2. the installation of the organisation's POS system is registered with the EHRI and the POS system has a unique POS instance ID;

3. the organisation has met certain administrative criteria, as specified by the jurisdiction, for trusted user management; and

4. the user has registered with the organisation and has a unique POS system user ID (i.e., unique within that organisation and POS system).

### 7.4.8 Service Components

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

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

### 7.5 Access Control in the Desired Future State

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

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

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

Access control decisions are driven by access control policy. Such policy is among the most important of the many policies listed in section 10.3 that are required for the effective functioning of this architecture.
Several access control methodologies must therefore be provided as part of a unified access control service. This service ensures the confidentiality and integrity of PHI. The methodologies are:

a) **role-based access control**, which relies upon the professional credentials and job titles of users established during registration to restrict users to just those access privileges that are required to fulfil one or more well-defined roles\(^{52}\).

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

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

### 7.5.1 Description

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

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

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

---

\(^{52}\) Note that patients/persons are not typically system users, although patients/persons who are able to access all or part of their data online (e.g., via a portal) would indeed be system users who are exercising the role of “Patient”.

\(^{53}\) Discretionary access control is familiar to anyone who has ever used a Windows PC connected to a LAN. The owner of a file is free to grant access rights to the file to others (hence “discretionary” access control). As described in the text, it is presumed that when user A confers discretionary access to a specific patient/person's EHR onto user B, user B has already been registered as a bona fide user of the EHRi. User A is responsible only for granting access, not for attesting or in any other way verifying the identity of user B prior to B becoming registered as a user.
7.5.2 Rationale

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

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

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

Figure 9: Access Control in the Desired Future State

**Figure 9: Access Control in the Desired Future State**

**Privacy and Security Architectural Services**

- Identity Protection Services
- Anonymization Services
- Consent Directives Mgmt Services
- Identity Mgmt Services
- User Authentication Services
- Encryption Services
- Access Control Services
- Secure Auditing Services
- Digital Signature Services
- General Security Services

**POS System Access Control Services**

- Invocation of Common Access Control Services
- Domain Repository Access Control Services

**Privacy and Security Conceptual Architecture Version 1.1**

Copyright © 2005 Canada Health Infoway Inc., All Rights reserved

Page 53
7.5.3 Approaches to Role Based Access Control

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

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

- Professional roles evolved over time to meet the needs of treatment and care; they were not designed with information access in mind. Nevertheless, each regulated healthcare professional is governed (e.g.: in legislation or regulation) by the professional practices as set out in the governing law or regulation that define the nature of the practice. This can be used as a basis of determining the types of information and services needed in the conduct of that profession.

- EHRi roles determine which data elements and functions can be accessed within the EHRi. They do not apply to system functions and data within a POS system. The complexity of EHRi roles depends largely on the complexity of EHRi services, data grouping and access privileges. By way of example, an EHRi that allowed users to view, but not update, EHR data grouped into a few basic categories (health profile, prescription drug profile, lab results, and diagnostic images, say) would not require a large number of roles to be defined. The question of whether professional roles can be mapped effectively to EHRi roles depends in part on the complexity of EHRi roles and therefore depends ultimately on the complexity of EHRi services, data grouping and access privileges.

- POS system roles are determined by the implementing organisation and in some cases by a pre-set role functionality built into the POS system. These roles are often geared to the (sometimes idiosyncratic) features of the POS system and may not map in a straightforward manner to EHRi roles.

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

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

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

2. **Role deployment model 2: POS system roles are mapped to EHRi roles.**
   Standardise a set of EHRi roles as in 1 above and then map POS system roles defined within an organisation to standardised EHRi roles for every organisation connecting to the EHRi within a jurisdiction. There are two ways of technically accomplishing this:
   a) by having each organisation adopt a jurisdictional POS system role schema and then i) have the organisation's POS system or middleware include the jurisdictional POS system role within HL7 messages and ii) have the EHRi map the jurisdictional POS system role to the standardised EHRi role; or
   b) by taking each organisation's roles, mapping them (in consultation with the organisation) to the standardised EHRi roles, and then performing this mapping each time the organisation's POS system includes a local POS system role within an HL7 message. Option b may be easier for...
an organisation to implement technically because it transfers the mechanics of role mapping to the EHRI. This transfer comes at a cost in terms of implementing and maintaining these role mappings within the EHRI and a cost in terms of transactional overhead on each transaction. Either way, the exercise of mapping roles will be organisationally painful.

