Ontario Health

Ontario Health Entitlement Management Procedures Manual

Version: 1.2

Document Owner: Manager, Business Delivery

Ontario Health

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

APPROVER(S)	TITLE/DEPARTMENT	APPROVED DATE
Farzana Banik	Manager, ONE® ID Business Delivery	
Anuj Marya	Manager, ONE® ID Product	

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
0.1	2017-02-07	Initial Draft	John Woodward
0.2	2017-06-15	Security feedback incorporated	John Woodward
0.3	2017-07-28	Additional Security feedback re access criteria incorporated	John Woodward
0.4	2017-08-23	Account Management and ONE ID Business Feedback incorporated	John Woodward
1.0	2017-08-30	Approved version	John Woodward
1.1	2017-10-13	Feedback from Account Management and Security Incorporated	John Woodward
1.2	2020-09-22	Ontario Health rebranding & URL updates	John Woodward

Document Sensitivity Level

Low

About this Document

1.1. Purpose

This document formally defines the procedures to support the entitlement management requirements defined in the Ontario Health Identity Provider Standard and applies to Health Information Custodians (HICs) that will provide their Agents and/or Electronic Service Providers with access to electronic services provided by Ontario Health and/or protected by the Ontario Health Identity Federation.

1.2. Scope

This document addresses functions owned by Ontario Health and describes background information regarding Ontario Health's Entitlement Management Framework and Identity Federation to provide requisite context for the associated procedures. This includes:

- Detailed requirements for Entitlement Management Support Roles (Legally Responsible Person, Sponsor, & Local Registration Authority (LRA)) as well as procedures for establishing and maintaining these roles within a given organization.
- Procedures to add, change, or revoke an individual's entitlement to access a service under the authority of a Health Information Custodian (HIC).
- Detailed requirements for tracking an organization's user entitlements and entitlement requests.

1.3. Out of Scope

The following items are out of scope for this document:

- Entitlement management procedures for services that are not federated and/or are not managed by Ontario Health.
- Detailed identity management procedures.

1.4. Audience

This document is primarily intended for LRAs who have been given the authority to perform the tasks described on behalf of one or more HICs, though individuals fulfilling other roles (e.g. Sponsors) may also benefit from its content. It is assumed that the audience has completed requisite LRA training and has an intermediate level of understanding of the concepts surrounding identity and access management.

Important: **This guide is not intended for LRAs leveraging ONE® ID for Identity and Access Management.** The processes described in this guide are consistent with those in the *ONE® ID LRA Procedures Manual* but ONE® ID LRAs will find that document more directly applicable to supporting their organization's users.

1.5. Approach

This document is intended to serve as a knowledge base for LRAs and, as such, provides requisite background information on the Ontario Health Entitlements Management Framework, Ontario Health Identity Federation, and

the LRA role before describing the procedures they must execute in order to manage user entitlements. Concepts, processes, and policies not managed by Ontario Health but related to an LRA's duties are described at high level in order to provide context.

Entitlement Framework

"Entitlement" refers to an individual's authorization to access an electronic service and their access privileges within said service. Being granted an entitlement requires that an individual meet the access criteria established by the respective application provider and be authorized to access the service under the authority of an approved organization.

This section provides a high level overview of Ontario Health Entitlement Framework, including:

- **Access Criteria** – Conditions set by the respective application provider to determine who may/may not access their service
- **The Sponsorship Model** – Framework to establish accountability between the service, the HIC, and its Agents
- **The Local Registration Authority (LRA) Role** – The individuals who manage user entitlements on behalf of their organization
- **Ontario Health Identity Federation Authorization Service** – The centralized system used for entitlement management for services within the Federation

The Entitlement Management Framework validates an individual's authorization to access services but not their identity. Both appropriate entitlement and identity management are required to ensure secure and reliable access to services. For more details regarding Identity Management, refer to Section 3.

2.1. Access Criteria

Access criteria define both the requirements that a user must meet before accessing a Delivery Channel or Service and what constitutes acceptable use of the service. They may also define permission levels within a service (i.e. role-based access controls) based on the specific data/functionality the user must access.

Access Criteria for Clinical Systems

The following requirements broadly apply to all clinical systems:

1. Access may only be granted to Agents of HICs whose purpose of access is to collect PHI for providing or assisting in the provision of health care.
2. Access **must not** be provided if requested for the purpose of research.
3. Access **must not** be provided if for purposes other than providing or assisting in the provision of health care, e.g., providing access for the purposes of:
    - Program planning, evaluation, or monitoring
    - Risk or error management
    - Improving the quality of care, programs, and services
    - Education and training (unless the individual is a student or resident who requires access to provide care)

- For processing payments.

