Common Understandings paper, except where otherwise permitted, if an individual has placed a consent directive to mask personal health information, that consent directive should be enforced in the home jurisdiction, and the masked information should not be disclosed to another jurisdiction.

Nevertheless, a number of considerations remain. For example:

- In situations where information subject to a consent directive is not disclosed to another jurisdiction, the care provider in the jurisdiction requesting the information must be advised that information has been masked and is not being disclosed.
- Where permitted because the patient has provided consent or the situation meets a jurisdiction’s override criteria, the information may be disclosed from the source jurisdiction to the requesting jurisdiction. If this is the case, after the care episode, the individual may wish to re-mask the information in the second jurisdiction. According to the Common Understandings paper, the second jurisdiction should make efforts to re-mask the information in accordance with its legal framework and technology currently in place in the jurisdiction, and the patient should be notified of the results. It must be recognized, however, that the second jurisdiction may not permit masking of data at the same level of granularity, if at all.
• Jurisdictions also need to determine how non-residents will be made aware of the consent rules when being treated and how any consent wishes will be communicated and managed in the case of an emergency.

• Consistent with the Common Understandings paper, it is thought that at minimum, there will need to be notification of the public and providers about consent management practices should there be a circumstance which calls for cross-jurisdictional access of personal health information. Some jurisdictions have considered entering into a bilateral agreement between jurisdictions regarding EHR information flows, and as part of these agreements, may wish to ensure that the rules around consent management between the jurisdictions are understood and managed consistently.

• Jurisdictions also need to consider how individuals and providers will be uniquely identified across jurisdictional boundaries.

While technically, in the future, it may be possible for inter-jurisdictional HIAL to HIAL communication to facilitate consent management, interoperability of this nature may be complicated by variation in consent rules and processes.

IMPORTANT OF COMMUNICATION

This project focuses on the technical aspects of consent management. However, consultations with stakeholders have highlighted the importance of communication and education as part of the consent management implementation strategy. A communication strategy would help inform and manage the expectations of individuals, health care providers and other stakeholders. It could assist individuals in making choices about their personal health information and could provide clarity to health care providers concerning their role in the consent management process. The Common Understandings paper provides some insight into information useful to patients, providers and others in this respect.6

Consideration should be given to the need for ongoing communication to individuals, healthcare providers and other stakeholders as the health information ecosystem matures and boundaries between health information systems change.

FUTURE PROOFING

There was general agreement among the jurisdictions represented in the Working Group that systems and consent directive requirements and processes may change over the next few years as more solutions come online and the public becomes more aware of consent options.

6 “Privacy and EHR information flows in Canada: Common Understandings of The Pan-Canadian Health Information Privacy Group”, Canada Health Infoway, June, 2010 pp 22-23.
Designing capacity and flexibility, such as the ability to become more or less granular, into the CMS system will allow for future evolution of consent policies. This approach may help protect the investment not only of jurisdictions, but also of vendors.

Some examples of potential changes include:

- Jurisdictions may allow individuals to connect with the EHR system to change or update their own consent directives.
- Effective ways to accommodate finer granularity may be developed.
- Jurisdictions may allow researchers to solicit individuals to consent for the use of their EHR information for research purposes and it could be decided to record this consent in the consent management solution. If this is the case, then a consent management system may need the capacity to record significantly more consent directives.
- Jurisdictions may require information systems at various levels (point of service, regional and provincial) to ensure ‘persistence’ of a consent directive – that a directive captured in one system can move to another system within the ecosystem. Organizations considering the procurement and implementation of a centralized consent management system will need to take interoperability into consideration to accommodate this potential requirement.
- The nature of health information itself may change, e.g., genetic information.

OWNERSHIP

Investment in consent management solutions entails both capital investment and ongoing costs. Capital investment may not be a one-time cost, but rather, incurred incrementally as new system investment decisions are made. Ongoing funding is required for system maintenance, upgrades and interfaces with new systems being introduced as well as the related non-technical activities associated with a consent management service, such as governance, policy development and communication (see above), not to mention the related human resource requirements for the management of consent directives.

Considerations:

- When considering the overall cost of a CMS, factors such as granularity, interface with paper records, connectivity, integration of features such as consent options for HSU, can be expected to have a bearing on implementation and operating costs.
- A domain by domain approach may be easier to implement quickly, however, it may cost more in the long term to manage and maintain as more domains are established.
- Building flexibility into the system to support the evolution of legislation and business requirements may result in initial solution development costs. These product costs
may be offset by reduced solution operational and maintenance costs over the life span of the solution.

- A federated or centralized consent directives solution could reduce development, acquisition and implementation costs related the CMS components of additional domains. In addition, it could simplify the management of the consent solution which could translate into reduced CMS operating costs.

Finally, as a CMS has the potential to touch many components of the EHR, there may be ownership considerations that extend beyond cost. Jurisdictions will need to determine how to identify a business owner to undertake the coordination and management effort that will go into the development and implementation of a CMS solution.

FRAMEWORK FOR MANAGING CONSENT (GOVERNANCE)

As time goes on, jurisdictions may wish to consider the development of a jurisdiction wide governance framework for making decisions around consent management for electronic health records. This may be independent of, or integrated with, the broader EHR governance system. While this does not propose to be an exhaustive discussion regarding consent governance, some thoughts raised by the Working Group include the following.

A framework for managing consent could include two levels:

1. Strategic level which includes the development and maintenance of consent related polices.
2. Tactical level which includes operationalizing the policies and overseeing consent activities. This structure becomes more relevant once the CMS is live and there is no longer a project supporting the development and implementation of the consent management solution.

Issues to consider in developing the governance framework as it relates to the strategic level include, but are not limited to:

- Who (which groups, entities, functions, or individuals) is responsible for:
  - Making decisions about the consent management model which will be referenced by organizations participating in the health information ecosystem.
  - Developing jurisdictional policy around consent management (including the level of granularity which will be supported; the conditions under which a

---

7 See Privacy and EHR Information Flows in Canada; Common Understandings of the Health Information Privacy Group Section 3: Accountability for Information Governance for a discussion of EHR governance, Canada Health Infoway, June 30, 2010
8 See White Paper on Information Governance of the Interoperable Electronic Health Record (EHR), Canada Health Infoway, March, 2007
consent directive may be applied across the ecosystem; the high level model for access and overrides; and the approach to HSU).

- Making decisions about the management of the CMS as a whole.
- Developing and approving policy/directives/rules enforced in the CMS.
- Developing policies and plans related to CMS monitoring and audit activities.
- Developing a communication strategy for key audiences including providers, other system users and the public.

Issues to consider in developing the governance framework as it relates to the tactical level include, but are not limited to the development of operational policies and procedures around:

- Processes to create a consent directive, such as whether or not to notify individuals once a directive has been activated/implemented.
- Processes to validate change or update a consent directive, including whether a newer consent directive automatically supersedes a previous consent directive.
- Processes to re-evaluate a consent directive when an individual previously deemed incapable of making a directive becomes capable.
- Processes around maintaining the historical record of disclosure directives and setting out retention schedules and their implementation.
- How audits will be implemented.
- Specifics around override mechanisms.
- Processes by which a substitute decision maker may enact a consent directive, provide override authorization or otherwise reinstate access to personal health information.
- How consent will be managed for those HSU activities which allow for it.
- How complaints about the CMS as it relates to unauthorized collection, use or disclosure will be managed.
- Details around how consent directive expiry dates (if any), retention, archiving, and destruction will be managed.

The governance framework may serve to provide both the public and the provider community a sense of confidence in a coordinated, transparent and accessible approach to consent management across the health sector and may minimize fragmentation and duplication of effort as it relates to management of consent directives. Finally, it may assist other jurisdictions considering similar strategic and tactical issues.
4. Health System Use

The term ‘Health System Use’ (HSU) refers to the use of personal health information for clinical program management (including quality improvement and decision support), health system management (including analysis, planning, monitoring), population health surveillance, and research.

Provision for the collection, use and disclosure of personal health information for health system use is included in health-sector specific statutes in Canada. The manner in which the statutes provide for this varies.

For HSU purposes, the term ‘collection’ can include both ‘direct collection’ and ‘indirect collection’. The term ‘collection’ generally implies ‘direct collection’ that is, information which is provided directly by the individual to a health care provider or other entity authorized to collect the information. Alternatively, ‘indirect collection’ refers to personal health information collected from a source other than the individual. An example of this is when personal health information is collected and used for the planning of the health system. This indirect collection for authorized purposes is generally permitted without consent and therefore consent directives do not apply. On the other hand, there are circumstances when indirect collection may not occur without the individual’s express consent.

Health information and other statutes generally place conditions on the use of data for health system use. For example, they often require researchers to obtain the express consent of individuals whose health information they wish to collect and use, unless the requirement is waived by a research ethics review board. Further, there is typically a requirement that if it is possible to conduct research using non-identifiable information (such as anonymized, de-identified or aggregate information), then such information must be used instead.

A consent management solution could be configured to accommodate provision for the capture of consent for research purposes. It would assist in keeping track of those who permit their personal health information to be used for research purposes. Such functionality could also have value for other health system use if legislation or policy evolves over time. It is important to note that this type of functionality may need to accommodate large volumes of ‘opt in’ directives as research is sometimes conducted on large patient populations.

It bears restating that health system use of personal health information does not generally require consent (other than for research) and further, the individual cannot limit use of this information. Jurisdictional policies determine exactly how this is operationalized in each province.
BUSINESS CONSIDERATIONS

The following are HSU business considerations:

- The cost of integrating consent options for HSU into existing domain-based approaches may be a consideration, particularly if there are many domains.

- It is likely that in certain jurisdictions data for HSU will be pulled from a data warehouse. If the information is in a data warehouse there are a number of issues raised regarding consent. For example:
  - Will the data in the data warehouse be de-identified or pseudonymized?
  - Will the consent directives placed by individuals be embedded in the data warehouse? Or, will the information of those who have issued a consent directive be withheld from the data warehouse?

- A CMS may need to accommodate consent for research as consent does not generally apply to most other HSU activities.

- Consideration also needs to be given to the storage of research requests and the associated consents. If they are going to be stored in the EHR consideration will need to be given to whether they will be built into the consent management solution or handled in another manner.
5. Consumer Health Solutions

Individuals can now also establish their own personal health record. While the features available in personal health record systems vary from product to product, they generally provide an individual with an opportunity to create their own personal health file, input self-reported data, interface with special health applications, access health information sites and, in certain circumstances, download their information from a provider-based electronic system. Some systems even permit data to be uploaded from a personal health record to a provider-based system. Personal health records are generally commercial in nature and available to interested individuals for a fee, however there are applications that are offered in the public sector. A key feature of consumer health solutions is that the individual consumer has control of what information is collected and what is shared from the record and with whom, and who has access rights to the record.

For the purpose of this project it is important to draw a distinction between private and public sector solutions.

- Public sector: the consumer health solution is integrated into or operated by the jurisdiction, such as in the case of some portals, and interoperability between the private and public sector applications may be required.
- Private sector: the consumer health solution, the commercially available personal health record software is not integrated or operated by the jurisdiction, and interoperability between the private and public sector applications is not required or likely. Private sector applications are out of scope of this project.

Within Canada some jurisdictions have already implemented or are in the planning stages for integrating the EHR and public sector consumer health solutions. These may take the form of portals associated with domain applications where individuals can view their personal health information and, in some circumstances, input their self-reported information.

BUSINESS CONSIDERATIONS

There are a few considerations which are specific to public sector consumer health solutions and consent. These include but are not limited to the following:

- Proxies are often a key feature of consumer health solutions. Proxies are people, such as relatives or friends of an individual who have been given permission to access that individual’s personal health record. A proxy is not the same as an alternate or substitute decision maker which is a legal entity with certain rights to decision making in the EHR. Jurisdictions contemplating integration of a consumer health solution within the larger EHR framework will need to allow for proxies within the consent management solution and will need to determine how to deal with them within their
identity management framework. While the manner in which consent directives will be accommodated in consumer health solutions is yet to be seen, it would make sense that consumers should be able to self-report/enter consent directives as part of the solution.

- Once an individual enters data into the CHS and that data is made available to the EHR, the information will become subject to the EHR consent framework and will need to be managed as personal health information originating from any other domain application.

- It remains uncertain how consent will be managed when PHI moves from a CHS to an EHR and/or from an EHR to a CHS.

- As more consumer health solutions are developed it may be expected that consumers’ awareness of the way in which personal health information may be controlled will translate into an increase in the number of requests for consent directives for jurisdictional EHR systems.
6. **Business requirements for a consent management solution**

This section of the document will address business level requirements for an interoperable consent management solution. The articulation of common Business Requirements will facilitate the development, design or acquisition of an enterprise\(^9\) level solution for the management of consent directives. The Business Requirements identified by this project cover the spectrum of jurisdictional needs and therefore, vendor solutions meeting these requirements should be in a position to respond to pan-Canadian requests. That said, jurisdictions will implement only those business requirements that are appropriate to their specific jurisdiction’s needs.

This section will be of benefit to several audiences:

1. **Jurisdictional privacy specialists**
   - This section will provide privacy specialists with insight into the business requirements of a consent management solution.

2. **Vendors of consent management solutions**
   - A clear articulation of common Business Requirements will help vendors in developing consent management solutions that meet stated pan Canadian requirements.
   - This section will provide insight into the technical Business Requirements of a consent management solution.

3. **Information Technology specialists**
   - Business level definition of solution requirements is the first phase to ensuring that Information Technology (IT) solutions meet business needs. IT specialists can leverage the definition of common business requirements to develop or choose the appropriate technology solutions.