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

These three approaches are summarised in Table 2.

### Table 2: Approaches to Role Based Access Control

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

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

**7.5.3.1 A ROLE FOR PATIENTS/PERSONS AS USERS OF THE EHRI**

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

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

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

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

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

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

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

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

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

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

To be effective for access control, there must be some means of associating patients/persons with each work group. While it may work well for organisations and clinics, structural work group based access control has some disadvantages when applied to the EHRI because this assignment of patients/persons to work groups is difficult to administer. In healthcare institutions such as hospitals, this is a function of patient admitting and works well for hospital POS systems but there are no automated means by which the EHRI could independently infer which persons are currently admitted as patients to a given hospital, A POS system could report this
information to the EHRi, but subsequently using this information to restrict the access of users of those same POS system may be, from a security point of view, of questionable utility. For clinics too, the association of patients/persons to primary care groups is a registration function fulfilled within the clinic. As rostering of patients/persons to primary care providers is relatively uncommon in Canadian jurisdictions, there is no current source of information available to automate the assignment of patients/persons to primary care work groups.

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

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

1. it can be difficult to maintain group membership and keep it up to date. This is especially true of functional work groups that can change membership frequently. Only work groups based on very stable structural relationships would be readily amenable to providing basis for access control for the EHRI.

2. it can be difficult to infer the relationships of patients/persons to the work group without their being explicitly assigned. There is one notable exception as mentioned above: when the work group consists of a given person's past care providers, it may be possible to infer the composition of this group and its relationship to the patient based on the origin of data in the patient's EHR. This special case could be referred to as a "circle of care" work group (see below).

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

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

### 7.5.5 Approaches to Discretionary Access Control

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

1. when a family physician refers a patient/person to a specialist.

2. when a family physician transfers care of a patient/person (and also a copy of attendant health records) to another family physician. In jurisdictions that have arranged for custodial control of the health profile portion of a patient/person's EHRI to be placed in the hands of the
patient/person’s primary care provider (with attendant responsibility for update and maintenance), this transfer of control would be a necessary component of administering the health profile.

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

Note that security requirement 6354 ensures that discretionary access control does not “trump” role based access control; i.e., conferring access to a patient/person's record to another healthcare provider does not expand their role based access privileges. If a healthcare provider does not have a role that allows access to a prescription drug profile for example, then granting them access to a patient/person's EHR will not allow them to access the prescription drug profile of that patient/person – the point being that their role does not allow them access to the prescription drug profile of any patient/person.

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

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

7.5.6 Availability Requirements

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

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

7.5.7 Implications of Access Control for Provider Registries and User Registries

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

1. In the case of EHRI trusted user management, a user who is also a regulated healthcare provider will have a record in the provider registry. To implement EHRI trusted user management, professional roles (family physician, dentist, pharmacist, …) must be recorded in the provider registry for regulated health professionals. This basic role information would consist of the regulated healthcare profession that the regulated healthcare professional belongs to and the specialisation involved where applicable (e.g. the medical specialty, if any, that a physician licensed to practice).

2. As there will also be a need to register EHRI users who are not regulated healthcare professionals, the user registry will need to contain role information captured during the registration of, for example, delegated EHRI users (see section 7.3.4 above).

3. POS systems will transmit role information as per section 7.5.3 and this information will be available during a user's EHRI session.

54 See the Requirements document listed in the Reference section at the end of this document.
The above contains an implicit assumption about user registries:

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

### 7.5.8 Policy Enforcement

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

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

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

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

### 7.5.9 Process Flow

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

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

The Process is then as follows:

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

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

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

The Process

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

7.5.10 Requisites
EHRI components required are:

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

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

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

7.6 Consent Directives Management in the Desired Future State

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

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

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