4. If an agent or Electronic Service Provider has multiple roles, e.g., is both a clinician and a risk manager, they may be assigned access for the purposes of collecting PHI for providing or assisting in the provision of health care. It is the HIC's responsibility to ensure that the end user understands their permissions and obligations.

Access Criteria for Administration Components of Clinical Systems

Administration Components provide non-clinical functionality required to support clinical system, e.g. error handling, reporting, etc. The following criteria broadly apply to all administration components:

1. Access must only be granted to a HICs Agent and/or Electronic Service Providers for the purpose of providing support for the defined and permitted roles of the respective clinical systems. Roles/functions might include:
    - Administrators may require access to error queue management functionality to correct and process messages
    - Privacy officers may require access to privacy reports to generate audit reports
    - Data mapping specialists may require access to the terminology mapping functions to map codes and terminologies.
2. These individuals must not be granted access to functionality intended for those providing healthcare or assisting in the provision of health care (e.g. clinicians).

Service Specific Access Criteria

In addition to the broad requirements described above, more specific criteria may be established by the respective services and may include mandatory training, professional license requirements, affiliation with an organization, etc. Organizations receive detailed information regarding service-specific access criteria as part of service implementation and agree to abide by it by entering a legal agreement with the respective application provider. Appendix A may be used as a reference regarding the access criteria for various services.

2.2. The Sponsorship Model

Generally, Personal Health Information may only be shared with agents acting on behalf of authorized Health Information Custodians. The Sponsorship Model identifies which HICs are authorized and which individuals are acting as their agents, establishing a chain of accountability from the Delivery Channel to the HIC, to the end user. Figure 1 illustrates this model.

Delivery Channels and Application Providers

A Delivery Channel (DC) is an online platform which presents one or more applications/services (e.g. ConnectingOntario presents the Clinical Viewer and OLIS services). DCs make access decisions for the platform while Application Providers (APs) determine what information will be made available to users. DCs and APs determine which HICs are eligible to access their systems (typically by entering into a legal agreement) and advise them of the access criteria for their agents. Depending on their ability to meet these criteria, a HIC may or may not be authorized to sponsor users for all services available via a given DC.

Health Information Custodians

Sponsoring Organizations must be HICs if consuming services for clinical use and the two terms may be used interchangeably in this or other eHealth documentation. HICs apply the access criteria provided and authorize end

users to access both the DC and one or more of the services it presents. In providing authorization, Sponsoring Organizations affirm, in their capacity as a HIC, both that an individual has met the access criteria and that they may act as the HIC's agent when accessing the channel/services. This relationship may be described as the user accessing the service "Under Authority Of" (UAO) the respective HIC.

Within the Sponsorship Model, HICs are represented by 2 roles:

Legally Responsible Person

The Legally Responsible Person (LRP) is a signing authority within the organization. They sign all requisite legal agreements on behalf of the organization and provide oversight to its entitlement management practices, nominating Individual Sponsors and LRAs.

In cases where the LRP does not have visibility into their organization's day-to-day identity and access management operations, it is recommended that they delegate their responsibility to a more appropriate resource by formally notifying Ontario Health, refer to Section 5.1 for more details regarding this process. With the exception of signing legal agreements, LRP Delegates are considered to have the same authority as LRPs with respect to Identity and Access Management.

Individual Sponsor

Individual Sponsors provide authorization to end users on behalf of the HIC. They apply the appropriate access criteria and communicate user sponsorship to LRAs. When eligible to sponsor access to multiple services, organizations must determine which individuals may provide sponsorship for which services, i.e. sponsor are not, by default, eligible to authorize access to all services.

End Users

End users act as agents of HICs within the Sponsorship Model. They are accountable to HICs who are, in turn, accountable to DCs and APs for meeting all access criteria and abiding by any terms of use.

