Canada Health Infoway

Inforoute Santé du Canada

Pan-Canadian iEHR Technical Project

Consent Directive Management Services (CDMS) Guidelines

Use Case Model
Version 1.5

August 7, 2007

Document Information

Author:	Marion Lyver, MD
Contributors:	iEHR Technical Team and Stakeholders
Creation Date:	March 6, 2007
Last Updated:	August 12, 2007~~August 7, 2007~~
Language:	English
Document Number:	IG5SA0902-0002 (Consent Directive Management Services)
Document Status	In Progress
Infoway Project	IG5SA0902 (iEHR - Technical Project)
Distribution	iEHR-pan-Canadian Stakeholders Groups / Reviewers
Contact Information	Toronto Office: 150 King Street West, Suite 1308 Toronto, Ontario M5H 1J9 Tel.: (416) 595-3171 Toll free: 1-888-733-6462 Fax: (416) 593-5911 http://www.*Infoway*-inforoute.ca

Version Tracking

Document name: IG5SA0902-0002-iEHR-Tech-Project-Consent_CDMS Use Case Model vx.x_yyyymmdd_initials

Version	Author(s)	Change Description	Date
1.0	Marion Lyver, MD Lead, Consent Directive Management Track iEHR Technical Project	First Draft	2007-March-06
1.1	Marion Lyver, MD	Revised based on input from iEHR Technical Project team	2007-March-22
1.2	Marion Lyver, MD	Revised based on further research	2007-March-26
1.3	Marion Lyver, MD	Revised based on feedback from HIPAAT and review of other use cases provided by the jurisdictions as requested by the track lead	2007-April-23
1.4	Marion Lyver, MD	Revised based on discussions and review at the iEHR Technical Project Stakeholder Workshop held April 24-26, 2007, Toronto.	2007-May-25

Version	Author(s)	Change Description	Date
1.5	Marion Lyver, MD	Revised based on feedback from consent workshop participants, including feedback on other consent documents	2007-August-7

Copyright Notice

TABLE OF CONTENTS

I INTRODUCTION

1.1 Purpose

The purpose of this document is to provide a Use Case Model for Consent Directive Management and the Consent Directive Management Services (CDMS) component of the EHRi Privacy & Security HIAL Common Services.

The following items will be presented:

Use Case Actors
Use Cases.

Use cases addressed in detail include:

- Create, change, and cancel a Consent Directive to Disclose PHI
- Override a Consent Directive to Disclose (with consent; without consent - emergency override)
- Mask specific PHI
- Create a Keyword
- Respond to a request for a person's Consent Directive History
- Create, Change, Reinstate Consent to Participate
- Administrative Use Cases (Appendix 1)

Other use cases listed below have been included at a lower level of detail or as discussion items for future consideration:

- CDMS Internal Use Cases
- Extra-Jurisdictional Access Request
- Public Health Access Request
- Record Author Denied Access
- Circle of Care Member Denied Access
- Attempted Access based on possession of a paper copy of a person's record
- Consent Directive or User's Privileges Change during User Session
- Person Creates/Modifies/Cancels their own Consent Directive
- Other Masking Use Cases.

1.2 Glossary, Acronyms, References

See specific iEHR Technical Project Consent documentation related to these topics.

II USE CASE ACTORS

The following actors represent the individual users or systems that will utilize or interact with the CDMS components of the HIAL Common Services and its related systems. In many instances, these actors reside outside of the EHRi (i.e. their actions cannot be strictly controlled by the EHRi) and will interact directly e.g. web browser application (WBA) or indirectly [through point of service (PoS) systems] with the EHRi. Whenever possible, the use cases will group actors into common roles based on the common functionality requirements of the CDMS and its related systems.

This analysis considers the following actors i.e. the users that will interact with the EHRi and/or the CDMS and its related systems. (For a complete set of comprehensive definitions, see the CDMS Glossary 20070806 v1.3.)

1. Client Registry
A trusted source of information on individuals that is available to authorized users. It consists of a system or a combination of systems where a person's essential identifying and demographic information (e.g. Name, Date of Birth, Gender, Personal Health Number) is securely stored and maintained.

2. Consent Directive Management Services (CDMS)
The principal system under analysis in the use cases that will provide the Consent Directive Management software services. The CDMS is a HIAL P&S Common service that translates privacy requirements arising from sources such as legislation, policies, and individuals' specific Consent Directives, and applies these requirements in an EHRi environment.

The CDMS will itself be an actor upon other systems that lie outside the boundary of the CDMS.

3. EHR Consent Registrar (may also be known as a Consent Manager or Consent Administrator)
Individuals or organizations responsible for capturing, recording and reporting Consent Directives respectively. They may also have responsibilities for distribution and collection of related Consent Directive materials e.g. public Notices; Consent Directive forms; information/FAQs, etc. Individuals would be affiliated with designated and authorized EHR Program Management entities e.g. provincial/territorial Ministry of Health health card offices or other authorized agencies e.g. hospitals or other healthcare facilities.

4. Healthcare Facility
A facility where healthcare services are delivered.

5. Healthcare Organization
The organization responsible for governance and operation of a healthcare facility.

6. Healthcare Provider
Any supplier of a healthcare service, whether an individual or an organization, whether publicly or privately funded. This includes healthcare professionals who are regulated by a professional standards regulatory body and legislation, or regulated by an equivalent practice-standards setting body and legislation e.g. paramedics under the Ambulance Act.

Special privacy and security implications may accrue to some types of healthcare providers e.g. emergency care providers may have emergency override provisions that allow them to retrieve or update patient/person records and/or information within records that would not normally be accessible to other healthcare providers.

7. HELP Desk
A support service established by an EHR Program Management Office (PMO) or third party agent contracted by the PMO to assist people with understanding their Consent Directive options and completing their directives and to answer related questions.

8. Information Security Officer
A person responsible for information security e.g. security of paper files, networks and computers within the organization that process and store information, and for promulgating, enforcing and administering relevant security policies within the organization.

9. Person/Patient
Patient is an individual scheduled to receive, receiving, or who has received a health service**.**

In the context of the CDMS system, a patient or other individual who is granting or denying consent, or who has granted or denied consent for access to and disclosure of their personal health information (PHI) from the EHRi to authorized users who will be using the CDMS services to view, and where applicable, manage the person's Consent Directives. In Quebec, it is also someone who is granting or denying or who has granted or denied Consent to Participate i.e. has permitted or not permitted the collection and storage of their PHI in the EHRi.

10. Point of Service (PoS) system
The clinical application systems (e.g. EMR, EPR, ADT, LIS, etc.) that operate at healthcare facilities. These systems may access the EHRi to view a person's PHI, and if authorized, manage their Consent Directives.

11. Privacy Officer/Chief Privacy Officer
An individual who oversees all activities related to the development, implementation, maintenance of and adherence to an organization's policies and procedures covering the privacy, confidentiality and often the security of PHI.

12. Provider Registrar
An officer or process that registers or facilitates the registration of new EHRi users into the Provider Registry and captures essential credentials, role, facility/organization and identifying demographic information, as well as capturing or creating system access information such as user identification and password.

13. Provider Registry
A trusted source of information on healthcare providers that is available to authorized users. It consists of a system or a combination of systems where a healthcare provider's information profile (i.e. name, practice address, professional certification, healthcare organization affiliation, role, etc…) is securely stored, maintained and made available to other systems and users. Optimally, a single jurisdictional registry would be implemented for both healthcare provider and non-healthcare provider users.

14. Registration Clerk
An officer or process that registers or facilitates the registration of patients/persons into a PoS system. It includes hospital ADT clerks and medical receptionists.

III USE CASES

There is a natural and necessary tension between the protection of personal health information (PHI) and the desire to enable effective access to that information for healthcare providers. The challenge is to minimize workflow impact, while providing persons/patients (and their healthcare providers) with the confidence that their Consent Directives regarding access to their PHI will be respected.