---

\(^9\) The term ‘enterprise’ is used in this section to refer to solutions that are implemented at the jurisdiction rather than local level.
This section is organized in the following groupings:

- Access and authorization to consent management solution
- Solution configuration
- Data capture, storage, retrieval and enforcement of directives
- Reporting and analytics
- Maintenance of historical data and archiving
- Notification and alerts
- Conflict identification/ resolution
- Overrides
- Logging
- Viewing of data

The following guiding principles build on the guiding principles set out in the Introduction of the paper. These guiding principles relate specifically to architectural considerations of consent management solutions:

- The solution MUST be configurable:
  - Configuration of the product is the responsibility of the organization that is implementing the CMS.
  - Due to the variability of business requirements across jurisdictions it is important that consent management solutions support a user driven capability to configure the consent management solution to meet jurisdiction specific requirements. These configurable features will accommodate policy-based requirements that may change over time. The configuration of consent solution parameters would also include the ability to turn on or off certain features. Configurable features include but are not limited to the following:
    - Support configuration for bilingual interfaces for administrators and end users of the CMS.
    - A variety of consent models, which include, but are not limited to implied or express consent models.
    - Levels of granularity for masking directives.
    - Consent directive duration.
    - Consent for override and override duration.
In 2008 and 2009, for its iEHR Technical Projects I and II, Infoway collaborated with its stakeholders to develop requirements for a consent management solution. These requirements were reviewed and further developed by this project’s Working Group. The results are the business requirements listed in the table below. Architecture requirements will be addressed in section 10: Functional Requirements of a Consent Management Solution. Included in that section are requirements such as message-based interface, creation and storage, and identity and access management.

It bears repeating that the business requirements documented below are intended to provide guidance to jurisdictions which may be considering the development or procurement of a CMS. The requirements are written from a pan-Canadian perspective. It is a high level series of business requirements including potential future-oriented requirements that will provide a framework for jurisdictions.

It is important to note that the business requirements are written using the terms ‘MUST’ and ‘should’ intentionally. Where a requirement is identified as a ‘MUST’, the expectation is that vendors include it as a feature or functionality of a CMS product. Where the term ‘should’ is used, the expectation is that vendors may include this feature or functionality in a CMS product.

Finally, jurisdictions will determine which of these requirements are applicable to them and undoubtedly will need to provide vendors with more detail on their specific requirements. It is also important to note that the choices made may impact interoperability of the consent solution.

<table>
<thead>
<tr>
<th>#</th>
<th>Business requirement (BR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BR1</td>
<td>The Consent Management Solution (CMS) <strong>MUST</strong> have Identity Management (IDM) capability whether this is part of the solution or it integrates with an external IDM solution. This requirement allows for the definition and management of the identities of those who administer the system. Using external IDM capabilities enables any existing jurisdictional IDM system to be leveraged which will eliminate the need for multiple system users to have multiple IDs and passwords. The CMS <strong>should</strong> integrate with external IDM solutions used as part of Consumer Health Solutions, Portals and Personal Health Record solutions.</td>
</tr>
<tr>
<td>#</td>
<td>Business requirement (BR)</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BR2</td>
<td>The CMS <strong>MUST</strong> support Role Based Access Controls (RBAC) for all system users. The definition of roles for system users, administrators, and individuals are to be supported. The administration of roles <strong>MUST</strong> be a configurable feature of the CMS.</td>
</tr>
<tr>
<td>BR3</td>
<td>The CMS <strong>MUST</strong> enforce individual consent directives and jurisdictionally specified rules.</td>
</tr>
<tr>
<td>BR4</td>
<td>The CMS <strong>MUST</strong> provide for the ability to create, store, change and remove an access code (keyword, password) when used for the masking/unmasking of PHI. The activation of this feature <strong>MUST</strong> be a configurable feature in order to meet varied jurisdictional requirements. Management of keywords <strong>should</strong> take into account the possibility of interfaces with Consumer Health Solutions, Portals and Personal Health Record solutions.</td>
</tr>
<tr>
<td>BR5</td>
<td><strong>Solution configuration</strong></td>
</tr>
<tr>
<td></td>
<td>The CMS <strong>MUST</strong> support, in both official languages, administrative functions for the configuration and management of the CMS. For example:</td>
</tr>
<tr>
<td></td>
<td>1. Consent forms (paper and electronic)</td>
</tr>
<tr>
<td></td>
<td>2. Various drop-down lists related to consent directive management and access, e.g. jurisdictionally determined reasons for consent override</td>
</tr>
<tr>
<td></td>
<td>3. Notifications (alerts), including but not limited to:</td>
</tr>
<tr>
<td></td>
<td>o those which are configurable to meet jurisdiction specific alert protocols</td>
</tr>
<tr>
<td></td>
<td>o the conditions under which an alert is generated</td>
</tr>
<tr>
<td></td>
<td>o definition of which users should receive alerts and how (e-mail, system flag, fax, pager)</td>
</tr>
<tr>
<td></td>
<td>o whether the system would generate a letter to send to individuals if an override has been activated</td>
</tr>
<tr>
<td>BR6</td>
<td>The CMS <strong>MUST</strong> support the configuration and management of jurisdictionally specified consent models and default rules such as;</td>
</tr>
<tr>
<td></td>
<td>• Level of granularity of consent directives</td>
</tr>
<tr>
<td></td>
<td>• Types of consent directives</td>
</tr>
<tr>
<td></td>
<td>• Use of keywords</td>
</tr>
<tr>
<td>#</td>
<td>Business requirement (BR)</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------</td>
</tr>
<tr>
<td><strong>Data capture, storage, retrieval and enforcement of directives</strong></td>
<td></td>
</tr>
<tr>
<td><strong>BR7</strong></td>
<td>The CMS <strong>MUST</strong> support the ability to capture an individual’s consent directives.</td>
</tr>
<tr>
<td><strong>BR8</strong></td>
<td>The capture, update and de-activation of consent directives <strong>MUST</strong> support the use of structured data elements including but not limited to the following:</td>
</tr>
<tr>
<td></td>
<td>1. Types of consent:</td>
</tr>
<tr>
<td></td>
<td>- Collection of PHI in the EHR</td>
</tr>
<tr>
<td></td>
<td>- Use of PHI for care</td>
</tr>
<tr>
<td></td>
<td>- Disclosure of PHI</td>
</tr>
<tr>
<td></td>
<td>- PHI for Health System Use (HSU) including:</td>
</tr>
<tr>
<td></td>
<td>- Clinical program management</td>
</tr>
<tr>
<td></td>
<td>- Health system management</td>
</tr>
<tr>
<td></td>
<td>- Population health surveillance</td>
</tr>
<tr>
<td></td>
<td>- Research</td>
</tr>
<tr>
<td></td>
<td>2. The identifier of the individual recording the consent directive</td>
</tr>
<tr>
<td></td>
<td>3. Jurisdictionally determined customizable fields which identify categories of data, e.g. genetic information</td>
</tr>
<tr>
<td></td>
<td>4. PHI disclosure exclusion and inclusion categories, e.g. by provider, organization, application, clinical domain</td>
</tr>
<tr>
<td></td>
<td>5. How consent directives were received, e.g. in writing, form, verbally</td>
</tr>
<tr>
<td></td>
<td>6. Relevant dates such as start and end dates for consent directives.</td>
</tr>
<tr>
<td></td>
<td>7. Reason for override and identifier of person overriding an individual’s consent directive.</td>
</tr>
<tr>
<td></td>
<td>8. Relevant dates for an override, such as duration and change to expiry date.</td>
</tr>
<tr>
<td></td>
<td>9. An individual’s request for ‘no override without consent under any circumstances’ and prevent override as requested.</td>
</tr>
<tr>
<td></td>
<td>10. Name and relationship of substitute decision makers/proxy who are providing consent on an individual’s behalf</td>
</tr>
<tr>
<td></td>
<td>11. The unique client or individual identifier</td>
</tr>
<tr>
<td></td>
<td>12. The unique provider, clinician or administrative staff identifier</td>
</tr>
<tr>
<td></td>
<td>13. Location of paper or scanned consent directives in document format, e.g. scanned paper forms, PDF documents.</td>
</tr>
</tbody>
</table>

**Note:** Consent directives may be captured using standalone consent processes such as a separate centrally managed consent application supported by a HELP desk. Paper copies may be retained locally or submitted in bulk for central storage.
<table>
<thead>
<tr>
<th>#</th>
<th>Business requirement (BR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BR9</td>
<td>The CMS <strong>MUST</strong> allow for configurable fields (combination box, drop-down lists, yes/no).</td>
</tr>
<tr>
<td>BR10</td>
<td>The CMS <strong>MUST</strong> support the administration of data elements to be captured.</td>
</tr>
<tr>
<td>BR11</td>
<td>The CMS <strong>MUST</strong> have the ability to store consent directives in a central repository within or external to the product and support the ability to read data stored in the central repository.</td>
</tr>
<tr>
<td>BR12</td>
<td>The CMS <strong>MUST</strong> support the capture and management of multiple consent directives for an individual.</td>
</tr>
<tr>
<td>BR13</td>
<td>The CMS <strong>MUST</strong> support the storage, retrieval and viewing of status (e.g. active, inactive) for a specific consent directive.</td>
</tr>
<tr>
<td>BR14</td>
<td>The CMS <strong>MUST</strong> have the ability to retrieve or view a list and the details of an individual’s current consent directives and his or her history, including overrides and directives stored in external repositories or other EHRs within a jurisdiction.</td>
</tr>
<tr>
<td></td>
<td>The CMS <strong>should</strong> support the ability of Consumer Health Solutions, Portals and Personal Health Record solutions to retrieve and view the details of an individual’s current and historical consent directives, including overrides and directives stored in external repositories or other EHRs within a jurisdiction.</td>
</tr>
<tr>
<td>BR15</td>
<td>For authorized users, the CMS <strong>MUST</strong> support retrieval and viewing of who has viewed, accessed, overridden and/or updated an individual’s consent directives.</td>
</tr>
<tr>
<td>BR16</td>
<td>The CMS <strong>should</strong> support the merging or separation of multiple consent directives, e.g.:</td>
</tr>
<tr>
<td></td>
<td>• In the event that EHR records with different unique identifiers e.g. Health Insurance Numbers or eCID’s, are identified as belonging to the same person; or records with the same unique ID are identified as belonging to different people, the CMS should support the merging and unmerging of consent directives.</td>
</tr>
<tr>
<td>BR17</td>
<td>The CMS <strong>MUST</strong> provide support for the unique identification of individuals, including proxies and substitute decision makers.</td>
</tr>
<tr>
<td>#</td>
<td>Business requirement (BR)</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------</td>
</tr>
</tbody>
</table>
| BR18 | The CMS **MUST** be able to:  
- Establish the association between the PHI and the conditions under which it may be disclosed  
- Enforce consent directives after data is requested and before it is transmitted to the requestor  
- Block the transmission where it would violate a directive and where no exception for such a disclosure exists; and  
- Inform POS systems that a consent directive exists and provide an option for how to proceed. |
| BR19 | The CMS **MUST** record, store (in the Consent Repository), retrieve, interpret and support multiple ways of applying (in conjunction with other HIAL Common Services as necessary):  
- Consent related business rules to manage a person’s consent directives and allow authorized users to comply with, or override (where permitted) such directives when retrieving or updating PHI  
- Consent disclosure rules, e.g. role-based access permissions  
- Masking rules which indicate for example:  
  o Who has access to the masked data and who does not  
  o The duration of a user’s access to view masked information e.g. end date (where applicable). |
| **Reporting and analytics** |  
| BR20 | The CMS **MUST** have ability to produce reports. This **MUST** be a configurable feature. Reports **MUST** be soft and/or hardcopy.  
  
A basic set of reports **should** be available and include but is not limited to the following:  
- Consent directives history report (by individual, by date range)  
- CMS administration log report (how many directives applied and for which domain)  
- Access log report (by location, by user, by role, by individual, by date range)  
- Consent directives override report  
- CMS metrics as determined by the solution administrator |
<p>| BR21 | The CMS <strong>should</strong> support the export of data to external analytics solutions. |</p>
<table>
<thead>
<tr>
<th>#</th>
<th>Business requirement (BR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Maintenance of historical data and archiving</strong></td>
</tr>
</tbody>
</table>
| BR22 | The CMS **MUST** support the storage and retrieval of an individual’s historical consent directives and associated overrides.  
The time period for the duration of an individual’s consent **MUST** be a configurable feature in order to meet specific jurisdictional requirements. |
| BR23 | The CMS **MUST** have the capability to archive information either internally or externally to the CMS. |
|    | **Notification and alerts** |
| BR24 | The CMS **MUST** support the generation of system alerts to authorized system users. The following are examples of system alerts that **should** be supported;  
- Unauthorized viewing and / or updating of consent directive attempts, for example:  
  - Where x number of unsuccessful attempts have been made to log in (system log location and map location to individual to be notified e.g. Privacy Officer assigned to facility)  
- Override of an individual’s consent directives by a health care provider or other person  
- The system also should be configurable to generate a letter directed to the individual whose data has been accessed through an override  
- Failure in creating or modifying an individual’s consent directives  
- Failure to override a consent directive  
- Confirmation of masking/removal of masking for a record or category of records (where masking is implemented).  
The generation of system alerts **MUST** be a configurable feature assigned to administrative personnel. |
<p>|    | <strong>Conflict identification/resolution</strong> |
| BR25 | The CMS <strong>MUST</strong> support the identification, notification and resolution of consent rule conflicts between new or modified and existing rule sets at the time of consent rules capture. |</p>
<table>
<thead>
<tr>
<th>#</th>
<th>Business requirement (BR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Overrides</strong></td>
</tr>
</tbody>
</table>
| BR26 | The CMS **MUST** support the override of an individual’s consent directives, for example, in a medical emergency, or when the individual is deemed a danger to him/herself or others. (This assumes override is permitted under jurisdictional legislation or policy.)  

For an override, the CMS **MUST** capture the user, location, reason and duration of the override as well as whether the override was activated based on consent by either the individual or substitute decision maker/proxy or without consent (as permitted by legislation).  

This **MUST** be a system administrator configurable feature. |
|    | **Logging**                                                    |
| BR27 | The CMS **MUST** log all actions related to the CMS and consent directives.  

This **MUST** be a system administrator configurable feature. |
|    | **Viewing of data**                                           |
| BR28 | The CMS **MUST** allow CMS IT system administrators, to access and view Consent Directives and related override details electronically when necessary for system administration or support.  

The CMS **should** allow an individual to access and view his or her consent directives and related override details electronically. |
7. Architecture: An introduction

The previous sections of this document have outlined business considerations and requirements of a Consent Management Solution. In the architecture sections of this document, the architectural options and considerations for a solution are presented.