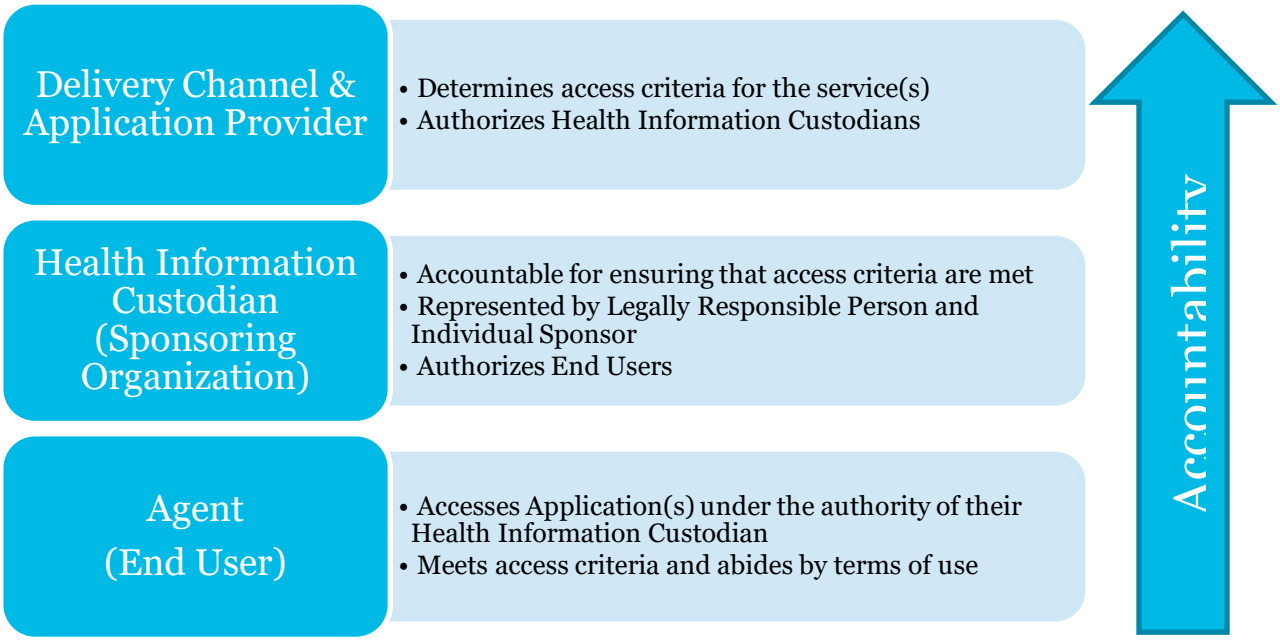


Figure 1 - The Sponsorship Model

2.3. The Local Registration Authority Role

Local Registration Authorities (LRAs) are responsible for managing entitlements on behalf of sponsoring organizations. They support the Sponsorship Model by performing the administrative work necessary to provision access for authorized users. LRAs represent the Sponsoring Organization to Ontario Health for the purposes of submitting entitlement management requests (e.g. add, revoke, change).

LRAs are the resources expected to execute the processes defined in Section 5, although the LRP and/or LRP Delegate may also execute them. Depending on how their organization implements the Sponsorship Model, LRAs may also be assigned the Sponsor or End User roles, though the responsibilities of these roles remain distinct. Refer to Section 4 for a complete description of the LRA role.

2.4. The Federation Authorization Service

The Federation Authorization Service is the centralized means of managing user entitlements within the Ontario Health Identity Federation, tying user entitlements to the Sponsorship Model. The service captures the authorization details provided by LRAs and it may be leveraged by Delivery Channels to support access decisions.

Important: The Authorization Service only manages entitlements for select Federated Services. Some services may rely on other systems to manage entitlements but all must align with the processes described in Section 5. Appendix A provides service-specific details regarding how entitlements are managed.

Usage

Use of the Authorization Service requires that the Sponsorship Model be established for the respective HIC, meaning:

- The DC and AP must confirm to the Federation Operator that the HIC has completed service implementation steps and may authorize users for access.
- The HIC must have established the requisite roles (e.g. LRA & Sponsor) to support entitlement management procedures.

As the Authorization Service is integrated with the Ontario Health Identity Federation, only entitlements for accounts issued by Federated Identity Providers may be captured. HICs seeking to use the Authorization Service must therefore make use of either ONE® ID or an approved Local Identity Provider for user authentication.

Authorization Processes

At a high level, LRAs submit Authorization Requests to Ontario Health based on their organization's internal sponsorships processes and Ontario Health creates or updates an authorization record accordingly. Detailed processes to use the Authorization Service align with those defined in Section 5.

Entitlement Data

The Authorization Service captures the information reflected in Table1 to uniquely identify the user and their associated entitlements. Note that this table is not meant to reflect actual field names within Authorization Service; it presents the entitlement data elements as "friendly names" to promote understanding. While these data elements are

captured for all authorizations, some may be limited or pre-determined depending on the nature of the request, the service, or the HIC authorizing the request. Further details regarding requisite entitlement data can be found in Section 5.