Informational consent involves what will be collected, with whom it will be shared and how long it will be retained, as well as tracking access and interpreting Consent Directives as they move through the interactive elements that constitute healthcare service [Source: CHI EHR PSA Use Cases, Nov. 2004]

The use cases below describe the key interactions between various actors and the CDMS in business terms.

See ***Appendix 2*** *for the* ***CDMS Use Case Model for the "core" use cases described in this section.***

3.1 Supporting Use Cases

1. The user logs on to the EHRi through their PoS system or through an EHRi Clinical Portal.

2. The EHRi user is authenticated through jurisdictionally approved mechanisms e.g. user ID and password, digital signature, biometric, etc.

3. The EHRi user is authorized to access a person's PHI with privileges based on identity, role, relationship to the person e.g. patient, facility, workgroup and/or category of permissions assigned e.g. view only; view and manage consent.

4. The identity and demographic information of the person (to whom a Consent Directive applies) is confirmed in the Client Registry. If CR validation fails, e.g. an error condition is returned, the user manually invokes a CR Update use case or the EHRi system automatically updates the CR information.

3.1.1 Administrative Use Cases

These use cases address an important part of the overall Consent Directive Management processes, and there may be a need for standard messages for certain components beyond those covered in the use cases that follow e.g. electronic exchange of forms, electronic retrieval of forms, etc.

Workshop participants regarded administrative uses cases as primarily jurisdiction-specific and assigned them a lower priority than the use cases that have been included in this model.

For interested stakeholders, additional information and discussion related to these use cases has been included in ***Appendix 1 – Administrative Use Cases***.

Specific Use Cases

3.1.2 Create Consent Directive to Disclose PHI

Business Description: This use case is initiated when a person visits their healthcare provider's office or other designated EHR Consent Registrar e.g. hospital, Ministry health card registration office, to complete their Consent Directive to Disclose (CDD) their PHI from the regional EHRi repositories. The use case ends when a valid CDD has been saved in the EHRi.

Pre-Conditions:

1. The person has indicated they do not have existing CDDs for disclosure of their PHI from the EHRi.

2. The person has reviewed the relevant consent information on the jurisdictional website, including Consent Directive forms.

3. The user has accessed and reviewed online public information with the person or their SDM regarding Consent Directives, including the implications of completing such directives and has addressed questions the person had regarding the information.

4. The person or their SDM has acknowledged their understanding of the information e.g. an acknowledgement tick box on the form, which is then captured when creating the electronic Consent Directive.

5. The person or their SDM has provided appropriate proof of identity documents in accordance with jurisdictional requirements e.g. Driver's License, Birth Certificate.

Assumptions:

1. The primary form of Consent Directive information capture will be electronic.

2. Where required, the relevant jurisdictionally approved Consent Directive will be completed if the person wishes to grant or deny consent to disclose their PI/PHI from the EHRi.

3. The completed Consent Directive will be accompanied by written detailed consent information and explanations as required from healthcare providers or HELP desk staff to ensure that the consent is knowledgeable or informed as per jurisdictional legal requirements.

4. Information about a substitute decision maker (SDM) who is completing the Consent Directive on the person's behalf will be made available to the CDMS either from another system or will be entered into and accessible from the CDMS Consent Repository. Location of SDM information *may* be determined at the jurisdictional level or at the pan-Canadian level (TBD).

   [*Note: Where SDM identification and contact information should be stored e.g. in the Consent Repository along with Consent Directive information or in the CR was a topic of discussion at the April 2007 iEHR Technical Project workshop. This has been included in the CDMS Requirements Framework Section 3.0 - Issues List.]*

5. Online information regarding Consent Directives, implications of granting or denying consent, completion of forms and forms for downloading will be provided as part of the CDMS and/or through a separate application for general (public) access.

6. Consent Directive forms will mirror the consent model in place in the jurisdiction e.g.

   - express consent (full opt in) (express consent model)
   - express consent with exclusions (partial opt in) (express consent model)

- denial (refusal) (full opt out) (implied consent models; also applicable to deemed and no consent models where the jurisdiction chooses to treat PHI in the EHRi as if an implied consent model existed)
- denial (refusal) with inclusions (partial opt out). (implied consent models; deemed and no consent models as noted in previous bullet).

7. Paper copies of Consent Directives will be stored for the required period as directed by jurisdictional legislation e.g. on microfiche; electronically as scanned documents.

8. The microfiche number, electronic ID or the ID of the physical location of stored copies may be stored in the Consent Repository.

9. At the time that a new Consent Directive is created and stored, the CDMS will ascertain if the new directive conflicts with existing directives and report the problem at that time or take steps to resolve it.

Basic Flow:

1. The user accesses the CDMS application, selects the person if not already selected, and then selects the Manage Consent option.

2. The CDMS displays the Manage Consent screen to the user. The screen may be populated with the person's name and/or some demographic data.

3. The Manage Consent screen displays the Consent value e.g. Y, N or Blank. If no choice has been set, the value is set to Blank. If the value is set to Y, the user may submit a request to view the person's Consent Directive History and/or currently active Consent Directive(s).

4. The user asks the person to select/confirm the consent conditions/constraints they wish to apply to their Consent Directives. e.g. from pick lists. For example:

    - What data can (or cannot) be disclosed e.g. all PHI; for PHI for a particular domain; other levels of granularity as implemented by the jurisdiction
    - Which users can (or cannot) access the data to be disclosed (assumes additional limitations based on users' roles) e.g. all users except; no users except; only the users specified
    - Which users can (or cannot) access data that is not to be disclosed (masked data) e.g. all users except; no users except; only the users specified.

5. The user Records the Consent by entering the relevant Consent Directive data e.g. from pick lists, that is provided by the person (face-to-face questioning) or from a Consent Directive form that the person has pre-completed (to be validated with the person). Types of data expected to be captured includes:

    a. Person or SDM proof of identification documentation (added to demographic section of the directive *if* SDM data is being captured with other Consent Directive data) (location of SDM data TBD)
    b. Person's identifier and other demographic information (from CR)
    c. Form of consent e.g. Grant Consent to Disclose all PHI; Grant Consent to Disclose some PHI; Deny Consent to Disclose any PHI; Deny Consent to Disclose some PHI
    d. Consent conditions/constraints - on data; on users; other constraints e.g. indications, clinical context
    e. Method of receipt of directive e.g. in person; mail; telephone; fax, electronic

f. Consent event dates e.g. date received; effective date (date signed); data recorded; end date; (*other dates are applied automatically through direct links with other EHRi components e.g. patient's date of death in the CR)*
g. Indicator of Consent to Participate status (flag) (if req*uired e.g. in jurisdictions with express consent models)* e.g. Yes; No; Not Determined *(or a specific Consent Directive may be required – see Use Case 3.1.10)*
h. Free text notes.

6. The user reviews the Consent Directive data with the person to ensure it has been recorded accurately before the data is transmitted to the EHRi.

7. After the data is transmitted, the CDMS responds by:
   - Notifying the user of success/failure of the Record Consent request
   - If the Consent to Participate flag has been promoted to the EHR Index or the CR, updating the EHR Index/CR appropriately.(assumes Consent to Participate status needs to be captured as per jurisdictional requirements)
   - Creating and transmitting an audit record to the Secure Auditing Service.

10. The user provides the person with a printed copy of their electronic Consent Directive if requested, or agrees to send an email copy. (assumes secure email).

11. The user requests the person to sign a printed copy of the electronic Consent Directive or ensures that a pre-completed paper Consent Directive form has been properly signed. The signed copy is retained and stored (manually or electronically) by the EHR Consent Registrar. *[Note: In the near future, it is expected that a person will have some means of electronic identification that can be leveraged for non-repudiation e.g. a digital signature. Once that is in place, retention of paper forms should not be required.]*

12. The use case ends.

Post-Conditions: A valid Consent Directive to Disclose the person's PHI is saved in the EHRi.