As part of the pan-Canadian review of the consent directive landscape, considerable variations in jurisdictional requirements were identified. The architectural options are based on the principles identified in the ERHS Blueprint and Common Security Services\(^\text{10}\) and on these variations in jurisdictional requirements. As a result this document will present several architectural solution options as information for consideration when jurisdictions are in the process of designing, acquiring and implementing a CMS. The document will discuss considerations for exchanging consent directives in a way that allows for solutions to interact with one another by using standard messaging and taxonomy.

The main functionality of a CMS includes the creation, storage, management and enforcement of consent directives. The CMS also offers auditing, reporting and analytics as supporting functionalities. These functions are described in this section.

This section will expand on three architectural deployment options for a CMS:

- Central consent management
- Consent management as part of clinical domain
- Federated consent management

These options are based on a review of Canadian jurisdictions. The ‘central consent management’ and ‘consent management as part of clinical domain’ models were the most commonly described in the material reviewed. In review with the project Working Group, it has been recognized that a ‘federated consent management’ model may meet the near future needs of some jurisdictions.

PROJECTS THAT HAVE INFORMED THE CMS ARCHITECTURE CONSIDERATIONS

As indicated in the Project Scope section in the Introduction of this document, the scope of the architecture sections includes the CMS, interfaces and connection points to supporting EHR systems and common services, mechanisms for the exchange of consent directives, and architectural, design and deployment options for the CMS. Previous work listed below completed by Canada Health Infoway in the area of consent has also been levered and taken into consideration, including

---

\(^{10}\) Blueprint and Common Services, Canada Health Infoway
- iEHR Technical Project (Tech I) (2007)
- iEHR Technical Project II (Tech II) (2008)
- Electronic Health Record Solution (EHRS) Blueprint (2003; revised 2006)

For more information about these projects and initiatives, see Appendix E.
8. Architectural deployment models and considerations

There are many different design and deployment options for a Consent Management Solution. Consent directives can be managed at different levels, including jurisdictional, regional and POS. This section of the document discusses three generic consent solution deployment models: ‘centralized consent management’, ‘consent management as part of the clinical domain’, and ‘federated consent management’. These models are described from the perspective that all components of the CMS (capture, storage, management and enforcement), are deployed in a common way. However, it is also possible to have hybrid design and implementation solutions, for example, centralized capture, storage and management with domain-based enforcement.

Further, in some jurisdictions, different legislation may apply to the EHRi and local POS and may involve different rules for each, some of which may relate to consent management. For example, in a particular jurisdiction, an individual may be permitted to mask all or no PHI in a jurisdictional data repository; however at the acute care facility in the same jurisdiction, an individual may be able to mask information from all but one provider. The legislation may provide for both of these scenarios.

Since several consent models may co–exist simultaneously within a jurisdiction, business owners and solution designers must assess the associated operational and system management tradeoffs. For example, when there are several different consent deployment models in a jurisdiction, there may be different processes and solutions for capturing, storing and managing consent directives, which may make interoperability more difficult to achieve across the jurisdiction. This may result in a fragmented approach and additional complexity to managing and enforcing consent directives which, in turn, may not support the individual’s directions. The deployment model considerations associated with this complexity will be discussed in section 11 CMS Architectural Considerations, Co-Existence of Multiple Consent Models.

It is important to note that the deployment models presented in this section are intended to be generic models or patterns of deployment. It is understood that within each generic model a jurisdiction may consider specific deployment scenarios which are dependent on their current or future CMS component deployments. These specific deployment scenarios are not covered in this section.
The presentation of the deployment models is structured in the following sequence:

1. A high level description of the model and its core assumptions.
2. A high level diagram illustrating each of the major components of the deployment model.
3. A discussion of the architectural considerations specific to each model.

CENTRALIZED CONSENT MANAGEMENT DEPLOYMENT MODEL

A centralized CMS model is an enterprise level or jurisdiction-wide implementation of a consent management solution. It typically has centralized capabilities to capture, store, enforce, and provide management features. In the context of an EHR, the centralized CMS is part of the Privacy and Security Common Services and relies on the HIAL to provide enforcement. This deployment model has a centralized store for the consent directives and a common messaging format and interface standard for interactions with other systems. These interfaces are used by other systems that need to have knowledge of or update consent directives. In a centralized CMS model, all consent directives are in one system, one place, thereby reducing the likelihood of any misapplication or omission of an individual’s consent wishes.

Diagram A is an illustration of a centralized CMS model. In this illustration the components of the CMS are as follows:

- The capture of a consent directive generally takes place using a viewer such as the EHR viewer or other centralized mechanism that may be deployed in a decentralized manner.
- The storage of the consent directives is managed by the Consent Repository.
- The enforcement takes place and is managed by the HIAL.
- The policy management is managed by the Consent Repository for the rules, and by the EHR Viewer for the user interface component.

This deployment model is based on the following core assumptions:

- The CMS deploys all components in a centralized manner including capture, storage and enforcement.
- The CMS rules and audit features operate in a centralized manner.
- Consent directives are captured via a CMS interface (i.e. a user interface, or a web service) that can be accessed from multiple locations and by multiple users depending on jurisdictional requirements.
The level of consent granularity is determined and enforced by the centralized deployment of the CMS. Multiple levels of consent granularity can co-exist as required.

The core components of the Centralized CMS model are:

- A centralized consent repository
- A centralized CMS functionality within the HIAL operating within a Services Oriented Architecture (SOA)
- A CMS web interface supporting the capture and management of directives
Diagram acronyms

- **R PHI** – Restricted Personal Health Information i.e. a masking or disclosure restriction is applied to this information
- **CDD** – Consent Directive Data

Together with legislation, policy and technological considerations, there are a number of features and requirements specific to a centralized CMS deployment that should be considered. While this is not a comprehensive list, it should be noted that a centralized CMS deployment model provides:

- Consistent messaging and terminology
- Common mechanisms for the capture, storage, update, and deactivation of a consent directive
- A common interface to facilitate enforcement, reporting, and auditing of consent directives
- A single mechanism for analytics and reporting
- Centralized access to consent data for data warehousing for statistical and analytical purposes
- A standardized mechanism for managing rule-sets to accurately and consistently respect an individual’s wishes

In order to successfully deploy this model, jurisdictions need to create a design, deployment and operational strategy that takes into consideration the harmonization of existing consent management policies.

**DOMAIN-BASED CONSENT MANAGEMENT DEPLOYMENT MODEL**

Currently the clinical domain based consent management deployment model is being used by most jurisdictions in Canada. In this model each of the clinical domains has its own consent management solution. This means that consent management is integrated within the clinical domain solution and the capture, storage and enforcement of consent directives take place within the clinical system. Diagram B illustrates where consent directives are stored and managed in relation to the broader architecture.

Clinical domain repositories include internal components for the management of the consent rules. Most clinical domain repositories do not have capability to share consent information with other information systems without modification. In a domain-based model, consent directives are registered separately for each of the domains. In the event that an individual wants a consent directive to span several clinical domains, the consent directive is entered multiple times. The domain-based model also does not allow for seamless integration of
consent messages with POS systems since the domain-based deployment model may not have the capability to share consent information with external systems. In order to provide such functionality, interfaces must be developed.

This deployment model is based on the following core assumptions:

- CMS functionality exists within the clinical domain repository.
- The CMS within the clinical domain repository is not currently sharing or capable of sharing consent directives and/or consent rules with other components of the EHR.
- The level of consent granularity functionality may vary by clinical domain repository.
- Consent directives are recorded, stored and enforced using mechanisms that are specific to each clinical domain repository.

Some consent management functionality exists in most clinical domain repositories deployed across the country. Together with legislation, policy and technological considerations, there
are a number of features and requirements specific to a domain-based CMS deployment that should be considered. While this is not a comprehensive list it should be noted that a domain-based CMS deployment model:

- Provides implementation and management within the context of a single clinical domain repository.
- Provides the potential for rapid implementation of domain-specific rule sets and consent policies.
- Requires management of multiple locations to create, store, enforce, and manage rule-sets for directives.
- May require more complex arrangements than other models for creating, updating and deactivating consent directives and for logging, auditing and reporting of directives.
- Requires the consideration of the total cost of ownership including the potentially lower cost for design and deployment per clinical domain, and the potentially higher cost for managing multiple consent stores, rule sets and enforcement points.

FEDERATED CONSENT MANAGEMENT SOLUTION DEPLOYMENT MODEL

The term ‘federation’ can refer to multiple computing and/or network providers agreeing upon standards of operation in a collective fashion. The term may be used when describing the inter-operation of two distinct, formally disconnected, telecommunications networks, IT infrastructures and/or business solutions that may have different internal structures.

The federated CMS deployment model offers many possible deployment scenarios. The CMS can be federated by having multiple purpose-built CMS-to-CMS federations. This may include a domain CMS to domain CMS federation, or a domain CMS to a centralized CMS federation, or finally a centralized CMS federated to multiple other centralized CMS deployments. These scenarios depend upon jurisdictional design decisions, policies, and integration/evolution of current systems. Regardless of the deployment scenarios, the following core assumptions apply:

- Common functionality between federated CMSs.
- Common taxonomy, and information exchange format (i.e. messaging format).
- The federation is instantiated between CMS components at or above the HIAL. (Federation between CMS at the POS level and CMS in the HIAL are not part of this deployment model.)
- The same level(s) of consent granularity must be supported between federated CMSs.
A federated consent management model is distributed in nature. In other words, the solution components may reside in a number of locations. The manner in which the components work together can vary; there can be multiple instances of the same CMS distributed across various locations or different functions of a comprehensive solution may be dispersed. For example, each instance of a CMS could support a subset of the overall functionality of capturing, storing, or enforcing consent directives.

Irrespective of the distribution arrangement, a key requirement of a federated solution is not only that all system components must work in tandem to provide a coordinated solution, but that there also be a harmonized approach to consent rule sets and overall CMS functionality. It can be challenging to maintain this level of harmonization and synchronicity in a federated solution -- the systems can become out of synch and harmonization of rule sets difficult to achieve and maintain.

For example, in a federated CMS deployment model, an instance of a CMS holds an individual’s consent directives. These consent directives may need to be synchronized with other federated CMSs in order to ensure the interoperability of consent directives across the federated model. Synchronization triggers should be designed to ensure the replication of consent directives across all the CMS components in a timely manner.

That being said, in jurisdictions with multiple operational CMSs which are deployed in a standardized manner, the federated approach may be the best approach for creating a jurisdiction-wide solution. It may also be a viable interim solution for jurisdictions considering migration from a domain-based model towards a centralized model. Some jurisdictions may purposefully choose a federated model as it can build redundancies into the system which prevent a single point of failure.

One example of a federated model is presented in Diagram C. In this illustration, the capture, store, and consent rule set enforcement take place in a number of Consent Repositories geographically dispersed across the jurisdiction. These CMSs synchronize consent directives and consent management rules, as well as logging information for auditing purposes. The enforcement may be provided by a single, common HIAL, although it is possible to have multiple regional HIALs synchronized to provide the enforcement functionality.

Alternatively, if domain-specific CMSs are federated into an overall jurisdictional solution, the enforcement and management of directives may occur within the clinical domain CMS.

A federated model can include many sub-scenarios, including one which takes into consideration POS systems. As each instance may be unique, this paper does not address the many potential scenarios which may be faced by jurisdictions.
Several jurisdictions are contemplating a series of federated interoperable EHRs (iEHRs), each having the ability to function both independently and in conjunction with each other when required. It is expected that the federated CMS deployment model would be able to function within the iEHR implementation model as long as synchronization and availability issues have been addressed.
Together with legislation, policy and technological considerations, there are a number of features and requirements specific to a federated CMS deployment that should be considered. While this is not a comprehensive list it should be noted that a federated CMS deployment model:

- Can integrate existing consent data-stores to build the solution.
- Can be used as a building block and interim solution towards a centralized CMS, should a jurisdiction choose that option.
- Can build in redundancies which can prevent a single point of failure.
- Accommodates large systems if there is a harmonized model in place.
- Requires synchronization of consent directives.
- May require additional components and infrastructure to facilitate synchronization and availability of the federated components of the CMS.
- Requires consent directives based on standards and/or specifications to share directives across the federated landscape.
- May need to upgrade and/or change an existing CMS in order to support the federated deployment model.
- This model can be cost effective if existing solutions have taken a standardized approach as existing solution components can be leveraged.
CMS DEPLOYMENT MODEL COMPARISON

The following table presents a comparison of the three CMS deployment models.

<table>
<thead>
<tr>
<th>Comparison of Consent Management Deployment Models</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TYPE</strong></td>
</tr>
<tr>
<td>Centralized</td>
</tr>
<tr>
<td>A centralized CMS model is an enterprise or jurisdiction-wide level implementation of a consent management solution</td>
</tr>
<tr>
<td>The CMS will deploy all components in a centralized manner including capture, storage and enforcement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CMS USER INTERFACE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
</tr>
<tr>
<td>Common interfaces provide functionality, including for example, the capture, storage, update, enforcement, management, and auditing of consent directives</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>STORAGE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
</tr>
<tr>
<td>Storage takes place in a single consent or other dedicated repository</td>
</tr>
</tbody>
</table>
Business and Architecture Considerations for Interoperable Consent Solutions: A discussion document

Design considerations for the synchronization of directives based on standards and/or specifications is required to support the federation of CMSs.