Data Element	Description
Type of Request	Either add or revoke service
Login ID	The Login ID of the individual authorized for service access
Identity Provider	The accredited body that issued the Login ID
Health Information Custodian	The organization which has sponsored the user for access
Delivery Channel	The platform on which the authorized service will be consumed
Service	The Service for which the individual has been authorized
Role	Service Specific information regarding the individual's level of access

Table 1 – Entitlement Data Elements

Ontario Health Identity Federation Overview

The Ontario Health Identity Federation is a business and technology framework which establishes trust amongst member organizations with respect to end user identity validation, authentication, and access. Common agreements, policies, and technology standards enable secure access to provincial services via local credentials.

The Ontario Health Identity Federation allows organizations to authenticate users locally and send the requisite information to federated services which, in turn, allow access. The established trust within the Federation ensures confidence that the information shared is both valid and secure and enables a "Single Sign-On" (SSO) experience for end users such that they can use a single Login ID & password to access both local and provincial services. This section provides a high level description of the Identity Federation Framework, including:

- **Infrastructure of Trust** – the foundation that permits secure online sharing of Personal Health Information
- **Organization Roles and Responsibilities** – member organizations may fulfill one or more roles within the Federation
- **Entitlement Pre-Requisite** – User Entitlements require a credential to authenticate the user's identity to a sufficient level of assurance

LRAs must be familiar with the Identity Provider(s) (IDP) used by their organization and the federated services its users access; detailed information on these topics should be provided by the respective IDP/Service. The material in this section is provided as background information for LRAs such that they can understand how these components support identity and access management within the Federation and make informed decisions regarding user entitlements.

Important: Not all services rely on Federation infrastructure however alignment with its Identity Standard is a pre-requisite for accessing all services managed by Ontario Health, i.e. requirements for identity assurance and authentication must be met before Personal Health Information can be accessed online, regardless of the technical specifics.

3.1. Infrastructure of Trust

Trust is a cornerstone in the effective delivery of healthcare services and that includes the electronic delivery of personal health information. While trust can be established within care teams though professional or personal relationships, the eHealth Identity Federation is intended to help establish trust on a provincial scale.

Federation relies on legal agreements to bind member organizations to a shared set of policies, processes, standards, and infrastructure related to Identity, Authentication, and Access (IAA) Management. The IAA business and technology infrastructure of member organizations need not be identical, but it must conform to criteria established by the Federation and be capable of interfacing with Federation Infrastructure.

Because all member organizations are operating within a common framework, they can have confidence in the security and integrity of one another's practices, i.e. Federated Delivery Channels can trust Federated Identity

Providers and accept authentication of their users. Criteria for Federation membership includes but is not limited to the following:

Identity

- Users must have their identities validated with sufficient rigor to ensure that individuals are who they say they are
- Credentials must uniquely identify users within the Federation
- Users must be authenticated prior to their credentials being updated

Authentication

- Passwords used for authentication must meet standards for strength, complexity, and validity period
- Additional authentication factors (e.g. location, hardware token, etc.) must be available when required for access to Federated Services

Access

- User authorization to access Federated Services may be granted only by organizations approved by the service
- Access and Identity Management are independent, i.e. a change to a user's service authorization(s) will not necessitate a change to their credentials.

3.2. Organization Roles

Member Organizations may fulfill one or more roles within the Federation:

Federation Operator

Ontario Health fulfills the role of Federation Operator and is responsible for establishing/enforcing policies & standards, entering into agreements with member organizations, and managing technical infrastructure (referred to as the "Federation Hub" in this guide). The Federation Operator works with member organizations to establish and support their role(s) within the Federation.

Identity Provider

Organizations with the Identity Provider (IDP) role create and maintain credentials for end users based on their real world identities and authenticate them for access to Federated Services. IDPs must comply with Federation business and technology standards with respect to user identity management and authentication and complete technical integration such that they can pass validated data to the Federation Hub.

An organization must assume this role in order to enable an SSO experience for its users. Organizations that are not IDPs may leverage ONE® ID, the Provincial IDP, for user authentication to Federated Services.

Delivery Channel

Delivery Channels (DCs) provide an online interface (e.g. a Portal) through which end users may access one or more applications/services. DCs make access decisions and present services to users based on authentication messages from the Federation Hub. A DC need only integrate with the the services it presents and the Federation Hub; it can accept IDP authentications as they have been routed through the Federation Hub.