Variations:

- The person mails or faxes their completed Consent Directive form to an EHR Consent Registrar. The person's identity and information on the completed form are validated through other approved processes (automated and manual).
- The person completes additional Consent Directives e.g. for different domains.
- The person requests a Keyword. (See Use Case 3.1.4.)

3.1.3 Mask specific PHI

Note: *This use case is being included in order to illustrate the use of the HL7v3 Mask Records transaction.*

Business Description: A patient visits her healthcare provider (family physician) to request that recent records of test results and the related diagnosis (Hepatitis B) be masked from everyone other than the family physician. She works at the local hospital and does not want her co-workers or other employees to get access to this information.

Pre-Conditions:

- The patient has an existing Consent Directive allowing access to all of her PHI in the EHRi to all healthcare providers involved/who may be involved in her care.

- The family physician has explained the risks of masking with respect to:
    - its possible impacts on ability to provide appropriate assessment and treatment
    - the need to create a Consent Directive to Disclose that is specific to the masked data
    - the possibility of overriding that directive without her consent in an emergency situation i.e. to allow other providers to view her masked data, or
    - overriding the directive with her express consent (or keyword where applicable).

- The patient has indicated that she wishes to proceed with the masking.

Assumptions:

1. The CDMS will ensure that masked data is recognized as such and that unauthorized access is prevented.

2. The CDMS may have additional responsibilities and functions with respect to masking requests and data masking (TBD).

Basic Flow:

1. The physician accesses the LIS and requests all lab test results for the patient from the preceding two days.

2. The physician selects the Hepatitis B lab test results from the list returned.

3. The physician submits a request to mask the Hepatitis B lab test.

4. The physician accesses the Shared Health Record (SHR) and submits a request to List Health Conditions.

5. The physician selects the diagnosis of Hepatitis B from the list returned.

6. The physician submits a request to mask the diagnosis of Hepatitis B.

7. The relevant EHRi services respond by:

    - Notifying the physician of the success/failure of masking of the Hepatitis B lab result.
    - Notifying the physician of the success/failure of the masking of the diagnosis of Hepatitis B.
    - Creating and transmitting audit records of the masking events to the Secure Auditing Service.

8. The physician creates a Consent Directive to support disclosure of the masked data to the family physician. (See Use Case 3.1.2. – Create Consent Directive to Disclose.)

9. The CDMS responds by:

    - Notifying the physician of the success/failure of the Record Consent request.
    - Creating and transmitting an audit record to the Secure Auditing Service.

Post-Conditions:

- The specified records are masked.
- A Consent to Disclose Directive specific to the masked data is stored in the EHRi.

Variation 1: Workshop participants proposed that this use case could be approached alternatively without the use of masking messages - by the creation of a single Consent Directive, based on the specific data category (Hep B related), that denies access to all authorized users except the family physician.

This variation would invoke Use Case 3.1.2. – Create Consent Directive to Disclose PHI.

Variation 2: The person requests a Keyword to allow her to control who has access to her Hep B diagnosis and lab test results. Keywords and masking are usually exclusive, but both options could be offered e.g. a keyword could be used to allow the person to directly control access to their masked data. Placing a keyword on the records means only those who know the keyword can see them – exception – override of the keyword. (See Variations for use cases 3.1.7 and 3.1.8.) Without the Keyword, anyone who submits a query against those records will get an error message "Keyword required".

3.1.4 Create a Keyword (to permit a person to directly control who accesses and views their PHI data in the EHRi)

Business Description: A person requests her healthcare provider, other EHR Consent Registrar or HELP Desk staff to help her create a Keyword to ensure that she has direct control over who can see her sensitive PHI.

Pre-Conditions:

- A Consent Directive granting Consent to Disclose PHI already exists and is stored in the EHRi.
- The person has reviewed online information regarding the purposes and uses of a keyword.
- The user has accessed and reviewed the online public information with the person or their SDM regarding keywords, including the creation and protection of keywords and the implications of using a keyword, to ensure they understand the use and implications of a Keyword.
- The person has not had a keyword previously.

Assumptions:

1. A person will only have one keyword for all of the PHI in the EHRi that they wish to control/restrict access to, regardless of the number of Consent Directives they have created to disclose their PHI.

2. Multiple keywords may need to be considered as the scope and detail of the PHI in the EHRi increases and more data that is considered sensitive is collected. Possible options may include:

    - A keyword for a specific category or categories of records
    - A keyword for a specific record or record(s).

3. A person may change their keyword as often as they wish. However, frequent changes will require the person to advise all users (to whom they have given the Keyword) each time it changes. The likelihood of the person forgetting the Keyword will increase with frequent changes.

4. The CDMS (or a separate application) will have functionality to address forgotten keywords including password hints.

Basic Flow:

All Steps in Use Case 3.1.2. – Create Consent Directive to Disclose are assumed or the creation of the Keyword is the start of the use case.

1. The user directs the person or their SDM to a private data entry screen where the "Create Keyword/PIN" functionality is available as well as a separate alphanumeric keypad for the person to enter the keyword.

2. The person/SDM (or the user on the person's behalf) enters the requested information. (Screen may be populated with the person's name and demographic data since the person has already been validated in the CR.)

3. The person/SDM/user selects the type of PHI they want the Keyword to apply to from a pick list or data enters the specific information.

4. The system requests the person to enter a Keyword and then to confirm it.

5. The Keyword is issued to the person.

Post-Conditions: Keyword is stored in the Client Registry (to be confirmed).

3.1.5 Change a Consent Directive to Disclose

Business Description: A person wishes to change some of the conditions and constraints on an existing Consent Directive to Disclose their PHI.

Pre-Conditions:

- A Consent Directive to Disclose already exists in the EHRi.
- Pre-conditions 2. to 5. in use case 3.1.2 – Create Consent Directive to Disclose - as applicable.

Assumptions:

1. If a Consent Directive is changed, the new version replaces the previous version.

2. The new version has a unique ID that is linked to the unique ID of the previous version of the directive. This will allow the directives to be linked for purposes of reviewing Consent Directive History.

3. Consent Directives that are replaced will remain available for auditing or reporting purposes, but will no longer be subject to CDMS application and interpretation prior to allowing access to the PHI to which they pertain.

Basic Flow

1. The user submits a List Consent Directives request and is presented with information about the Consent Directive (s) that currently exist.

2. The user asks the person which directive(s) they wish to change.

3. The user submits a Get Consent Directive request for the selected Consent Directive that is to be changed. The Directive is displayed on the screen.

4. The user asks the person what changes they wishes to make in terms of the conditions/constraints to be applied to the Consent Directive e.g. from a pick list. The options are the same as for Use Case 3.1.2 - Creating a Consent to Disclose Directive.

5. The user enters the changes to the Consent Directive data and any additional explanatory text notes the person wishes captured.

6. The user reviews the Consent Directive data with the person to ensure it has been captured accurately before the data is transmitted to the EHRi.

7. The user sends a Record Consent message to the EHRi.

8. The CDMS responds by:

    - Notifying the user of success/failure of the Record Consent request
    - Creating and transmitting an audit record to the Secure Auditing Service.
    - Notifying (or requesting other HIAL services to notify) authorized users who have access to the person's PHI, and have expressed an interest in such notification, of a change in the person's Consent Directives. (UK has a concept of "legitimate relationship" between provider and patient that could be utilized to facilitate this type of notification.) *[Note: Broad user interest in this functionality needs to be determined. It was raised by participants in the April 2007 consent workshop. This type of notification could quickly become onerous and complex.]*

9. The user provides the person with a printed copy of their new Consent Directive if requested, or agrees to send an email copy (assumes secure email).

10. The user requests the person to sign a printed copy of the new Consent Directive. The signed copy is retained and stored by the EHR Consent Registrar (assumes that digital signature capability is not yet available).

11. The use case ends or repeats if the person wishes to change more than one Consent Directive.

Post-Conditions: Previous Consent Directive is superseded (replaced by) a new version.