### MESSAGING/STANDARDS/SPECIFICATIONS

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Domain-based</th>
<th>Federated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized deployment uses a common messaging, terminology and interface standard for interactions with other systems</td>
<td>Each domain CMS has a specific messaging and terminology format. Sharing of consent directives across domains is not performed.</td>
<td>Federated CMS deployment relies on common messaging and terminology standards to share consent directives across the federated CMSs</td>
</tr>
</tbody>
</table>

### HIAL

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Domain-based</th>
<th>Federated</th>
</tr>
</thead>
<tbody>
<tr>
<td>All interfaces to the CMS are via the HIAL using standardized messaging.</td>
<td>CMS interfaces are not managed by the HIAL. Interfaces to CMS functionality are via the domain interface.</td>
<td>All interfaces to the CMS are via the HIAL using standardized messaging. This includes communication between HIALs and/or domains.</td>
</tr>
</tbody>
</table>
### CAPTURE

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Domain-based</th>
<th>Federated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent directives are captured through a central single interface mechanism (e.g. user interface, web service) which can be accessed through multiple locations by multiple users</td>
<td>Consent directives are captured in each of the clinical domain specific user interfaces.</td>
<td>Consent directives are captured using CMS interfaces specific to each CMS. Content and functionality of this process must at a minimum be harmonized across the federated entities.</td>
</tr>
</tbody>
</table>

### ENFORCEMENT

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Domain-based</th>
<th>Federated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforcement and management of the rule sets and consent directives takes place in the CMS common service within the HIAL</td>
<td>Enforcement and management of the consent directives and rule sets takes place within the clinical domain repositories</td>
<td>Enforcement and management of the rule sets and consent directives may take place within the CMSs responsible for the data query. This may occur in either the HIAL based CMS, a federated HIAL CMS, or a domain based CMS across the jurisdiction</td>
</tr>
</tbody>
</table>

Centralized CMS functionality is located in the HIAL and operates as a service in compliance with Services Oriented Architecture (SOA) as part of the Privacy and Security Common Services and will rely on the HIAL to provide enforcement |

Each clinical domain solution has its own mechanism for enforcement |

Federation is instantiated between CMS components at or above the HIAL |

Enforcement may be provided by a single common HIAL, although it is possible to have multiple regional HIALs synchronized to provide the enforcement functionality |
If domain-specific CMSs are federated into an overall jurisdictional solution, the enforcement of directives may occur within the clinical domain repository CMS.

### MANAGEMENT / MANAGE RULE SETS

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Domain-based</th>
<th>Federated</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS manages rule-sets and audit features centrally</td>
<td>Multiple locations and methods to manage rule-sets for directives</td>
<td>Federated CMS deployments require a harmonized approach to consent rule sets and overall CMS functionality</td>
</tr>
<tr>
<td>A centralized CMS has a standardized mechanism for the management of rule sets.</td>
<td>Each clinical domain solution has its own mechanism for rule set management which may vary in functionality</td>
<td>Synchronization and harmonization of management functionality is required for the interoperability of rule sets.</td>
</tr>
<tr>
<td>Rule set management occurs in the Centralized Consent Repository. Common interfaces are provided by the CMS for the purpose of managing the CMS rule-sets, and access the auditing interfaces.</td>
<td>Rule set management occurs within each domain based CMS. Each domain CMS has a unique Consent Repository and user interface.</td>
<td>Rule set management can occur in the Consent Repositories or can happen at the domain depending on the federation model utilized.</td>
</tr>
<tr>
<td>The level of consent granularity is determined and enforced by the centralized deployment of the CMS</td>
<td>Each domain can have its own level of granularity</td>
<td>The level of consent granularity is determined and enforced by each of the federated CMSs. The consent granularity levels must be harmonized to allow for interoperability.</td>
</tr>
</tbody>
</table>
Multiple levels of consent granularity can co-exist as required, provided they are harmonized across the federation.

<table>
<thead>
<tr>
<th>IMPLEMENTATION/COST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized</strong></td>
</tr>
<tr>
<td>Possible lower overall cost of consent management in a jurisdiction, especially when taking into consideration the reduced maintenance costs of several solutions associated with other deployment models.</td>
</tr>
<tr>
<td>In a centralized deployment model jurisdictions need to invest in creating a design, deployment and operational maintenance strategy that takes into consideration harmonization of consent management policies at the existing domain-based deployments, gathering and integrating all stakeholder requirements and providing overarching governance. All these issues can add to the complexity and initial investment into the CMS</td>
</tr>
<tr>
<td>Initial investment could be higher than other deployment models</td>
</tr>
</tbody>
</table>
Allows for simplified implementation and management within the context of single clinical domain repository

Mechanisms are required to inform all CMS enforcement points of the existence of a consent directive. This can be achieved by synchronization or indexing.

Most clinical domains solutions do not have capability to share consent information with other information systems without modification

Multiple tasks are required to ensure consent directives are created, updated, and deactivated in more than one domain which can increase the effort required to manage and maintain the overall solution

### LOGGING / AUDIT / REPORT

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Domain-based</th>
<th>Federated</th>
</tr>
</thead>
<tbody>
<tr>
<td>The functions of logging, auditing and reporting are centralized as part of the CMS common services.</td>
<td>Multiple locations and methods for logging, auditing and reporting</td>
<td>Audit logs may exist on multiple systems. Functionality may be required for synchronization, and is required for consolidation and correlation of these logs in order to provide auditing, reporting, and analytics.</td>
</tr>
<tr>
<td>A single mechanism for supporting analytics and reporting</td>
<td>Each clinical domain solution has its own mechanism for logging, auditing, reporting and providing analytics</td>
<td>A single or harmonized mechanism for supporting analytics and reporting</td>
</tr>
</tbody>
</table>
## INTEGRATION

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Domain-based</th>
<th>Federated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration to a common CMS is facilitated by having a single interface for messaging and terminology</td>
<td>Most clinical domains do not natively have capability to share consent information with other information systems without modification</td>
<td>Federated CMS deployment model would be able to function within the iEHR implementation model as long as synchronization and availability issues have been addressed.</td>
</tr>
<tr>
<td></td>
<td>Does not allow for efficient integration of consent messages with other systems as each domain CMS has a different messaging and terminology format. Additionally, the domain-based deployment CMS may not have the capability to share consent information with external systems</td>
<td>All system components must work in tandem to provide a coordinated solution</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flexible implementation possibilities, e.g.:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multiple instances of the same CMS distributed across various locations</td>
</tr>
</tbody>
</table>

## DEPLOYMENT IMPLICATIONS

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Domain-based</th>
<th>Federated</th>
</tr>
</thead>
<tbody>
<tr>
<td>A centralized CMS model where all consent directives are stored in one repository using a common consent rule-set, minimizes the potential to misapply or omit an individual’s consent wishes</td>
<td>Consideration should be given when multiple consent rule-sets are required to prevent conflicts</td>
<td>A federated CMS deployment model offers many possible deployment scenarios, e.g.:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Clinical domain solution CMS to clinical domain solution CSM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Clinical domain solution CSM to centralized CMS</td>
</tr>
<tr>
<td>Easy access to consent data</td>
<td>Consideration should be</td>
<td>Federation between CMS at</td>
</tr>
<tr>
<td>for data warehousing for statistical and analytical purposes</td>
<td>given to accommodate creating, updating or deactivating consent directives for an individual who has consent directive in multiple clinical domain solutions</td>
<td>the POS level and CMS in the HIAL are not part of this deployment model.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Analytical capability must take into account the fact that each clinical domain solution has its own mechanism for logging, auditing, reporting</td>
<td>The same level(s) of consent granularity must be supported between federated CMS’s</td>
<td></td>
</tr>
<tr>
<td>Implementing on a domain by domain basis can accommodate differing objectives and timelines</td>
<td>Redundancies can be built into the system to prevent a single point of failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If existing solutions have taken a standardized approach, this model can be cost effective since existing solution components may be utilized</td>
</tr>
<tr>
<td></td>
<td>Can be used as a building block and interim solution towards a centralized CMS solution</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>May need to upgrade and or change an existing CMS in order to support the federated deployment model</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If there is a harmonized model in place, this can provide an excellent solution for large deployments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A robust design is required in order to introduce harmonization and</td>
</tr>
</tbody>
</table>

February 29, 2012
Business and Architecture Considerations for Interoperable Consent Solutions: A discussion document
CMS INTEGRATION TO POINT OF SERVICE APPLICATIONS

The previous sections discuss the possible CMS deployment models operating at the HIAL or domain level. These will be referred to as EHR CMS models in the following section. The Working Group has confirmed that several POS applications, namely Hospital Information Systems (HIS) have a limited set of CMS capabilities. It is anticipated that POS applications will benefit greatly from a common set of CMS requirements, functionalities and design considerations. The following section will discuss CMS-enabled POS deployment models and implementation considerations. While several permutations of CMS-enabled POS deployment models exist, this section will focus on those having the highest probability of occurring in jurisdictions. Jurisdictions are encouraged to consider deployment models that best meet their business requirements and architecture context.

The following core assumptions are applicable to all CMS-enabled POS deployment models:

- The POS/CMS capable deployment models can be integrated into any of the three EHR CMS deployment models described above.
- It is assumed that POS applications wishing to implement their own CMS capability will incorporate the full range of CMS requirements and functionalities described in this document.
- The direct federation of CMS-enabled POS to other POS solutions is deemed unlikely therefore is not discussed in the CMS-enabled POS deployment models.
- A consent directive that restricts disclosure may need to be respected not withstanding where the PHI is stored. As an example, a consent directive (request to mask) placed on PHI at the jurisdictional clinical domain model may also apply to the same PHI if stored in a POS application. This implies that a POS CMS capable application may need to store, enforce and exchange standardized consent directives.
CMS-ENABLED POS ACCESSING MASKED PHI FROM EHR

In the event that a POS application accesses PHI stored uniquely in a jurisdictional clinical repository such as a Shared Health Record (SHR) or a Laboratory Information System, the consent directives would be enforced at either the clinical domain level (domain-based CMS Deployment Model) or at the HIAL level (centralized CMS deployment model). This is referred to as a rule enforcement point. Depending on the consent directive, the POS application would receive a response indicating that partial PHI was shared and masked PHI would not be shared with the POS applications.

The CMS-enabled POS application would not be required to enforce a consent directive as this would occur at the CMS enforcement point.

CMS-ENABLED POS ACCESSING LOCALLY MASKED PHI FROM POS

A CMS-enabled POS accessing locally stored masked PHI would be responsible for enforcing locally stored consent directives applicable to the locally stored PHI. This would ensure that locally stored and managed consent directives would be enforced upon a local access. However, it is possible that consent directives applicable to locally stored PHI could be captured and stored at the EHR level. In this case the directive applicable to the locally stored PHI would not be applied. In the event the above is possible, jurisdictions should give serious consideration to having the CMS-enabled POS consult the EHR level CMS(s) to ensure that an individual’s disclosure wishes are enforced.

The POS application can make standardized requests of the EHR CMS provided that its validation and enforcement capabilities are built in a SOA model and exposed to POS level applications.

Another consideration is a harmonized approach to the level of granularity between the EHR CMS(s) and the POS CMS. Consideration must also be given to architectural design issues associated with potential network capacity challenges associated with CMS-enabled POS solutions being required to access the EHR CMS for each access to locally stored PHI. Caching techniques are one of the possible solutions to this issue.

CMS-ENABLED POS ACCESSING PHI SHARED BETWEEN POS AND EHR REPOSITORIES

PHI may be stored simultaneously in both POS applications and in EHR repositories. A consent directive applicable to the shared PHI may be captured, managed, stored and enforced in either the POS or the EHR environments.

To ensure that an individual’s consent wishes are applied correctly it will be necessary for the CMS-enabled POS application to enforce any locally stored directives in addition to directives stored in the EHR CMS.
Several design options should be considered in this scenario. One option would be for the POS application to enforce locally stored directives and use an EHR CMS Application Programming Interface (API) to obtain the EHR CMS consent directive for analysis and subsequent enforcement. In this case the harmonization of consent directive level of granularity is critical to a successful implementation.

It is also important that the POS application be able to share and enforce EHR CMS stored consent directives. A common set of consent messaging specifications and taxonomy are critical to the implementation of this model.

**CMS-ENABLED POS SHARING MASKED PHI WITH ANOTHER POS SYSTEM**

In some implementations CMS applications may be directly connected to each other without the use of a HIAL intermediary. In the event that PHI which would normally be shared between POS applications such as an eReferral is masked, it is assumed that the source CMS enabled POS application would enforce any consent directives before sharing PHI. In this example, masked PHI would not be shared with another POS application. The CMS enabled POS application sharing PHI would be a consent rule enforcement point.

**CONSIDERATION FOR A DESIGN/DEPLOYMENT ROADMAP**

As noted in the Business Considerations sections, as jurisdictions evolve their approach to consent management there may be significant benefits to developing a transition plan or roadmap. There are infinite starting points for a roadmap, just as there are a multitude of existing and potential consent management solutions. As each jurisdiction develops its own roadmap and determines how best to implement and/or transition a CMS from one deployment model to another, it is important to take into account all potential business and architecture considerations, impacts and risks, deployment/operational costs and business strategies. This promotes a balanced approach to development of a deployment roadmap.

An example of a business consideration is the deployment of CMS enabled POS applications gradually over time. This infers that consent directives applied to PHI after data is stored in multiple POS applications may not be enforced equally across POS applications. The CMS deployment roadmap should take into consideration how various POS applications would or would not synchronize applicable consent directives as CMS enabled POS applications come online.

Domain specific CMSs are deployed in several jurisdictions and may eventually be migrated to a centralized CMS or into a federated CMS deployment model. In some cases a centralized model may be the ultimate deployment model goal. However, a jurisdiction may need to move to a federated model or a hybrid first. During the federated phase, several issues need to be taken into consideration, such as synchronization and harmonization of consent directives as they are created and updated.
Moving to a centralized model from a domain model can be complicated and requires detailed assessments and planning in a phased approach. Another approach could be for newer clinical domains joining the EHR infostructure to deploy a centralized consent management solution for the new domains and gradually introduce the existing domains to the centralized CMS.

A key component of a good consent management model is a consistent model. For instance, should a federated model be the model of choice, the system will function more seamlessly if each CMS within the entire solution is approached in the same manner.
9. Consent Management Design Requirements

ARCHITECTURAL

As part of the design requirements of the CMS, there are many elements that must be taken into consideration. The CMS must create, store, update, override, audit, and enforce consent directives. In order to provide these functions, the CMS must rely on other systems as part of the EHR infrastructure. Examples of these systems include the HIAL and the Client, Location and Provider Registries. As part of the overall CMS design, communication interfaces must be built and configured between these systems and the CMS.

The storage of the directive is also part of the CMS. In some designs, this takes place as part of the CMS; in others it can be part of the Client Registry (CR). Interfaces for the storage of the directive are required if the storage takes place in another system such as the CR.