3.1.6 Cancel (abort) Consent Directive to Disclose

Business Description: A person decides that a particular Consent Directive to Disclose her PHI is no longer required e.g. specific directive preventing disclosure to her ex-husband because her ex-husband is now deceased. [Note: Some jurisdictions may refer to this use case as Remove Consent Directive.] *Q: Could this be achieved through a Record Consent transaction that simply changes the End Date to the requested cancellation date?]*

Pre-Conditions: The Consent Directive exists and is active i.e. subject to CDMS processing.

Assumptions:

1. Consent Directives that are cancelled will remain available for auditing or reporting purposes, but will no longer be subject to CDMS application and interpretation prior to allowing access to the PHI to which they pertain.

2. No Consent Directive will be physically deleted from the EHRi.

Basic Flow:

1. The user submits a List Consent Directives request and is presented with information about the Consent Directive (s) that currently exists.

2. The user asks the person which Consent Directive they wish to cancel.

3. The user selects the specified Directive and submits a Get Consent Directive request. The Directive is displayed on the screen.

4. The user reviews the Consent Directive data with the person to confirm that the Directive is to be cancelled and not replaced with another version.

5. The user sends a Cancel Consent Directive message to the EHRi.

7. The CDMS responds by:

    - Notifying the user of success/failure of the Cancel Consent Directive transaction.
    - Creating and transmitting an audit record to the Secure Auditing Service.
    - Notifying (or requesting other HIAL services to notify) authorized users who have access to the person's EHR, and have indicated an interest in such notification, of a change in the person's Consent Directives. (UK has a concept of "legitimate relationship" between provider and patient that could be utilized to facilitate this type of notification.) [Note: *Broad user interest in this functionality needs to be determined as noted on use case 3.1.5.]*

8. The user provides the person with an acknowledgement form to sign, which affirms the person's request to cancel the Consent Directive.

9. The user provides a copy of the signed acknowledgement form to the person on request. The signed copy is retained and stored (manually or electronically) by the EHR Consent Registrar.

10. The use case ends or repeats if the person wishes to cancel more than one Consent Directive.

Post-Conditions: The Consent Directive remains stored in the CDMS Consent Repository or elsewhere in the EHRi, but is no longer subject to retrieval or application/interpretation by the CDMS. *[Q: Is there any value in flagging cancelled directives?]*

3.1.7 Override Consent Directive to Disclose (with consent) (grant temporary access to view masked data)

Business Description: The patient discussed in Use Case 3.1.3 (Mask specific PHI) has a consult with a specialist regarding her diagnosis of Hepatitis B.

Pre-Conditions: The specialist logs on to his EHRi account and swipes the patient's health card. He requests access to a clinical profile of any PHI sent to the EHRi in the past month. He receives a warning message indicating "There were 6 masked records that were not returned." The patient indicates the nature of the information that is masked. The specialist advises that he needs to see the masked information in order to complete his assessment and prescribe a course of appropriate treatment. *[Note: Workshop participants expressed concern that returning the number of masked records may reveal enough information for the provider to infer the nature of the data in the masked records. This response message originates with CeRx and should be reviewed in terms of possible privacy issues.]*

The patient grants consent for the specialist to view all of her masked data for a limited time e.g. for 24 hrs after the conclusion of the encounter (this covers the period for the return of any test results the consultant might order).

Assumptions:

1. The masked records remain masked throughout the period the user is given access to view the records.

2. Override with consent allows only the user who initiated the request to view the masked records unless the person consents to allowing others e.g. user delegates, to also view the masked records.

3. The duration of permission to view the masked data should be specified in the override request e.g. up to 24 hrs after the end of the user session, and relevant legislated and policy requirements as well as jurisdictionally specified criteria.

4. The same user may re-access the data multiple times within the specified time frame and criteria.

5. Policies will need to be implemented regarding the copying and sharing of masked data that is disclosed for a limited time to a specific user or users.

Basic Flow:

1. Follows Use Case 3.1.2 - Create Consent Directive to Disclose the masked data to the specialist for a specified period, or is a submit Override Request with the default reason as "person has granted temporary consent".

2. When the specialist retrieves the masked data, it is flagged as "masked", [reminding the physician that the data is sensitive and should not be disclosed to anyone else in the way other non-masked data might be].

3. The CDMS responds by:

    - Notifying the physician of the success/failure of the Record Consent Override request.
    - Creating and transmitting an audit record to the Secure Auditing Service.
    - Terminating access when the physician logs off at the end of the patient session (default) or based on the time parameters included in the override request.

Post-Conditions: The masked record remains masked but accessible to the physician during the period of temporary access. Once the access time limits expire, further access requests are denied to the specialist.

Variation: **Patient has a keyword that she gives to the physician to allow viewing of her masked records**. [With a Keyword, there may be no need to mask the records, since those records cannot be viewed by anyone who does not have the Keyword.]

- The physician clicks on the "Enter Keyword/PIN" tab and the patient provides the physician with her keyword, or,
- The patient asks the physician to pull up the "Enter Keyword/PIN screen to allow her to enter the keyword herself.
- The physician submits a request for retrieval of the masked PHI controlled by the Keyword. The request includes the encrypted Keyword.
- The CDMS compares the Keyword with the version stored on the patient's Client Registry record. If successfully matched, the CDMS allows the masked PHI to be transmitted.
- The masked information is displayed.

3.1.8 Override Consent Directive to Disclose (without consent) (Emergency Override)

Business Description: The same patient (as in Use Case 3.1.7) is brought to the local hospital ER by ambulance in an unconscious state. She appears jaundiced and minimally responsive. Identification found on her person is used to confirm her identity in the Client Registry. While the ER physician is dealing with the patient's immediate life threats, he requests the ER Charge Nurse to access and review the patient's records in the EHRi.

Pre-Conditions: The Charge Nurse logs onto the EHRi and validates the patient's identity in the Client Registry. She attempts to access the patient's PHI and receives a message that access is denied. [Alternatively, she receives a message that "There are 6 masked records that were not returned."] The ER physician asks the nurse to submit an override request.

Assumptions

1. Only authorized users whose assigned role(s) includes override privileges will be permitted to submit an emergency override request.

2. Emergency override may be used to override all existing Consent Directives or only those specific to certain PHI that the user has a need to access e.g. to support clinical decision-making.

3. The reason for emergency override will be provided by the authorized user requesting the override and will be logged in the EHRi.

4. Emergency override may allow only the authorized user who requested the override to view the masked/restricted access data or may allow a group of authorized users e.g. in a facility or department to view the data.

Basic Flow:

1. The ER nurse selects the Record Override Consent option.

2. The nurse receives a message advising that:

    - the override event will be logged in the EHRi Secure Auditing Services including the reason for override
    - a notice will be sent to the Chief Privacy Officer (CPO) of the hospital who will then notify and follow-up with the person whose directives are being overridden.

3. The nurse submits an Override of All Consent Directives request [or a request to see all masked data" or all masked data in the following categories"] which includes the reason for override and additional text notes (if required) to allow full disclosure of all the patient's records in the EHRi.

4. The requested information is displayed to the nurse.

5. At the end of the nurse's session, she logs out and her access privileges to view the data are terminated then or at a later time as specified by jurisdictional emergency override rules e.g. for 24 hours post-override.

6. The CDMS responses include:

    - Verifying the user's role to determine if she is authorized to override the person's Consent Directives
    - Notifying the nurse if the override was successful/unsuccessful
    - Creating and transmitting a record of the override to the Secure Auditing Service (user ID, date, time, reason for override, etc.)
    - Notifying (or requesting the Secure Auditing Service to notify) the Chief Privacy Officer of the override (*to allow the CPO to provide written notice to the person of the override occurrence). [This requirement may be jurisdiction specific.]*
    - Requesting the HIAL Access Services to terminate the user's access privileges in accordance with the override time limits.

Variation: **Patient has a keyword but is unconscious and unable to provide it to the healthcare providers.**

- If an SDM is available who knows the keyword, an emergency override may be unnecessary.
- If the keyword is unknown, an emergency override request results in the requirement for a keyword being ignored.
- Alternatively, an authorized user could override a person's keyword in an emergency by submitting a request to the EHR HELP Desk to reset the keyword to null (BC Pharmanet allows this). However, this is problematic for several reasons:
    - The person would have to be notified that their Keyword was reset and would have to re-establish their keyword if they wished, after the override.
    - In re-establishing their keyword, the person would likely want to set it to its original value to avoid having to inform all of the people that currently have access to that keyword that there is a new keyword.
    - Once the ER physician/nurse resets the keyword, none of the patient's other authorized providers would have access to her PHI without instituting an override request themselves.

Post-Conditions: Consent Directives are re-instated once the override period ends.

3.1.9 Respond to a request for a person's Consent Directive History

Business Description: A recently discharged patient is having a dispute with her local hospital, claiming that the ER staff viewed some of her PHI in the regional EHRi repositories that they did not have permission to view. This has resulted in considerable embarrassment to her, given that she is an employee of the hospital. She asks her family physician to obtain a record of her Consent Directive History for the past 6 months as well as an audit record of accesses to her PHI.

Pre-Conditions: The patient has PHI and Consent Directives stored in the EHRi.

Assumptions:

1. Only authorized users that are designated EHR Consent Registrars will have authority to retrieve a person's Consent Directives and Consent Directive History, and only under specified circumstances.

Basic Flow:

1. The family physician forwards the patient's request for their Consent Directive History to the EHR PMO (phone, fax, mail or online). They forward the request to the CDMS Administrator. [This may also be a direct request from the physician to the CDMS Administrator.]

2. If the family physician is authorized to access the Consent Directive History, then he/she submits the request directly e.g. via their PoS system or the EHRi Clinical Portal.

3. The CDMS Administrator (or the family physician if authorized to access the history):
    - Logs on to the CDMS application
    - Enters the person's identification information to validate their identity (may require the person to be present face-to-face if this information has not been provided to the Administrator)
    - Submits a Get Consent Directive History request.
    - Prints the history returned and provides a copy to the person.
    - Analyses the history if the person requests a report on the details of the history. If the physician prints the history, he/she submits a request for a formal audit report to the CDMS Administrator or the EHR PMO.

4. The request is automatically logged to the Secure Auditing Service.

5. The request for an audit record of accesses to the EHRi is a Secure Auditing Services Use Case i.e. a supporting use case for this use case model and out of scope for this model.

Post-Conditions: Audit records logged for the user requests.

3.1.10 Create a Consent Directive to Participate (to allow collection and storage of PHI) in the EHRi

Business Description: A person contacts an EHR Consent Registrar to grant Consent to Participate and create their Consent to Participate Directive.

Pre-Conditions:

- The person indicates they have not completed any prior Consent Directives to Participate.

- The person has reviewed the relevant consent information on the jurisdictional website, including Consent Directive forms.
- Use case 3.1.2 Pre-conditions (2. to 5.) as applicable.

Assumptions:

1. Consent to Participate (agreement to collect/store data in the EHRi) will be mandated in all jurisdictions except Quebec where jurisdictional legislation specifically requires express consent or refusal for this purpose.

2. Recording a person's Consent to Participate or Refusal to Participate may require a specific Consent Directive, or alternatively, the information may be captured as part of a Consent Directive to Disclose (CDD) (Quebec model). (This use case assumes the creation of a Consent to Participate directive.)

3. Any authorized user will be allowed to view a person's Consent to Participate status through the CDMS system, prior to attempting access to the person's PHI in the EHRi.

Basic Flow:

1. The CDMS displays the Manage Consent screen to the user.

2. The Manage Consent screen displays the Consent to Participate value e.g. Y, N or Blank. If no choice has been set, the value is set to Blank.

3. The user confirms the person's Consent to Participate option – Consent to Participate granted and changes the value to Y.

4. The user Records the Consent to Participate by entering the relevant Consent Directive data:
    a. Person or SDM proof of identification documentation (assumes SDM data is entered in the Consent Repository; this is TBD)
    b. Form of consent i.e. Express Consent to Participate
    c. Method of receipt of the directive e.g. in person; mail; telephone; fax, electronic
    d. Consent event dates e.g. date received; date recorded; effective date (date signed); end date; (*other dates are applied automatically through direct links with other EHRi components e.g. patient's date of death in CR)*
    e. Free text notes.

5. The user reviews the Consent Directive data with the person to ensure it has been recorded accurately before the data is transmitted to the EHRi.

6. After the data is transmitted, the CDMS responds by:

    - Notifying the user of success/failure of the Record Consent request
    - If the Consent to Participate flag has been promoted to the EHR Index or the CR, updating the EHR Index or CR. *[Note: Location of flag TBD. CR is probably the most appropriate location but this will require a change to the pan-Canadian CR specs.]*
    - Creating and transmitting an audit record to the Secure Auditing Service.

7. The user provides the person with a printed copy of their Consent Directive if requested, or agrees to send an email copy. (assumes secure email).

8. The user requests the person to sign a printed copy of the recorded directive or ensures that a pre-completed Consent Directive form has been properly signed. The signed copy is retained and

stored by the EHR Consent Registrar (assumes no digital signature available, at least for initial EHRi implementations).

9. The use case ends.

Post-Conditions: A valid Consent Directive to Participate is stored in the EHRi.

3.1.11 Change Consent to Participate Status (deny consent) - Create Refusal to Participate Directive

Business Description: The person in use case 3.1.10 contacts her healthcare provider (a designated EHR Consent Registrar) to change her Consent to Participate status after hearing a news story about a major privacy breach of bank records perpetrated by sophisticated hackers. She wants no more of her PHI sent to (collected in) the EHRi and no further disclosure of her existing PHI in the EHRi.

Supporting Use Cases:

- Record Consent to Disclose Directive change to full Revocation of Consent to Disclose PHI in the EHRi.

Pre-Conditions:

- Pre-existing Consent to Participate Directive
- Pre-existing Consent to Disclose Directive
- Other pre-conditions 2. to 5. as applicable from use case 3.1.2.

Assumptions:

1. Changes to Consent to Participate status will be recorded as Updates.

2. Changes to a person's Consent to Participate status may require the completion of a specific Consent Directive e.g. Withdrawal of Consent to Participate; Reinstatement of Consent to Participate and/or submission of a request to the EHR Program Management Office or CDMS Administrator.

3. Under these circumstances, unless there are specific legal requirements preventing it, PHI should continue to be collected and stored in the EHRi to ensure information continuity in the event that the person subsequently reinstates their consent. In some instances, data collection may be limited only to PHI that is needed to meet mandatory reporting requirements e.g. for PH surveillance.

Basic Flow:

1. The CDMS displays the Manage Consent screen to the user.

2. The user queries to determine/confirm the person's existing Consent to Participate value e.g. View Person Consent to Participate Value.

3. The Manage Consent screen displays the Consent value as Y (Yes).

4. The user confirms the person's request to change their Consent to Participate value to N (No).

5. The user submits a request to Update the Consent to Participate value to N.

6. The user creates a Refusal to Participate Directive by entering the relevant Consent Directive data e.g. from a pick list or from a Consent Directive form that the person has pre-completed.

7. The user reviews the changes with the person before submitting a Record Consent (Refusal to Participate) request to the EHRi.

8. The user submits a List Consent Directives request in order to review the person's existing Consent Directives to Disclose PHI.

9. The user creates a new Consent Directive to Disclose (a Revocation of Disclosure) that will prevent all future attempts to access any of the person's PHI in the EHRi, including emergency access.

10. The CDMS responses include:
    - Notifying the user of success/failure of the requests to Update Consent to Participate status and Record Consent.
    - Invoking rules to prevent access to all existing PHI in the EHRi for that person
    - If the Consent to Participate flag has been promoted to the EHR Index or the CR, updating the EHR Index or CR. (Location of flag TBD).
    - Creating and transmitting required audit records to the Secure Auditing Service.
    - Notifying the EHR CPO of the change in participation status to Refusal to Participate (may be a jurisdiction-specific requirement)

11. The user provides the person with printed or email copies of their Consent Directives and requests the person to sign the printed copies that are retained by the Consent Registrar.