Another consideration is the actual enforcement of the directive. In a centralized model, the HIAL is seen as the enforcement point. As such, the HIAL must be configured or possibly modified to have this type of capability. In addition to these architectural design requirements, jurisdictions must consider the use of standards when designing solutions.

CONSENT MANAGEMENT STANDARDS

In order for a CMS to be able to communicate consent directives with other systems, standards are required as a means for common interpretation of this information. A high level review was conducted of standards available in Canada and other jurisdictions. The review revealed the three most commonly used standards available today in offerings by Commercial off the Shelf (COTS) CMS solution vendors and in development or in the deployment pipeline in Canada and internationally. These standards are:

- A messaging approach based on a set of messaging standards and terminology
- Using a CDA document which carries consent information, and
- Use of Extensible Access Control Markup Language (XACML) as means to communicate consent directives.

For a high-leveled description of these standards for consent management solution see Appendix F.

OPERATIONAL

After the CMS is designed and deployed, there are other requirements to be considered, such as how to maintain the rule-set, provide reports and generate alerts.
Consent rules are the interpretation of jurisdictional policy and legislation. This interpretation allows for the definition of general consent rule sets. These general rule sets reflect the jurisdiction’s consent model and are configured within the CMS. The CMS then, in turn, creates rules in a format that can be understood by computer systems. Diagram D is an illustration of this process.

The level of granularity with which consent directives can be applied within a jurisdiction is an example of a type of rule that is configured within the system. It is important to note that the CMS must be in a position to allow for jurisdictional level general rule sets to evolve over time.
Rule management is an important part of the CMS as it is where consent directives, including exceptions such as overrides, are translated into enforcement actions. The CMS can provide the functionality for rule management; however a jurisdiction will need processes to support the creation of these rules. These rules can also potentially conflict with each other.

The CMS should also have capabilities to create alerts based on certain rules. Each jurisdiction has different requirements for alerting. For example some jurisdictions have requirements for near real-time alerts any time an override takes place. An organization that has the capability for centralized alert distribution and is integrating the CMS with other systems within the EHR, can utilize the alerting system to distribute alerts across systems.

As CMSs are more broadly deployed, there may be business requirements for statistics and analytics in general. Business requirements could include information relating to the number of consent directives and geographic breakdown. A method to support analytics should be included as part of the CMS design and deployment. This can either be accommodated within the CMS itself or through integration with another system. For example some jurisdictions make use of analytical tools such as an Enterprise Data Warehouse (EDW) which may be available for integration with the CMS to provide reports.
10. Functional Requirements of a Consent Management Solution

This section will address the definition of architecture level requirements for an interoperable consent management solution. The following requirements are applicable to a CMS notwithstanding the CMS deployment model or consent model used by a jurisdiction. Each of the requirements supports a full featured CMS.

Note that non-architectural requirements for an interoperable CMS are presented in the Business Requirements section. Included in that section are requirements such as access and authorization to CMS configuration, data capture and storage, consent directive overrides, logging, and reporting.

The ‘MUST’ and ‘should’ conventions expressed in the Business Requirements section hold true for this section as well. Moreover, as is the case in the Business Requirements section, due to the variability of requirements across jurisdictions, the architectural elements MUST be configurable to meet jurisdiction-specific requirements. These configurable features will accommodate policy-based requirements that may change over time. The configuration of consent solution parameters would also include the ability to turn on or off certain features. Such configuration is the responsibility of the organization that is implementing the CMS.

<table>
<thead>
<tr>
<th>#</th>
<th>Architecture requirement (AR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Message Based Interface</td>
</tr>
<tr>
<td>AR1</td>
<td>The CMS <strong>MUST</strong> generate and consume open industry published messages and /or APIs.</td>
</tr>
<tr>
<td>AR2</td>
<td>A common consent messaging format <strong>MUST</strong> be used by the CMS and all the other components of the EHR.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> See Appendix F: Inventory of existing standards for a description of three of these messaging formats.</td>
</tr>
<tr>
<td></td>
<td>Creation and Storage</td>
</tr>
<tr>
<td>AR3</td>
<td>The CMS <strong>MUST</strong> support the creation and storage of the consent directives.</td>
</tr>
<tr>
<td>AR4</td>
<td>The CMS <strong>should</strong> have the capability to allow administrators to create consent directives in a secure manner from point of capture to storage.</td>
</tr>
<tr>
<td>AR5</td>
<td>Consent directives <strong>MUST</strong> be stored securely while maintaining the integrity of the directive and protecting the directive against unauthorized modifications.</td>
</tr>
<tr>
<td>#</td>
<td>Architecture requirement (AR)</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td></td>
</tr>
<tr>
<td>AR6</td>
<td>The interface to the CMS is the mechanism through which other systems communicate with the CMS. The interface to the CMS <strong>MUST</strong> support capabilities to consume consent directives, update directives, and override directives, queries on directives, as well as queries on who/why/where an override took place. These interfaces <strong>should</strong> be standards based. The Interfaces <strong>MUST</strong> be open and published messages and / or APIs not withstanding whether they are vendor proprietary or not.</td>
</tr>
<tr>
<td><strong>Update and Deactivate</strong></td>
<td></td>
</tr>
</tbody>
</table>
| AR7 | The CMS **MUST** have the ability to intake updates when a directive is changed, and to modify or deactivate applicable directives.  
**Note**: In order to provide this functionality the CMS must have a way to uniquely identify each directive and its association to an individual. |
<p>| AR8 | The CMS <strong>MUST</strong> record a copy (either physically or logically) or a version of the directive prior to the update. |
| <strong>Audit and logging</strong> | |
| AR9 | The CMS <strong>MUST</strong> have the capability to configure the events to be logged. |
| AR10 | The log files <strong>MUST</strong> be readily available for audit purposes. |
| AR11 | The audit functionality of the CMS <strong>MUST</strong> be able to work with other components of the EHR that create logging events for access to PHI. |
| <strong>Reporting</strong> | |
| AR12 | The CMS solution <strong>MUST</strong> have the capability to produce reports. |
| AR13 | The reporting feature <strong>should</strong> be able to create reports as determined by the CMS system administrator for the audit events. |
| AR14 | The generation of reports <strong>should</strong> be highly configurable and based on individual, practitioner, timeframe, or any combination of these parameters. |
| <strong>Identity and Access Management (IDAM)</strong> | |
| AR15 | An IDAM solution allows the CMS to commonly identify users of the solution and creates a common identity that achieves single sign on (one user name and password) for users. It also creates a unique way to identify users across the EHR for auditing purposes. When an Enterprise IDAM solution is part of the EHR the CMS solution <strong>should</strong> support the capacity to integrate with the IDAM. |</p>
<table>
<thead>
<tr>
<th>#</th>
<th>Architecture requirement (AR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Archiving</strong></td>
</tr>
<tr>
<td>AR16</td>
<td>The CMS <strong>MUST</strong> have the capability to archive directives.</td>
</tr>
<tr>
<td>AR17</td>
<td>Archiving <strong>MUST</strong> align with the legislative requirements of the jurisdiction and any policy set out by organizations within the jurisdiction.</td>
</tr>
<tr>
<td></td>
<td><strong>Cryptography</strong></td>
</tr>
<tr>
<td>AR18</td>
<td>The CMS solution <strong>should</strong> have the capability to sign, encrypt as well as unencrypt and validate digitally signed consent directives.</td>
</tr>
<tr>
<td></td>
<td><strong>Conversion of Consent directives</strong></td>
</tr>
<tr>
<td>AR19</td>
<td>An individual’s consent wishes are expressed as consent directives which then need to be captured by an authorized CMS system user. The CMS system user captures an individual’s consent directives via a human readable interface that allows for the recording of consent directive-related information, for instance, the individual’s name and demographic information and the details of the directive (e.g., mask all Laboratory information). Once recorded, the CMS <strong>MUST</strong> translate or convert the human readable format of the individual’s consent directives into machine readable consent rules to be stored and enforced whenever PHI is accessed.</td>
</tr>
<tr>
<td>AR20</td>
<td>The CMS <strong>MUST</strong> support the viewing of human readable consent directives and the storage of machine interpretable consent directives for enforcement.</td>
</tr>
<tr>
<td>AR21</td>
<td>The CMS <strong>MUST</strong> have the ability to either store both the human readable consent directives and machine readable consent rules or be able to convert machine readable consent rules into human readable consent rules on demand.</td>
</tr>
</tbody>
</table>
| AR22| The CMS **MUST** ensure the integrity of an individual’s consent directives as it may be a key auditing and incident investigative tool and used when, for example:  
  - The storage of an individual’s consent directives in both machine and human readable format or provide a means for the conversion of rules sets from one format to another is required on demand.  
  - Individuals are given the opportunity to consult their consent directives on-line via a Consumer Health Solution or Personal Health Record. |
11. CMS Architectural Considerations

A successful CMS deployment needs to interconnect with many external systems in order to provide the required functionality. The interrelationship between the CMS and these external systems is discussed in this section of the document. The Architectural Impact component in each of the sections speaks to the reason(s) why a CMS requires and relies on the external system and some of the implementation considerations of the interrelationships. It is also important to keep in mind that the external systems and the dependency of the CMS on these systems holds true irrespective of the three deployment models outlined earlier in the document. These system components are based on the Canada Health Infoway iEHR Blueprint architecture. These components can be deployed as recommended in the Blueprint or alternatively, their functionality needs to be emulated within the overall CMS design and implementation. For additional information and definitions of these components refer to the Canada Health Infoway Electronic Health Record Solution Blueprint\(^{11}\).

HEALTH INFORMATION ACCESS LAYER (HIAL)

The HIAL is a gateway that acts as an abstraction layer to separate POS applications from the EHR Infostructure. It is made up of service components, service roles, information models and messaging standards required for the exchange of EHR data and the execution of interoperability profiles between EHR Services.

The HIAL is broken down into two layers of services: the Common Services and the Communication Services.

The Common Services layer is an aggregation of services that provides common and reusable functions for the applications and systems that participate in an EHR Infostructure. It is focused on integration, privacy and security, system configuration, management and monitoring functions and makes those common functions available for all services in a given EHRI.

The Communication Services layer is an aggregation of services that provides system communication capabilities. It is focused on the receiving and sending of messages and the support of valid communication modes primarily between POS applications and an EHRI, EHRI to EHRI and possibly between components within an EHRI (e.g. Location Registry to Client Registry).

Some jurisdictions may implement HIALs in a federated manner, in which case each HIAL would implement its own CMS.

\(^{11}\) [https://www.infoway-inforoute.ca/working-with-ehr/knowledgeway/knowledge-center/657](https://www.infoway-inforoute.ca/working-with-ehr/knowledgeway/knowledge-center/657)
Architectural Impact

In a centralized and to a certain degree in a federated CMS deployment model the HIAL is an important part of the architecture. The HIAL is where the enterprise level CMS storage and enforcement components exist. Some of the important architecture considerations for the HIAL should include a flexible and configurable interface to introduce capabilities for integration of a CMS. This capability becomes more important when the CMS is deployed in a hybrid model, meaning that there is a combination of deployment models such as centralized and domain based. The HIAL with a strong and highly configurable orchestration capability will allow for easy configuration of consent rules.

In the case of a federated HIAL deployment, there are several implementation challenges with regard to a federated CMS deployment model. The following are some questions to consider:

- Whether or not consent directives will be federated and synchronized across the federated HIALs
- The redundancy advantages of synchronizing directives across federated HIALs
- Whether management and enforcement of consent directives be applied within each HIAL or across multiple HIALs
- Determining how logging and auditing functions will be accessible or federated across HIALs
- The means for operationalizing investigations across the federated landscape

CLIENT REGISTRY (CR)

Client Registries exist in most jurisdictions. They were implemented as foundations to the EHR infostructures across the country. A CR generally serves as a source-of-record (also referred to as a source of truth) for the patient records in a given jurisdiction. In a client registry an individual’s electronic identity is established and resolved (which is performed by linking and unlinking of records based on predefined set of attributes). In essence, the CR is a repository of identity data/information for individuals in a given jurisdiction. Since the CR is the means for uniquely identifying clients, it is a crucial component of the EHR with which the consent management solution to integrate as it enables the association of consent directives to clients.

CR implementations in most jurisdictions have a standard message interface that provides a standard integration mechanism. This means there is a standard format to query the CR and to receive a response in a format that is consistent with the expected format within the requesting system (e.g. the EHR viewer).
Architectural Impact

The primary function of a CMS is to record and enforce an individual’s wishes for masking or consenting to the use or disclosure of their personal health information. The CR is a critical component which supports a CMS because it allows for all applications to refer to a common source to uniquely identify individuals, ensuring that the personal health information of the ‘Bob Smith’ being accessed by a health care provider is indeed the information associated with the right ‘Bob Smith’.

The CR is an ideal place as part of the overall architecture to introduce attributes associated with an individual who has provided a consent directive. The directive is not typically stored within the CR, however, a flag attached to the individual’s identity data will inform the enforcement point to query the CMS in order to confirm the details of the consent directive.

Access to the CR by the CMS is typically done via the HIAL message brokering services. The CMS would make a request for information or transaction sets to the HIAL brokering service and it would ensure communication with the CR. This communication would use pan-Canadian CR messaging standards.

In the case where the CR is not fully integrated into a HIAL, the CMS must establish connectivity directly with the CR and use pan-Canadian endorsed messages to query CR transaction sets. This implementation scenario implies that the required business logic, sequencing of transactions and maintenance of pan-Canadian Standards be incorporated within the CMS.

Another issue that should be considered with CR and CMS, is that it is common practice to merge or split individuals within the CR. This practice can significantly impact the CMS. If an individual has a consent directive, the merge and split must consider any associated consent directives. If this is not conducted accurately, a directive could be erroneously omitted or the system may associate a directive with the wrong individual. Thus as part of the design of a CMS this issue must be addressed in order to avoid the incorrect application of a directive.