12. The use case ends.

Post-Conditions:

- Consent to Participate value is changed to N (No).
- Consent to Disclose Directive is changed to a Revocation of Consent to Disclose Directive.
- All access requests to the person's PHI from authorized users are denied and logged with the Secure Auditing Service.
- PHI will continue to be sent to the EHRi unless legislation specifically prevents ongoing collection.

Variation 1: **Jurisdiction and/or person requires/requests that no further PHI be collected in the EHRi after the person changes their Consent to Participate status to Refused (No).**

Additions to Step 10:

CDMS notifies (or requests other HIAL services to notify) all subscribed PoS source systems that are contributing PHI for the person, of the person's change in Consent to Participate status in order to ensure that no further PHI is pushed to the EHRi.

If standard CDMS and Alert/Notification messaging does not exist to accomplish this, the EHR PMO may need to undertake this as a manual/automated administrative function.

Variation 2: **As for Variation 1, but the person allows access to the data already in the EHRi to continue as before i.e. consent to allow access/disclosure prior/up to date "x".**

Assumptions:

1. The CDMS will need to ensure that no conflict exists between these directives (Consent to Participate Refused and Consent to Disclose pre-existing EHR data).

2. Rules must support disclosure under these circumstances. This may require a special type of Consent to Disclose directive or a specific override reason. Alternatively, collection and disclosure consents must be aligned i.e. no collection means no disclosure.

3.1.12 Change Consent to Participate Status (reinstates consent) - Create Consent to Participate Directive

Business Description: About 6 months after changing her Consent to Participate status to Refused, the person in Use Case 3.1.11 experiences a serious medical problem and realizes that access to her PHI is critically important. She asks to change her Consent to Participate status back to Yes.

Assumptions:

1. PHI collected in an EHRi prior to instituting a Refusal to Participate directive will not be deleted or removed.

2. PHI may continue to be sent to the EHRi during the time period that a Refusal to Participate directive is in effect depending on jurisdictional legislative and policy requirements.

Pre-Conditions:

- Consent to Participate exists with a value of N (No).
- Jurisdiction requires that data collection in the EHRi be discontinued during the time that a Refusal to Participate directive is in effect.

Basic Flow: As for Use Case 3.1.11 with the following:

Addition to Step 10:

CDMS notifies (or requests other HIAL services to notify) all subscribed PoS source systems that were contributing PHI for the person, of the person's change in Consent to Participate status (to Yes) in order to restart data transmission to the EHRi.

If standard CDMS and Alert/Notification messaging does not exist to accomplish this, the EHR PMO may need to undertake this as a manual/automated administrative function.

Addition to Step 11:

The user informs the person that her records may be incomplete because no PHI was transmitted to the EHRi during the time she had refused to participate.

Variation: The person claims that her healthcare provider failed to use her PHI in the EHRi to make appropriate care decisions during the effective period of the Refusal to Participate directive. No data was collected during this time period, but access to existing data was allowed. She files a complaint with the provider's professional college and requests relevant audit reports from the EHR PMO and CDMS Administrator.

This variation requires Secure Auditing Services use cases, which are out of scope for this use case model.

3.1.13 CDMS Internal Use Cases e.g. Evaluate Consent (out of scope)

Business Description: These use cases include consent validation, override and handling of keywords. Other internal use cases include those pertaining to management of the CDMS administrative functions.

Pre-Conditions: Consent Directives and PHI exist in the EHRi for a known identity in the Client Registry (CR).

Assumptions:

1. The CDMS must apply consent rules, in conjunction with other HIAL services as necessary, to ensure compliance with Consent Directives, as well as permit override of those directives if pre-defined conditions are met.
2. Consent Directives may be evaluated before data retrieval, and must be evaluated after data retrieval. Depending on the person's disclosure restrictions, the CDMS may need to evaluate some of the retrieved PHI in conjunction with the directives.

Attendees at the iEHR Technical Project Workshop (April 2007), identified these use cases as necessary, but non-core for the current project. It was recommended that they be addressed in a future track of work given the general requirement to document all use cases where the CDMS is the "system under design". Other HIAL services would be Actors in these use cases.

3.2 Additional Use Cases for Consideration

Given time constraints and other complexities, the following use cases were not considered as "core" use cases by attendees at the April 2007 workshop. They are included to allow jurisdictions to review the content and approach, validate assumptions and consider questions and issues raised. These use cases will also help to inform future Infoway project work on Consent Directive Management.

With the exception of Use Case 3.2.1 which is elaborated in more detail, these use cases are presented at a high level.

NOTE: With the exception of limited review of Use Case 3.2.1 (Extra-Jurisdictional Request for Access), these use cases were not discussed at the Consent Workshop.

NOTE 2: Use Case Assumptions in this section that are identified as not currently included in the Consent Directive Management Framework may be added depending on stakeholder feedback and support.

3.2.1 Extra-Jurisdictional Access Request (for a person's PHI in another EHRi)

This use case was of particular interest to workshop attendees from jurisdictions that are frequently involved in cross-border patient transfers as well as jurisdictions with active telehealth programs where providers and patients may be in different jurisdictions.

Business Description: A patient is visiting her aunt in Saskatoon for the first time. She develops throat pain and difficulty swallowing and decides to visit the local walk-in clinic in case she needs an antibiotic.

Pre-Conditions: The clinic has no records for the patient. She does not have a Personal Health Number (unique identifier) in Saskatchewan. She has no records in the Saskatchewan EHRi. She advises the receptionist that the doctor should be able to "see all of her records in Ontario" using his own computer.

Assumptions:

1. The requirements for consent in both source and requesting jurisdictions may have to be met in order to authorize the requesting EHRi user to retrieve the person's records in the source jurisdiction's EHRi.

2. If the consent rules in the disclosing jurisdiction are more rigorous than those in the requesting jurisdiction, the disclosing jurisdiction must ensure that access is denied.

3. Similarly, if the requesting jurisdiction has more rigorous consent rules than the source jurisdiction, access may be denied.

4. If access is denied under these circumstances, and there is a need to override, this may require the person's express consent, unless there is uniformity across jurisdictions with respect to override policies and rules.

Basic Flow:

- Register patient and create their Saskatchewan (SK) EHR
- Resolve client IDs (SK; Ontario)
- Request access to the person's records in the Ontario EHRi
- Receive notification that records exist for the person in the Ontario EHRi
- Receive notification that access to the Ontario records is denied.
- SK physician overrides access denial with the patient's express consent e.g. places a call to the patient's FP and asks that the FP either override the Ontario Consent Directive to allow temporary access to and transmittal of the patient's PHI or retrieve the patient's records and disclose them to the SK physician by other means e.g. telephone, fax, email.
- Create a Consent Directive to Disclose for the SK EHRi.

- CDMS responses (Ontario):

    - Internal validation of consent rules to determine if disclosure to the requesting jurisdiction meets the conditions/constraints of the person's Consent Directives as well as Ontario's (the disclosing jurisdiction's) legal and policy requirements
    - Notification of other HIAL services to prevent transmission of the person's PHI data to the SK EHRi
    - Where applicable, creation and transmission of an audit record of override with consent to the Secure Auditing Services.

- CDMS responses (SK):

- Consent rules processing to determine if the SK physician is allowed to access the patient's records in the Ontario EHRi based on the new Consent Directive created by the Ontario FP to allow temporary access to the SK FP.
- Notification of success/failure to Record (SK) Consent Directive
- Logging of Record Consent Directive event in the Secure Auditing Service.

Post-Conditions:

- An EHR record and Consent Directive exists for the patient in the SK EHRi
- SK EHR Index and EHR Locator are automatically updated to recognize the addition of the patient's EHR
- Temporary ON Consent Directive remains active until the duration of the consent expires.

3.2.2 Request for Pre-Fetch of DI Exams

Business Description: A referring physician schedules a DI exam for her patient at a facility associated with a regional DI Repository. The scheduled exam is sent to the RIS system for filling. The RIS system notifies the PACS system and the DI Repository in order to pre-fetch any relevant prior exams.

Assumptions [*Note: These assumptions have not been included in the Consent Directive Management Framework document because they were not discussed at the Consent Workshop and require stakeholder feedback.]*

1. Pre-fetching of DI or other existing reports and images for scheduled care or procedures requires submission of an automatic or manual user request to the CDMS to check the person's Consent Directives prior to disclosure of the records to the provider who is scheduled to see the patient or perform the DI exam.
2. The user requesting the records may not be the user who will be accessing and viewing the records e.g. Registration Clerk makes the request; Provider views the records.
3. The user performing the scheduled procedure/care may not be the user who reviews and reports on the results e.g. Radiologist performs the exam; another Radiologist interprets the results.
4. Consent Directives will need to be processed for each user/each step in the process where access to PHI is required.
5. The full set of prior exams may not be disclosed based on the person's Consent Directives, resulting in an incomplete set. Each of the users will need to be notified that records are missing.

3.2.3 Public Health (PH) Request to Access Records of Multiple Individuals in the EHRi

Business Description: A Public Health administrator submits a request to the regional health authority (RHO) (or has been pre-approved based on meeting specific RHO criteria) to query the regional EHRi and retrieve all ER patient records related to an outbreak of communicable disease e.g. filter ER encounter records based on a specific time period, location, symptoms indicative of the disease, etc.

Assumptions: [Note: These assumptions have not been included in the Consent Directive Management Framework document because they were not discussed at the Consent Workshop and require stakeholder feedback.]

1. Legislated PH investigative and bio-surveillance requirements will override Consent Directives that deny disclosure of PHI, if access to that PHI is required to support PH's mandate.

2. PH access for the protection of public safety will be an approved reason for override in every jurisdiction.

3. PH override will be done on an individual record basis rather than as a "blanket" override.

3.2.4 Record author is denied access to the record in the EHRi

Business Description: A patient who has filed a complaint against her family physician with his professional college wishes to create a Consent Directive, denying that physician access to any of her PHI in the EHRi, including records that the physician has authored.

Assumptions:

1. The default consent to disclose is that the author of a record in the EHRi (including authors who update or supersede a record) will have access to that record on an ongoing basis e.g. the provider who ordered the test gets to see the result, even if the record has subsequently been masked.

2. Denial of EHRi access to a record's author is not feasible for a number of reasons:

    - It forces a provider to retain their own separate records of all data, rather than accessing the EHRi for some of the data.
    - Given that providers are required by law to retain records of all their patient interactions and care activities, removing permission to see something in the EHRi that already exists in their local records does not achieve anything.
    - It keeps the provider from seeing important PHI such as the fact that a prescription they wrote has been stopped, which they have the right to see and is necessary to see to ensure safe and quality care.
    - If data can "vanish" in the EHRi, providers will not trust the EHRi and will not use it to support clinical decision-making and patient care.

The following assumptions were put forward at the Consent Workshop (April 2007) in support of this type of access control, but are not supported by the iEHR Technical Project team for the reasons noted above.

3. If a patient wishes to deny access to a record that a healthcare provider has authored, the patient will be required to create a Consent Directive that denies the provider access (either explicitly or by association).

4. If that same provider subsequently orders tests or provides care for the patient, they will be denied access to the results and related records in the EHRi unless the patient changes their Consent Directive and allows the records to be disclosed to the provider.

5. If a provider has a denial of Consent to Disclose Directive placed against him/her, that provider should also be barred from sending the patient's data to the EHRi.

3.2.5 Circle of Care member is denied access

Business Description: A patient is not comfortable with a particular provider on her care team. She asks her family physician to create a Consent Directive, denying that provider access to any of her PHI in the EHRi.

Pre-Conditions: The patient's family physician explains the Circle of Care concept to the patient to ensure she understands the implications with respect to denying access to her PHI to one or more members of the Circle.

Assumptions: [*Note: With the exception of #2, these assumptions have not been included in the Consent Directive Management Framework document because they require further stakeholder feedback.]*

1. Health professional standards of practice permit a provider to share a patient's healthcare information with other providers involved in the patient's care, without requiring further consent from the patient, other than as a courtesy i.e. consent to share with these providers is implied.

2. The default consent to disclose to members of the Circle of Care is that a patient's PHI in the EHRi will be automatically disclosed to all members of the Circle.

3. Based on clinical judgement, if another provider in the Circle determines that the records need to be shared with the provider who has been denied access, the provider seeking to share can ask the patient to provide temporary access to the records (override with express consent).

4. If a provider attempts to disclose the records without requesting override with express consent, the CDMS should issue a security alert to the disclosing provider, with automatic creation of an audit record in the Secure Auditing Service.

3.2.6 User attempts to access a person's PHI in the EHRi based on having a paper copy of the PHI

Business Description: A receptionist in a physician's office finds a paper printout of her ex-husband's PHI records from the regional EHRi and tries to access his full set of records using the identifiers she finds on the paper copy.

Assumptions:

1. Being in possession of a paper copy of a PHI record does not convey authority to access that person's records in the EHRi. This situation could result in a significant threat to a person's privacy.

2. Access to PHI under these circumstances should be denied unless the user has pre-existing authorized role-based access e.g. a patient hands a pharmacist she has not seen previously, a paper copy of a prescription and the patient does not have a Consent Directive in place that denies access to the user.

3.2.7 A person's Consent Directives or a user's access privileges change during a user session

Business Description: A user-session or patient-session allows access to a patient's PHI in the EHRi for several hours at a time, with screen locks at shorter time intervals. During this time period, Consent Directives, user access privileges or both may change.

Assumptions:

1. This is a PoS/Portal security issue, not a CDMS issue and therefore out of scope for the CDMS use case model.

2. If consent is given for a particular user to access and disclose a person's PHI in the EHRi, that user is obligated to treat that PHI as confidential. If they leave the PHI displayed on their workstation, or accessible while they are not in control of it, they are not meeting their obligations.

3.2.8 Person creates/changes/removes their own Consent Directive(s).

Business Description: A person accesses an EHRi portal to create, view and modify his or her own Consent Directives.

Assumptions *(Note: This has been briefly addressed as a single assumption (#42) in the Consent Directive Management Framework)*

1. The person will require a digital signature e.g. via a smartcard or other token in order to access the EHRi portal.

2. The person will need to be assigned consent management privileges by the EHR PMO or other EHR Consent Registrar.

3. Privileges will need to be reviewed and renewed at regular intervals as determined by the jurisdiction.

4. Privileges cannot be delegated to a SDM.

3.2.9 Other Masking Use Cases

3.2.9.1 A person wishes to mask their PHI at the point of data capture i.e. at the PoS system level rather than masking it in the EHRi.

Assumptions:

1. If a person has masked some of their PHI in a PoS system, they will be advised of the implications of sending this data to the EHRi. The person may request that this data be stored only in the PoS system or that it remain on paper (paper chart).

2. If PHI is masked at the PoS system level and sent to the EHRi, it will also be masked in the EHRi.

3. The CDMS and other HIAL services the CDMS invokes or otherwise interacts with will be able to recognize that PHI is masked upon receipt and process that PHI as if it was masked at the EHRi level.

4. Prior to masked data being sent to the EHRi, a CDD pertaining to the masked data should be reviewed/created/changed to ensure that it reflects the person's wishes regarding who will have access to the masked data in the EHRi.

3.2.9.2 A provider persists masked data from the EHRi in their EMR or other PoS System

Assumptions:

1. In general, the importing of EHRi data into PoS systems has inherent patient safety and medico-legal issues e.g. records get out of sync; EHRi inability to efficiently identify/notify PoS systems of a change in the data that was imported; possible violation of Consent Directives; medico-legal responsibilities if the data is changed erroneously at the PoS level and subsequently relied upon for clinical decision-making.