PROVIDER REGISTRY (PR)

A Provider Registry (PR) is a centralized directory providing a comprehensive and unambiguous identification of all providers practicing in a jurisdiction including doctors, dentists, pharmacists, nurses, lab clinicians, diagnostic imaging technologists as well as other healthcare professionals. It is the location where a Health Care Provider’s identifying information (for example, name, address, practice license number) is securely stored and maintained at a jurisdictional level and made available to other systems and users that interact with the EHR infostructure system.
As part of a consent management solution, identifying providers in a consistent way is critical. It is possible that a consent directive may be intended to have the effect of masking information from viewing by a specific provider, or a group of providers. The PR allows for the consent management solution to identify providers and apply any associated consent directives. Just as with the CR, the PR implementations in most jurisdictions have a standard message and interface that allows for integration with the consent management solution.

In addition, there may need to be a correlation established between a person’s Provider identity (or identities) and their login identities (see the IDAM section below). It is very likely that a consent directive that references a provider explicitly will use their provider identity. In order to be able to correctly apply a consent directive based on provider identity, there must be an ability to map login identity to one or more provider identities.

**Architectural Impact**

Similar to the CR, the PR allows for a unique way to identify each provider who accesses information from or contributes information to the EHR. In jurisdictions where a consent directive can be placed restricting information from being accessed by a particular practitioner, the PR becomes a crucial component to the CMS. Regardless of the legislative framework, the identity of the provider is important when auditing access to PHI by a provider, as well as audit investigations as triggered by suspicious activity or when an individual complains about the manner in which their consent directives have been managed. Therefore it is important for jurisdictions to ensure that there are appropriate logging mechanisms to support these audits.

Access to the PR by the CMS is typically done via the HIAL message brokering services. The CMS would make a request for information or transaction sets to the HIAL brokering service and it would ensure communication with the PR. This communication would use pan-Canadian PR messaging standards.

In the case where the PR is not fully integrated into a HIAL the CMS must establish connectivity directly with the PR using pan-Canadian endorsed messages to query PR transaction sets. This implementation scenario implies that the required business logic, sequencing of transactions and maintenance of pan-Canadian Standards be integrated into the CMS.

**LOCATION REGISTRY (LR)**

The Location Registry (LR) or Service Delivery Location Registry (SDLR) is a component of an EHRI which provides a comprehensive directory of all service delivery locations that deliver patient care (hospitals, clinics, physician offices, etc.). It is a trusted source of location information, which uniquely identifies where health services are provided. It is used in the
context of transactions between POS applications and an EHRi in order to resolve the identification of the locations so that a single identifier is used across systems that maintain EHR information about an individual. Secondly, the Location Registry supports EHR interoperability and other health information systems’ needs by providing services that maintain and communicate a current and accurate source of health service location information.

The existence of an EHRi Location Registry is dependent upon a jurisdictional level strategy, plan and policies for the establishment and management of unique identifiers of service delivery locations.

**Architectural Impact**

The LR can assist with consent directives that may have dependencies on location. The LR registry can be used to determine the association of a provider to a location where the practitioner practices from more than one location. If the LR is part of the jurisdictional EHR infrastructure, and the legislative and jurisdictional polices allow for the location-based consent directives, the LR should be utilized by the CMS.

**IDENTITY AND ACCESS MANAGEMENT (IDAM)**

The purpose of an IDAM solution is to provide a common source for an identity store for multiple applications to utilize across an enterprise. A unified identity store allows an organization to have a unified process for identification, authentication and coarse-grain authorization for all applications and therefore introducing efficiencies for users as well as system administrators. This allows a user to have a single user id and password for all the applications that they are authorized to use across the enterprise (single sign on). Administrators can have a single view of all the users within the enterprise to assign privileges and manage access to different applications within the enterprise.

An IDAM implementation within a jurisdiction and the integration of the IDAM solution and the CMS eliminates the need for the CMS users to be registered, and enrolled specifically to the CMS. Rather, the CMS becomes one of the applications to which the IDAM solution assigns access for particular roles. This, allows the users of the CMS to use their existing user ID and password to access the CMS. The automated enrollment process also allows new users of the CMS access to the system quickly and efficiently.

**Architectural Impact**

The IDAM enables a jurisdiction to have unified and automated processes for registration, enrollment, and entitlement for all system users, including users of the CMS.

In the event that IDAM functionality is not available or is not integrated with the CMS, the CMS must include provision for user management within the solution. The CMS must have
the capability to manage user identities and provide appropriate access control mechanisms for all users. A CMS-specific IDAM component will require either federated or distinct user IDs or passwords for its users. Additional passwords and user ids will introduce complexity and inefficiencies for CMS end users.

The ability to manage and perform auditing functions across CMS in the domain specific and federated deployment models will be difficult as the various IDAM components are not harmonized and may not have identical security rules. Each CMS IDAM will be a siloed implementation therefore system designers should give consideration to the multiple operational and management challenges associated with these approaches, especially if a jurisdictional view of an individual’s consent directives management is a requirement.

AUDIT

The CMS needs to support auditing requirements and must log the creation, modification, override and deactivation of a directive. The auditable events must also include date and time stamps as well as the user who committed the action and their location. It is also important to coordinate these logs with logs at the POS, and clinical domains where these directives are applied. When an override event has occurred, there are additional items which need to be logged. These may include who provided consent for the override, such as a substitute decision maker, the reason for the override and possibly, the confirmation that an automatic notice was delivered to an individual.

Architectural Impact

Transactional and system logging is how audit requirements are satisfied as part of technical solutions. However it is important to take into consideration that a CMS audit event may require a correlation of logs from multiple systems and applications. When logging systems are designed and built it is important to take a holistic approach to building and creating auditable events that encompasses all application and system logs. Another important consideration is that the enforcement points may have been architected such as they are not part of the CMS system but rather the part of the HIAL or another EHR component. These logs should also be included as part of the audit of consent rules.

CO-EXISTENCE OF MULTIPLE CONSENT MODELS

As described in section 2. Overview of Current Jurisdictional Consent Solutions, each jurisdiction defines its consent model on the basis of legislation, regulation and policy. However, there can be differences in how those models are implemented within a jurisdiction. For example, a POS system, such as a Hospital Information System may be able to mask at a finer level of granularity than the jurisdictional EHR. Differences such as these can also occur between POS applications such as EMRs or HIS. For example, each may
provide varying levels of granularity applicable only to their locally stored PHI. Such variability in how consent is operationalized in a jurisdiction may have important architectural and business considerations, especially when data elements that are collected, used and disclosed locally are also stored within jurisdictional clinical domain repositories.

**Architectural Impact**

As discussed in section 8. Architectural Deployment Models and Considerations, consent models are typically codified into consent model general rule sets by the CMS. This sets the framework for consent directives within a jurisdiction applicable to jurisdictional domain repositories.

In the event that rule sets applicable to jurisdictional domains differ from those applicable to POS environments, it may be necessary for POS systems to support varying consent models within the full range of CMS capabilities.

An individual may place a consent directive which masks PHI from all health care providers in a given clinic with the exception of one provider. If this PHI is shared with a jurisdictional data repository that has a different consent model, it needs to be determined how to resolve the discrepancy. The following are some of the issues that jurisdictions may wish to consider before deploying CMS:

- In the event that consent models are operationalized differently in jurisdictional clinical domain repositories and POS environments, and disclosure directives are placed on PHI collected at the POS level, jurisdictions may wish to consider how the affected data will be shared and stored in the EHR. This may require consideration of policy, business and architectural aspects.

- In the event that consent models are operationalized differently between the POS and jurisdictional clinical domain repositories, jurisdictions may wish to consider:
  - How the POS consent model could be reflected in the jurisdictional consent model and how this would be achieved from a messaging, storage and enforcement perspective.
  - If rule sets of differing consent models should be mapped or aligned.
  - The requirement for developing policies and operational procedures to support a manual process to resolve consent model rule set discrepancies.
  - The potential operational impacts of supporting multiple consent models in a federated CMS deployment model.
12. Concluding statements

Information consent is a complex topic. It involves the legislated rights of individuals to express wishes respecting their personal health information. These instructions must be documented, communicated and respected throughout the individual’s interaction with the health system, in both paper and electronic systems.

With the generous help of experienced subject matter experts from across the country this project was able to gain a solid understanding of consent solutions in use today in several Canadian jurisdictions and to explore policy, operational, technical and system design issues that factor into any discussion of a consent management solution for the EHR environment.

It is clearly understood from this work that a jurisdiction’s policy framework; governance structure; operational processes; current and future state EHR architecture; and choices around level of granularity, masking and overrides all contribute to the design and implementation of a CMS. Further, it became evident that a number of jurisdictions have already made headway in developing consent solutions for specific EHR components.

However it also became very clear that as more and more EHR components are implemented and subsequently integrated into the iEHR, the existing domain based solutions which were built to meet the needs of specific projects may become increasingly difficult to manage and sustain. For this reason, this project sees value in consistency between consent management solutions. It was recognized that a common set of requirements and specifications which accommodate the wide range of jurisdictional needs could help achieve interoperability at the jurisdictional level and in the longer term, across jurisdictions.

This document has identified certain challenges to deploy a CMS from a business, technical and architectural perspective. However, several jurisdictions have identified consent management as a top priority to meet their respective legislation obligations. In the process of producing this report there has been remarkable convergence amongst project participants regarding the nature of the consent management challenges to be solved and the approaches to solving them.

From a high level technical and architectural perspective, based on the information reviewed to date, the technological means exist for jurisdictions to acquire, or design and develop a CMS. Several vendors of CMS solutions were consulted during the course of this project and indicated that their current products meet the majority of CMS business requirements identified in this report. That being said, a common set of flexible specifications would facilitate interoperability. Such commonality could also make Canada a more attractive customer in the global marketplace for consent solutions.

It is our hope that this report will provide the foundation, so that as jurisdictions accept this challenge they will have a sense of the scope and the steps required to move forward.
Appendix A: Acknowledgements and list of Steering Committee, Working Group and Project Advisory Group Members

This document is a reflection of consultation with stakeholders on consent management solutions. It is not an endorsement by stakeholders or Canada Health Infoway of any particular approach or approaches to consent management solutions; rather it is a thoughtful discussion of the issues related to consent management solution development and deployment. We gratefully acknowledge the dedication, insight and information provided by all those who participated in this project.

CONSENT MANAGEMENT PROJECT STEERING COMMITTEE

The Project Steering Committee was responsible for:

- Providing executive oversight and direction to the project.
- Supporting the project by making resources available.

Steering Committee Membership

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dennis Giokas</td>
<td>Chair</td>
<td>Chief Technology Officer, Infoway</td>
</tr>
<tr>
<td>Ron Parker</td>
<td>Accountable Director</td>
<td>Group Director, Emerging Technology Group, Infoway</td>
</tr>
<tr>
<td>Fraser Ratchford</td>
<td>Sponsor</td>
<td>Group Program Director, Infoway</td>
</tr>
<tr>
<td>Joan Roch</td>
<td>Privacy</td>
<td>Chief Privacy Strategist, Infoway</td>
</tr>
<tr>
<td>Stanley Ratajczak</td>
<td>Privacy and Security Lead</td>
<td>Group Director, Emerging Technology Group, Infoway</td>
</tr>
<tr>
<td>Maureen Charlebois</td>
<td>Clinical Adoption and Benefits Evaluation</td>
<td>Chief Nursing Executive and Group Director, Clinical Adoption, Infoway</td>
</tr>
<tr>
<td>Terry Moore</td>
<td>Executive Regional Director</td>
<td>Executive Regional Directory, Ontario, Infoway</td>
</tr>
</tbody>
</table>
CONSENT MANAGEMENT PROJECT WORKING GROUP

The Working Group was a key part of the stakeholder engagement component of the project. The Working Group was composed primarily of representatives from the Health Information Privacy Group and jurisdictional privacy specialists. On behalf of their respective stakeholder groups and interests, the Working Group members were responsible for:

- Providing expertise and input into the project deliverables and raised any issues or concerns
- Confirming the stakeholder engagement strategy and representation for the broader Advisory Group
- Ensuring that project deliverables reflect their stakeholder perspectives/needs
- Providing updates and communications to the groups they represented as appropriate

Working Group Membership

<table>
<thead>
<tr>
<th>Name</th>
<th>Role/Organization</th>
<th>Constituency Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ron Parker (co-chair)</td>
<td>Accountable Director</td>
<td>Infoway Emerging Technology Group</td>
</tr>
<tr>
<td>Joan Roch (co-chair)</td>
<td>Chief Privacy Strategist</td>
<td>Infoway Privacy</td>
</tr>
<tr>
<td>Stanley Ratajczak</td>
<td>Privacy and Security Lead</td>
<td>Infoway Emerging Technology Group</td>
</tr>
<tr>
<td>Agnes Wong</td>
<td>Professional Practice &amp; Clinical Informatics</td>
<td>Infoway Clinical Adoption and Change Management Representative</td>
</tr>
<tr>
<td>Later replaced by Valerie Leung</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mimi Lepage / Kevin Rodkin</td>
<td>National secondary use of health information</td>
<td>Canadian Institute for Health Information Representatives</td>
</tr>
<tr>
<td>Later replaced by Anne-Mari Phillips</td>
<td></td>
<td></td>
</tr>
<tr>
<td>David Morgan</td>
<td>Privacy Manager</td>
<td>HIP Group Representative</td>
</tr>
<tr>
<td></td>
<td>Newfoundland and Labrador Centre for Health Information</td>
<td></td>
</tr>
<tr>
<td>Michelle McDonald</td>
<td>Director of Health Privacy &amp; Access</td>
<td>HIP Group Representative</td>
</tr>
<tr>
<td>Later replaced by Maria Lasheras</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Health Privacy Office</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nova Scotia Department of Health and Wellness</td>
<td></td>
</tr>
</tbody>
</table>
## CONSENT MANAGEMENT PROJECT ADVISORY GROUP

The Project Advisory Group represented a broader stakeholder group and was responsible for:

- Providing expertise as it related to project scope
- Indicating if, based on their perspective, the project deliverables would reasonably reflect their stakeholder perspectives
- Providing updates and communications about the project to their organizations and stakeholders, as appropriate
### Advisory Group Membership