2. CDMS and related HIAL services will not have control over access to the masked data once it is imported into a PoS system.

3. There is no ability to ensure that the patient's Consent Directives are honoured at the PoS level beyond the provider's discretion and willingness to respect the patient's wishes e.g. flag the record in the PoS as masked; honour the patient's Consent Directives.

4. If a provider attempts to import masked data (assumes the patient has granted the provider access to view the masked data) from the EHRi, mechanisms should be available to prevent this import – for example:
    - Explicit consent before import is allowed *(How to enforce this through the EHRi/CDMS?)*
    - Error message when import attempted
    - Alert/warning message when import attempted
    - Other mechanisms TBD.

5. If EHRi data previously imported into a PoS system is subsequently masked in the EHRi, mechanisms should be available to ensure that the PoS system is made aware of the EHRi masking event e.g. alert/notification to those PoS system(s) that have previously imported the relevant EHRi data; EHRi tracking of any EHRi data imported by a PoS system and tracking of the PoS system by ID.

3.2.9.3 A person wishes to mask their demographic data, but allow access to their healthcare data in the EHRi

Assumptions:

1. The risk of domestic violence or other known threats to a person's life or to their family may be avoided or reduced if their residence and contact/next of kin information is masked.

2. Only the minimum amount of data should be masked in order to attain the desired protection the person is seeking e.g. record level demographic data only; address and other contact identifiers in the CR excluding the PHN.

3. This type of masking will need to be examined in terms of potential impacts on patient identification in emergency care situations as well as impacts on risk avoidance/reduction, given that the EHRi is only one source of demographic data.

Masking limited to demographic data may require a specific flag in the CR.

Appendix 1 – Administrative Use Cases

Administer Consent Requisition and Forms Completion Processes

Currently, these processes involve few electronic components, but enhanced automation is expected in the near future.

Use cases include:

a) Develop and Distribute Notices of Disclosure
b) Develop relevant Consent to Disclose PHI Forms based on jurisdictional consent model
c) Distribute consent directive forms
d) Facilitate completion of consent directive forms
e) Collect completed forms.

a) Develop and Distribute Notices of Disclosure and related informational and communications materials

If the jurisdictional consent model is implied consent, the EHR PMO may be required to issue a public Notice that informs the public, providers and healthcare organizations of:

- the collection of PHI in and disclosure from the EHRi repositories
- the purposes for which their PHI may be accessed and used by authorized requestors in the EHRi context, and
- their right to fully or partially deny or revoke consent for such disclosure, (where legislation and policies permit), and
- where applicable, their right to deny or revoke consent to participate.

Possible use cases for electronic processes include:

- EHR PMO creates, updates and stores public Notices via an online facility (in addition to traditional means – mail, fax) as well as related explanatory information, FAQs, etc.

- person views, downloads Notices and related information and acknowledges review of same (the last point will require secure email and digital signature capability for people to access and use the EHRi Portal for this purpose)

- person sends an electronic (email) request to the EHR PMO to withdraw consent to disclose their PHI to the EHRi (future state – will require secure email and digital signature capability for the person to use the EHRi Portal for this purpose)

- electronic linkage from the Notice web page to Consent Revocation forms for the person downloading

- HELP desk staff provide assistance via email or telephone (implies staff with specific expertise and training in dealing with informational consent management) (see next point)

- HELP desk staff access the website and other Consent Directive information, with selected authorized access directly to the CDMS, to facilitate information requests and requests for assistance from the public.

c) **Develop Consent to Disclose Directives (forms) and related information materials.**

Consent forms and/or related materials should include/speak to:

- The person's identifying information and, where the person is incapable, information about the legally recognized SDM who is completing the form on behalf of the person.
- The nature of the person's PHI that may be disclosed, including SHR and domain repository data.
- The purpose for which the person's PHI may be disclosed, including benefits and risks of non- or partial disclosure related to healthcare.
- The type(s) of providers and location(s) of providers and other authorized users the person's PHI may be disclosed to
- The person's right to expressly consent to the disclosure of all or part of their PHI by completing and submitting the relevant consent form (applicable to "opt in" models).
- The person's right to expressly deny consent for the disclosure of all or part of their PHI by notifying the EHR PMO or other EHR Consent Registrar and submitting the relevant consent forms (applicable to "opt out" models).
- The process by which the person may expressly revoke (withdraw) their consent i.e. person originally gives consent to disclose, then changes their mind.
- The process by which the person may mask certain parts of their PHI and restrict access to the masked data through the use of Consent Directives and,
- The process by which the person may reinstate their consent to disclose all or part of their PHI.

Partial disclosure will require the person to identify the information that they do not wish to have disclosed. This can be achieved by:

- Documenting on the consent form, the specific names and other pertinent identifiers of the information e.g. medication name and DIN, diagnosis; and/or,
- Selecting one or more categories of information e.g. Demographics, Drug Information, Allergy Information, Health Condition Information, Lab Information and Diagnostic Imaging reports and/or,
- Manual means e.g. pharmacy printout; drug receipts; paper copy of person's chart with relevant information high-lighted – to be submitted with the consent form i.e. the person provides a document to the EHR Consent Registrar which can be used to identify the information that the person does not wish to disclose. This information is then captured on the consent form by the registrar.
    - This approach could result in potential disclosure of PHI to any number of persons in the administrative chain. However, consideration has to be given to people like seniors and others who have cognitive problems and/or lack full understanding of their medication names, details, etc. For them, it will be easier to bring in paper copies of relevant drug/other PHI to ensure that their Consent Directives are completed appropriately.

Controlling access to information may require the person to:

a) make a Consent Directive declaration that is inclusive or exclusive in nature, for example:

- Access to the PHI I have agreed to disclose is granted to all healthcare providers involved in my care with the exception of - list "x"
- Access to the PHI I have agreed to disclose is only granted to the following healthcare providers involved in my care - list "x", and,

b) specify access permissions e.g. by provider; facility; practice group; provider type, or

c) make a consent declaration on a provider-by-provider basis, or

d) create a keyword (password) which allows the person to grant access to all or selected PHI at their own discretion.

Possible use cases for electronic processes include:

- create, update and store consent forms via an online facility (in addition to traditional means – paper, mail and fax) and related explanatory information, FAQs, etc.

c) Distribute Consent to Disclose Directives and related information materials

Consent forms may be made available for electronic download by individuals or their healthcare providers from a dedicated EHR PMO site.

Possible use cases for electronic processes include:

- person views and downloads consent forms and related information
- person sends an electronic (email) request to the EHR PMO to withdraw consent to disclose their PHI to the EHRi (requires secure email and digital signature).

d) Facilitate completion, modification of Consent Directives

Possible use cases for electronic processes include:

- person's healthcare provider and/or HELP desk staff provide assistance via email or telephone
- HELP desk staff access the EMR PMO website and other Consent Directive information to facilitate information requests and requests for assistance in completing Consent Directives
- Designated HELP desk staff have authorized user access to all or selected CDMS services to facilitate requests for assistance in completing or updating Consent Directives

- Near future state: person electronically completes and digitally signs a Consent Directive and submits it via an EHRi Portal e.g. uses a smart card that captures the person's digital signature. [Note: IHE currently has a Digital Signature profile that allows a person to digitally sign Consent Directives.].

Note: The level of assistance to be provided by HELP Desk staff may be determined largely by the scope and complexity of Consent Directives in use in the jurisdiction. In many instances, healthcare provider assistance and possibly privacy officer assistance may be required.

e) Collect consent directives

See d) above for use cases.

Real time electronic reporting of consent is essential to ensuring timely access to information in the EHRi. The alternative manual process e.g. mail forms to the EHR PMO and log them, or log them by telephone will likely be used as an interim solution in most jurisdictions until such time as electronic processes or an operational CDMS is implemented.

Appendix 2 – CDMS Use Case Model (core use cases)