<table>
<thead>
<tr>
<th>Name</th>
<th>Role/Organization</th>
<th>Constituency Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ron Parker (co-chair)</td>
<td>Accountable Director</td>
<td>Infoway Solutions Products &amp; Services – Product Development</td>
</tr>
<tr>
<td>Joan Roch (co-chair)</td>
<td>Chief Privacy Strategist</td>
<td>Infoway Privacy</td>
</tr>
<tr>
<td>Stanley Ratajczak</td>
<td>Privacy and Security Lead</td>
<td>Infoway Solutions Products &amp; Services – Privacy &amp; Security</td>
</tr>
<tr>
<td>Maureen Charlebois</td>
<td>Chief Nursing Executive &amp; Group Director Clinical Adoption</td>
<td>Infoway Clinical Adoption and Benefits Evaluation/Change Management Representative</td>
</tr>
<tr>
<td>Mimi LePage</td>
<td>National secondary use of health information</td>
<td>Canadian Institute for Health Information Representative</td>
</tr>
<tr>
<td>Kevin Rodkin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deb McGinnis</td>
<td>Executive Director ehealth Privacy, Security and Legislation Office Ministry of Health, British Columbia</td>
<td>Health Information Privacy Group Representative</td>
</tr>
<tr>
<td>Debra Grant</td>
<td>Ontario Privacy Commissioner’s office</td>
<td>Privacy Oversight</td>
</tr>
<tr>
<td>Dan Meraw</td>
<td>Project Manager, Doorways</td>
<td>Jurisdiction Privacy Specialist Representative</td>
</tr>
<tr>
<td>Cindy Nikiforuk</td>
<td>CHIMA Representative</td>
<td>Canadian Health Information Management Association Representative</td>
</tr>
<tr>
<td>Dr. Patrick Ceresia</td>
<td>Chief Privacy Officer and Managing Director, Corporate Services</td>
<td>Canadian Medical Protective Association Representative</td>
</tr>
<tr>
<td>Chantal Léonard</td>
<td>CEO</td>
<td>Canadian Nurses Protective Society Representative</td>
</tr>
<tr>
<td>Brendan Seaton</td>
<td>Vendor Representative</td>
<td>Information Technology Association of Canada Representative</td>
</tr>
<tr>
<td>Lisa Ashley</td>
<td>Senior Nurse Advisor</td>
<td>Canadian Nurses Association</td>
</tr>
<tr>
<td>Later replaced by Margot McNamee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dr. Melody Isinger</td>
<td></td>
<td>Canadian Medical Association</td>
</tr>
</tbody>
</table>
Appendix B: Glossary

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

Jurisdictions will of course continue to use terms as defined in their own legislation and practice. However, the definitions of terms presented in this glossary reflect how the terms are used within this document for the purposes of discussing the business and architectural considerations of implementing a consent management solution. It is within this context and use, that the definitions were discussed with the Working Group members and met with their approval. Jurisdictions may decide that in other contexts and for their own purposes these terms may need to be re-examined.

Definitions have been taken in part from:

- 2011 Guidelines for the Protection of Health Information – COACH
- OIPC/AB [http://ipc.ab.ca](http://ipc.ab.ca)
- OIPC/O [http://www.ipc.on.ca](http://www.ipc.on.ca)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>‘Access’ is often defined in jurisdictional legislation to refer to an individual’s ability to view or receive copies of their own information. The term can also refer to activities under various access to information/freedom of information statutes. In other contexts, including the iEHR context, it often refers to any action that involves an authorized individual being able to view, use, or modify a record. If the term ‘access’ is used with no qualifier, it</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access control</td>
<td>A system which enables an authority to control access to areas and resources in a given computer-based information system (READ, WRITE, UPDATE, DELETE).</td>
</tr>
<tr>
<td>Authentication</td>
<td>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). In other words, when a user logs into a system, the system verifies that the individual who claims to be logging in, is the person logging in by using the information provided to it by the user (user ID, password, remote token key).</td>
</tr>
<tr>
<td>Clinical Domain Repository</td>
<td>A Domain Repository is a component of an EHR 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 recognized as part of an EHR are drugs, laboratory and diagnostic imaging.</td>
</tr>
<tr>
<td>Collection of PHI</td>
<td>The process of gathering or obtaining personal health information, either directly from an individual or indirectly (e.g. from an individual’s legally authorized individual or from a health service organization) 'Direct Collection' is information collected directly from individuals. ‘Indirect Collection’ is information gathered from other than the individual to whom the information relates. (2011 Guidelines for the Protection of Health Information – COACH) page 331.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>‘The property that information is not made available or disclosed to unauthorized individuals, entities or processes.’ ISO 7498-2</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Consent in the context of EHRs</td>
<td>An agreement, approval, or permission to collect, use and disclose personal health information. This relates to control over the INFORMATION in the record, not consent for treatment.</td>
</tr>
<tr>
<td>Consent Directive (see also Disclosure Directive)</td>
<td>The expression of an individual’s wishes with respect to the collection, use and/or disclosure of personal health information.</td>
</tr>
<tr>
<td>Consent Directive Data</td>
<td>The electronic representation (data) of an individual’s wishes with respect to the collection, use and/or disclosure of personal health information. This data is typically stored in a consent repository for use and management by a Consent Management System.</td>
</tr>
<tr>
<td>Consent Management</td>
<td>A system, process and/or set of policies for allowing individuals to determine what health information they are willing to permit their various care providers to access. It enables individuals to express privacy preferences. Consent management supports the dynamic creation, management and enforcement of individual, organizational and jurisdictional privacy directives.</td>
</tr>
<tr>
<td>Consent Management Solution</td>
<td>An information system or systems that provides for the capture, storage, update, deactivation and enforcement of consent directives.</td>
</tr>
<tr>
<td>Consumer health solution</td>
<td>A consumer health application is an electronic solution that enables the consumer to collect, retrieve, manage, use and share personal information and other health-related data. A consumer health application could include applications commonly known as personal health records and patient portals. If connected to a consumer health platform, the consumer health application provides access to the services provided by the platform and the personal information stored in the platform.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Custodian /Trustee          | An individual or organization that collects, uses, or discloses personal health information for the purposes of care and treatment, planning and management of the health system or health research. The individual jurisdiction’s legislation may include 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 organizations identified in regulations  
  - Affiliates/agents e.g. employees, volunteers  
  - Cancer Board  
  - Mental Health Board  
  - Ambulance Operators  
  - Persons who maintain and administer an EHR system |
<p>| Data Warehouse              | A relational database containing specifically structured data for query and analysis to support decision making in an organization. Data from one or more production databases or systems are copied to the data warehouse at regularly scheduled intervals so that queries can be performed without disturbing the performance or the stability of the production systems. |
| De-identified information   | Personal health information that has been modified so that the identity of an individual cannot be determined by a reasonably foreseeable method (2011 Guidelines for the Protection of Health Information – COACH) |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosure Directive</td>
<td>A tool that allows individuals to exert their right to choose who can have access to information within the electronic health record. (adapted from Ministry of Health, British Columbia <a href="http://www.health.gov.bc.ca/ehealth/dd.html">http://www.health.gov.bc.ca/ehealth/dd.html</a>)</td>
</tr>
<tr>
<td>Disclosure of Personal Health Information</td>
<td>To make the information available or to release it to another health information custodian, trustee or to another person, but does not include to use the information. Protection of Personal Health Information and Use of Personal Health Information. Ontario Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, s. 2</td>
</tr>
<tr>
<td>eCID</td>
<td>The ID that uniquely identifies a client in the EHRi where a transaction is being conducted. It is used only internally within the EHRi, and is never disclosed to POS applications.</td>
</tr>
<tr>
<td>Electronic health record (EHR)</td>
<td>An electronic record that provides each individual in Canada with a secure and private lifetime record of his or her key health history and care within the health system. The record is available electronically to authorized healthcare providers and the individual anywhere, anytime in support of high quality care. In an Electronic Health Record Infostucture (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.</td>
</tr>
<tr>
<td>Enforcement points</td>
<td>Enforcement points enforce an individual’s consent directive rules. Enforcement points are a logical entity or place on a server that enforces policies or rules with regard to consent directives when a request from a user or IT system wishes to access personal health information.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Enterprise solutions are implemented at other than the local level (e.g. regional or provincial/territorial).</td>
</tr>
<tr>
<td>Express consent</td>
<td>The most explicit method of obtaining consent. It may be provided orally or in writing (including electronically), and occurs when an individual specifically agrees to collection, use or disclosure of personal information for specified purposes. (Personal Information Protection Act (PIPA) Advisory #1)</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Implementing Consent Requirements for Customers, OIPC/AB</td>
<td><a href="http://www.oipc.ab.ca/Content_Files/Files/Publications/0001_Consent_20050420_Apr_2007.pdf">http://www.oipc.ab.ca/Content_Files/Files/Publications/0001_Consent_20050420_Apr_2007.pdf</a>)</td>
</tr>
<tr>
<td>Granularity</td>
<td>Consent directive granularity refers to the level of control over the type and level of information with which a consent directive is expressed, captured or enforced. For example, a consent directive at the level of an individual drug or laboratory test is more granular than at the level of a drug or laboratory repository. A consent directive at the level of a health care provider is more granular than at the level of a facility.</td>
</tr>
</tbody>
</table>
| 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. Exists where it is reasonable in the circumstances and as a result of the individual’s behaviour to believe that the individual knows:  
1. The purposes of the collection, use, or disclosure and how their personal health information will be used or disclosed; and  
2. That the individual may provide or withhold consent.  
Individuals can be informed of their rights and the privacy policies through posting of notices, brochures and pamphlets and/or discussions in the normal course of exchange that takes place between the individual and the health care provider.  
Once the individual is informed, in accordance with 1) and 2) above, consent can be implied if the individual continues to seek treatment or to provide information or behaves in a way which indicates by his/her observable behaviour that the individual is consenting to this collection, use and disclosure. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Individual           | The word ‘individual’ is used throughout this document to describe any person who is the subject of interest for a consent directive. This includes those who place directives, those who are substitute decision makers, and anyone who may receive health care.  

However, the term, ‘client’ will be used, as appropriate, in the appropriate section, for example when referring to the Client Registry |
| Key word             | A word known only to the individual about whom information relates and is provided in order to release information to a provider who is authorized by an individual to access their personal health information. |
| 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 (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.                                                                                                   |
| Override             | When a consent directive exists and a health care provider wishes to access masked data, there may be certain circumstances under which that data can be accessed.  

When a health care provider accesses data to which a directive is subject – it said to be ‘overridden’. |
| Personal health information | 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:  

- Information about the registration of the individual for the provision of health services,  
- Information about payments or eligibility for health care in respect to the individual,  
- A number, symbol or particular assigned to an individual to uniquely identify the individual for healthcare purposes,  
- Any information about the individual that is |

February 29, 2012  
Business and Architecture Considerations for Interoperable Consent Solutions: A discussion document
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>collected in the course of the provision of health services to the individual, and</td>
<td>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.</td>
</tr>
<tr>
<td>Information derived from the testing or examination of a body part or bodily substance.</td>
<td></td>
</tr>
<tr>
<td>Point of service (POS) system</td>
<td>The clinical application systems (e.g. hospital-based Admission Discharge, Transfer, Clinical Information System, Laboratory Information System, etc.) that operate at the many locations where healthcare services are delivered. 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 EHR 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.</td>
</tr>
<tr>
<td>Privacy</td>
<td>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. A.F. Westin, Privacy and Freedom, 1970 p. 7.</td>
</tr>
<tr>
<td>Proxy</td>
<td>An individual acting for another.</td>
</tr>
<tr>
<td>Provider</td>
<td>A health professional who provides care.</td>
</tr>
</tbody>
</table>
| Pseudonymization             | A particular type of anonymization that both removes the association with an individual and adds an association between a particular set of characteristics relating to that individual and one or more pseudonyms. (2011 Guidelines for the Protection of Health Information – COACH)
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record</td>
<td>A record of information in any form or in any medium, and includes information that is written, photographed, recorded, digitized or stored in any manner, but does not include computer programs or other mechanisms that produce records.</td>
</tr>
<tr>
<td>Research</td>
<td>A systematic investigation designed to develop or establish principles, facts or general knowledge, or any combination of them, and includes the development, testing and evaluation of research.</td>
</tr>
<tr>
<td>Substitute decision maker</td>
<td>In relation to an individual, means, unless the context requires otherwise, a person who is authorized under legislation to consent on behalf of the individual to the collection, use or disclosure of personal health information about the individual.</td>
</tr>
<tr>
<td>Use of Personal Health Information</td>
<td>The treatment or handling of information within an organization. Disclosure does not constitute ‘use’. (2011 Guidelines for the Protection of Health Information – COACH)</td>
</tr>
</tbody>
</table>
Appendix C: The Process Lifecycle of a Consent Directive

Consent directives have a life cycle from before the time they are created in a consent management system to the time they are no longer relevant and are removed from the active system. The cycle begins with individuals being made aware of the option to apply a consent directive. Individuals then make their wishes known to a party who can process them and enter them into a consent management system. The following sections provide an overview of the lifecycle.

CAPTURE

‘Capturing’ a consent directive includes receiving notice that an individual wishes to apply a consent directive and, if not already documented by the individual, documenting that notice and the particulars of the request. It also includes communicating this information to the system administrator who will physically enter the information into the information system.

The jurisdictions contributing to this paper have advised that, to date, this involves the individual obtaining a form, completing it and submitting it. The process for completion and submission of the form varies by jurisdiction and may also vary by domain within a jurisdiction.

In most, but not all, cases the potential implications associated with applying a consent directive are explained to an individual. This explanation may take the form of a document, like Frequently Asked Question (FAQ) sheets, or information provided by trained clinicians using scripts to ensure that individuals understand the implications of applying a consent or disclosure directive.

While paper processes are out of scope for this paper, the information collected on forms inform the data entered into the CMS, therefore it merits some discussion here. Forms and the associated information required for completion may be specific to the system, jurisdiction, and even to the domain within the jurisdiction. In general the information collected on the forms includes demographic information (e.g. first, middle, last name, address, date of birth, phone numbers, health card number) and preferred language. In some cases there are sections on the form which include security questions and answers, and for providing information specific to a designated substitute decision maker (e.g. someone who has been given authority to request a consent directive for another individual.)
Generally consent requests can be made by:

- An individual on their own behalf if they have capacity
- An authorized individual on behalf of another person (for example a substitute decision maker, proxy, or other legally authorized individual can place a consent directive on behalf of an individual who is too young or otherwise incapable and may not be able to consent on their own behalf)

Before the information documented on a consent directive form can be entered into the information system (created), information presented on forms is checked or validated. Information provided is generally cross-referenced with information from the Client Registry, Provider Registry, and/or Location Registry, where applicable, or other reference source or ‘source of truth’. For example, in the case of the Pharmaceutical Information Program in Saskatchewan, the information is checked against the Ministry’s health registration system. This ensures that the information being submitted is being provided by an authorized individual.

In some cases, once the information on the form is validated, a system administrator responsible for managing the process enters or ‘creates’ the directive in the system through a web interface. In another situation, the requesting individual is provided with a code that must be communicated to the administrative body to ‘activate’ consent. Once the call is made the consent directive is created in the system.

The forms used in this part of the process may be available to the individual in hard copy in their health care providers’ office; or downloadable from a website; or by placing a call to request a form from a consent directive administrator. Where manual forms are used, the signed forms are stored according to legislative requirements or organization policy. For example, in some instances the signed forms are scanned and stored electronically in a central repository, often within a ministry of health agency.

CREATE

Generally, designated individuals are permitted access to the consent management systems to ‘create’ the directive. This includes the process of making the required changes in the system to apply an individual’s consent directive. The actual procedure by which the consent directive is created is dependent on the jurisdiction and, on the functionality of the information system. Domains with consent management functionality, consent management systems and some jurisdictions which use the Health Information Access Layer (HIAL) to create consent directives, provide a viewer through which the administrator can create and
manage a consent directive, including adding users to system and configuring consent directives.

In some implementations, consent directives are documented on a manual form, validated and then entered into a temporary electronic format (e.g. an excel spreadsheet) to be sent to the administrator who will be creating the consent directive in the appropriate system. The electronic information is encrypted before transmission to the administrator responsible for creating the consent directive.

Once created, the system logs the date and time that it was created and then the consent directive must be stored. The location for storing consent directives is as varied as the systems in use. Consent directives may be stored in the domain solution or in a solution specifically designed for consent management. Many use the HIAL in some manner. This could include storing the directives directly in a centralized HIAL, in a separate repository within the centralized HIAL, in the Client Registry which may in reside in the centralized HIAL or within a regional HIAL that communicates with the provincial HIAL.

READ

When a user logs into a system and wishes to access personal health information of an individual, the system ‘reads’ or checks whether a consent directive has been created prior to permitting access to the information. This ‘read’ includes referring to any rules (policies) that may have been configured in the consent management system that may direct how the system permits access. One policy may be, ‘if a consent directive has been created for an individual, only permit access to personal health information according to the consent directive constraints which have been created’; or ‘on ‘reading’ that there is a consent directive, the rule may require the display of a ‘pop up window’ to alert the user that the information is subject to a consent directive or ‘when a pop up window’ is displayed, present an option to obtain the consent of the individual in that moment to ‘override’ the consent rule.

When a policy is read by a system and the system acts according to the policy, the system is said to be ‘enforcing’ the policy. Generally, policy enforcement in the ‘read’ stage of the lifecycle has been architected as a HIAL service. One of the functions of this enforcement service may be reconciling multiple consent directives when more than one has been created for a single individual. For example, a jurisdiction may have two provincial repositories, each with its own consent management functionality. When a consent management solution references these two repositories the policies in both systems are checked before displaying personal health information about an individual, and the appropriate action is taken to alert the user to what they can and cannot access. For example, Dr. X may be permitted to see an individual’s laboratory results in the laboratory domain but may be denied access to the drug repository.
UPDATE

From time to time, individuals may wish to adjust their consent directive. Processes for updating a consent directive are generally the same as for capturing and creating one. The individual expresses in writing their wish for a change, the information on the form is validated and the administrator then accesses the system and ‘updates’ the consent directive information in the system. These changes in the system are generally logged to include who directed the change, the administrator who made the change as well as the date and time of the change.

DEACTIVATE

- The term ‘de-activate’ refers to the end of the consent directive lifespan. At this stage, the consent directive is no longer in force. The lifespan of a consent directive may be set by the domain, system or jurisdiction rules. In most cases a consent directive is deactivated only when an individual requests that the consent directive be removed, or the directive reaches an ‘end date’. When a directive is being permanently deactivated, it is not completely removed or deleted from the system, rather it is logged to ensure an accurate consent history can be viewed for an individual.

The following lists the types of ‘deactivation’ or end dates which may be in place for a given directive:

- No set deactivation date
- Set deactivation date (a deactivation date is set on creating the consent directive)
- Deactivation upon request (an individual changes their mind and asks for a deactivation)
- Set deactivation period (for example, a consent directive may be in effect for a period of 3 years from time of creation and then automatically be deactivated)
- Deactivate when an incapable individual, whose consent directive was put in place by a substitute decision maker or alternative proxy, subsequently meets criteria for making an independent decision around consent (for example, in Ontario, when a child reaches age 16 and is otherwise capable).

Processes for deactivation upon request are generally the same as for capturing and creating one. Processes for accommodating other types of deactivation are dependent on the legislative framework in the jurisdiction and/or organizational policies that have been set out to accommodate these circumstances.
OVERRIDES

While not part of the life cycle per se, overrides are an important part of consent management. Overrides, sometimes also referred to as ‘break the glass’ provisions, are instructions or rules entered into the consent management system that supersede an individual’s consent directive. They allow authorized health care providers to view a specific individual’s health care information in an emergency situation, for example. An individual or substitute decision maker may also provide consent for the override when the circumstance presents.

An override is generally temporary in nature. The duration of an override is usually pre-set as a ‘policy’ or rule within the system which is read by the system at the time that an override is requested by a user. For example, in an emergency situation the override may be in effect for the duration of time that the clinician has logged into the system to review it and then the consent directive takes effect again on log-out of the system, or the temporary override may be in place for a set duration – anywhere from a number of minutes to hours depending on the jurisdiction or on the circumstance in which the override has been applied.

In addition to the provision for overrides in an emergency situation, where the provider may initiate an override without the consent of the individual, overrides may also occur with the verbal consent of the individual to whom the information relates or on the consent of a substitute decision-maker.

Systems with consent management provisions will log the user entering the override, the date and time that the override was created and may also include the reason for the override and who, if anyone, provided the consent for it.
Appendix D: International References

The following references were consulted in the development of this document. They have been appended here should readers wish to review this material independently.

AUSTRALIA

Shaping the future of healthcare: Privacy Blueprint for the Individual Electronic Health Record, NEHTA, 2008


DENMARK

Accomplishing EHR/HIE (eHealth): Lessons from Europe, Dr. Harald Deutsch, Fran Turisco, [www.CSC.com](http://www.CSC.com), July 2009

- [http://assets1.csc.com/health_services/downloads/CSC_Accomplishing_EHR_HIE_(eHealth)_Lessons_from_Europe.pdf](http://assets1.csc.com/health_services/downloads/CSC_Accomplishing_EHR_HIE_(eHealth)_Lessons_from_Europe.pdf)

Widespread Adoption of Information Technology in Primary Care Physician Offices in Denmark: A Case Study, Denis Protti, Ib Johansen, March 2010


ENGLAND

NHS Connecting for Health Website Summary Care Records (SCR)

- [http://www.connectingforhealth.nhs.uk/systemsandservices/scr](http://www.connectingforhealth.nhs.uk/systemsandservices/scr)
EUROPE

Accomplishing EHR/HIE (eHealth): Lessons from Europe, Dr. Harald Deutsch, Fran Turisco, www.CSC.com, July 2009


GERMANY

Establishing a Personal Electronic Health Record in the Rhine-Neckar Region, Oliver Heinze, Bjoern Bergh, Informatica Medica Slovenica 2009


NETHERLANDS

Accomplishing EHR/HIE (eHealth): Lessons from Europe, Dr. Harald Deutsch, Fran Turisco, www.CSC.com, July 2009


SWEDEN


UNITED STATES

Consumer Consent for Health Information Exchange: An Exploration of Options for Arizona’s HIEs, Kristen Rosati, Arizona Health-e Connection, in conjunction with Coppersmith Gordon Schermer & Brockelman P.L.C.


Developing a Universal Consent Form: Lessons Learned from Florida Medicaid, AHRQ Publication No. 10-0104-EF, September 2010


Individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment, National Committee on Vital and Health Statistics, Simon P. Cohn, February 2008

- [http://www.ncvhs.hhs.gov/080220lt.pdf](http://www.ncvhs.hhs.gov/080220lt.pdf)


U.S. Department of Health & Human Services, The Office of the National Coordinator for Health Information Technology, Privacy and Security in Health Information Exchange

Appendix E: Related Initiatives

PRIVACY AND EHR INFORMATION FLOWS IN CANADA: COMMON UNDERSTANDINGS OF THE PAN CANADIAN HEALTH INFORMATION PRIVACY (HIP) GROUP

The Canada Health Infoway-sponsored Pan-Canadian Health Information Privacy (HIP) Group developed and published a ‘common understandings’ paper in 2010, describing principles for appropriate and privacy-protective trans-jurisdictional disclosures of EHR information for care and treatment and secondary uses. The HIP Group is made up of provincial, territorial and national representatives from health/e-health ministries, established to work on privacy issues related to the inter-jurisdictional movement of EHR information in Canada.

The HIP Group’s ‘common understandings’ reflect principles that the Group generally agrees should be adopted consistently across jurisdictions. The paper establishes foundational principles, along with principles that address trans-jurisdictional disclosures of EHR information, patient control of their personal health information, disclosure for secondary use, and governance and accountability. The common understandings can be valuable in promoting consistency and informing jurisdiction work on health information privacy legislation, associated health information or e-health policies, information sharing agreements and business/technical requirements for EHR systems. They do not, however bind jurisdictions, and the paper emphasizes jurisdictional responsibility for decisions in these areas.

IEHR TECHNICAL PROJECT I (TECH I)

In 2007, Infoway funded an iEHR Technical Project (TECH I). One aspect dealt with questions relating to Informational Consent Directives Management. A set of pan-Canadian use cases and requirements for a ‘Consent Directives Management Service’ as described in the Infoway Privacy and Security Conceptual Architecture (2005) was developed. Additionally, a glossary of terms, jurisdictional overview, set of assumptions, a requirements framework, and a recommended set of next steps were produced.

The IT Privacy and Security Services Standards Collaborative Working Group (SCWG 8) then reviewed the documents to determine the level of acceptance from all constituencies and to set the stage for evaluating existing standards applicable to Information Consent that could be adopted or adapted to meet stated requirements.

The SCWG completed its review and update of all of the deliverables from the iEHR Tech Project, with the exception of the CDMS Requirements Framework document. It also produced an initial draft of an evaluation instrument to be used to compare and contrast various potential standards against the set of accepted requirements.
IEHR TECHNICAL PROJECT II (TECH II)

In August of 2008, Infoway funded the iEHR Technical Project II, with an Informational Consent portion mandated to provide direction and guidance to jurisdictional iEHR implementers and other stakeholders in achieving pan-Canadian interoperability of the HIAL Consent Directive Management Services (CDMS). A key objective was to solicit and gain consensus from as many Jurisdictional stakeholders as possible. The following Tech II project artifacts have influenced this report;

- Consent Management Solution (CMS) Functional Requirements
- Consent Standards Assessment and Recommendations
- Consent Directives Management Framework

PRIVACY AND SECURITY CONCEPTUAL ARCHITECTURE

This document identifies the privacy and security architectural requirements for an interoperable electronic health record (iEHR) to protect the privacy of individuals and maintain the confidentiality, integrity and availability of their personal health information. It provides the framework and conceptual architecture components for a fully interoperable consent management solution which can be leveraged by systems that are part of the iEHR. It features a centralized CMS deployment model which is the basis for one of the CMS deployment models discussed in this document.

ELECTRONIC HEALTH RECORD SOLUTION (EHRS) BLUEPRINT

The Electronic Health Record Solution Blueprint\(^\text{12}\) is a technology framework that enables the appropriate sharing of clinically relevant health information for an individual between health services providers across care settings and disciplines in Canada.

The Blueprint provides a vision and direction for how information technology can be employed to enable the many different information systems used in health care to interoperate - allowing an authorized health service provider to access information captured by other healthcare providers for the same individual.

The EHRS Blueprint was originally developed as a high level vision for how information could be securely and appropriately shared across Canada using information and communications technologies.

\(^{12}\) Electronic Health Record Solution Blueprint, 2015, Canada Health Infoway
Appendix F: Inventory of existing standards

MESSAGE BASED STANDARDS

Message based deployment of any solution including CMS, involves a set of messages that contains a message header and body. Both the source and destination of the message have a common understanding of the structure and definition of the header and body. There may also be a predefined terminology that is part of the message body. The message delivery and packaging may be based on technical standard such as XML or SOAP or it could potentially be a home-grown solution, although this is not recommended. The message body structure and terminology could also be based on a standard such as Health Level Seven International (HL7). Since some of these standards are commonly used and international standards, typically these standards will have a predefined set of messages that allow for interoperability outside of one organization without having to include software development toolkits or message building instructions.

CLINICAL DOCUMENT ARCHITECTURE (CDA)

Another possible deployment standard for a CMS is to exchange consent information between systems and organizations using Clinical Document Architecture or CDA. CDA is a standardized mark-up language used in the capture, storage and communication of clinical documents such as discharge summaries and progress notes. The documents may include text, images or other kinds of multi-media. CDA uses the HL7 Reference Information Model (RIM) and it is encoded using XML. CDA also has one single standard for the EHR instead of multiple messages. CDA can be deployed with a structured header and body, or can have a structured header with an unstructured body, therefore introducing flexibility in the deployment scenarios.

EXTENDIBLE ACCESS CONTROL MARKUP LANGUAGE (XACML)

XACML is an XML-based access control language in which access control rules are included with an XML document as an assertion. The access control rules can be as stringent as naming an individual, or can be more generic and limited to a role. With XACML, the destination must trust that the source is providing the accurate assertion and therefore the destination must have a trust relationship with the source. A scan of commercially available CMS offerings revealed that several vendors offer XACML as part of their solution.