Application Provider

Application Providers (APs) are responsible for the ehealth services presented by to end users by DCs. APs establish their own access criteria and may need to establish relationships with DCs and HICs independent of what's required for Federation, e.g. an AP may require a HIC to sign a distinct service agreement even if they are already a Federation member.

Health Information Custodians

HICs leverage Federation infrastructure to access ehealth services. They are likely to have relationships with Application Providers independent of their use of Federation (e.g. they may be required to sign a service agreement) as their role is to authorize users for access as per The Sponsorship Model. This role does not require technical integration with the Federation Hub, but an Organization would also have to assume the role of IDP to enable an SSO experience for its users.

3.3. Entitlement Prerequisite

Before an individual can be authorized to access a service their identity must first be verified with sufficient assurance to meet the requirements of the respective Application Provider, i.e. only valid credentials may be authorized for access. Identity Providers establish an identity assurance level for all registered individuals and issue credentials that may be relied on to authenticate an individual's identity. Such credentials are a pre-requisite for entitlement to access a service. Refer to the Ontario Health Identity Provider Standard for further details regarding Identity Assurance.

The User Registration Process is defined by the respective IDP and may or may not be executed by the same resource that manages entitlements. Regardless, the process must be completed prior to user entitlements being granted and the LRA must be able to confirm that the credential being granted access belongs to the individual being authorized. Refer to Section 4 for more details.

3.4. Identity Management Outside of Federation

Some services managed by Ontario Health are not integrated with Federation infrastructure (e.g. the ConnectingOntario Admin Portal). Such services still have identity assurance requirements and rely on IDP processes to ensure that they are met, i.e. an AP will issue a non-federated credential for their service only after the user's identity has been validated by an IDP. In these circumstances, IDP credentials are submitted as part of entitlement requests both as proof that such validation has taken place and to create an audit trail between the service credential and the user's identity.

Local Registration Authorities

"Local Registration Authority" is a common term in Identity and Access Management referring to anyone granted the authority to verify end user identities, issue them credentials, and/or manage access to services. Ontario Health uses this broad definition to refer to anyone authorized to interact with the Agency with respect to Identity and Access Management.

The responsibilities of individual LRAs are driven primarily by their sponsoring organization. Some organizations may consolidate all identity and access management support functions in a single role (that may or may not be called "LRA" within the organization) while others may divide responsibilities amongst several roles. From eHealth's perspective, anyone formally identified as an LRA is authorized to support entitlement management as described in this manual, even if they are not executing all processes.

Important: This manual is not meant to supersede an organization's internal practices or role definitions but rather to define the processes by which LRAs interact with eHealth systems and support personnel for the purpose of managing user entitlements. Interactions for other purposes and/or with other bodies are beyond the scope of this document.

4.1. Requirements

To become an LRA, an individual must be nominated by a Legally Responsible Person or their Delegate to act as an agent on behalf of their organization for the purposes of supporting identity and access management. Additionally, LRAs must:

- Be registered in Ontario Health's ONE® ID system at Identity Assurance Level 2. LRAs must be known to Ontario Health prior to submitting requests. Registration in ONE® ID allows the Agency to authenticate their identity as necessary.
- Complete Privacy and Security training material provided by Ontario Health. Additional training may be required, depending on the LRA's system role (see Section 4.4)
- Be familiar with their organization's Identity and Access Management practices. LRAs may be governed by internal processes/policies not covered in this guide.

In addition to authorization, registration, and training, it is recommended that LRAs:

- Have visibility into the relevant user group(s). Organizations that implement multiple services may require LRAs in multiple departments in order to support all users.
- Have appropriate authority within the organization. LRAs may need to reject or defer requests due to noncompliance and must be comfortable doing so.
- Have sufficient time available to fulfill their duties. The amount of time required is dependent on the size of the organization, the rate of turnover, and the internal processes used to manage sponsorship.

4.2. Entitlement Management Responsibilities

End users can only access services under the authority of a particular HIC if that HIC has provided them specific authorization to do so. It is the responsibility of LRAs to manage such authorization requests on behalf of one or more HICs, this includes:

Verifying user sponsorship

It is the responsibility of LRAs to verify that end users have received sponsorship from an appropriate authority within their respective organization. LRAs must know which individuals and/or roles within their organizations are eligible to authorize end users for access and follow the internal processes by which that sponsorship must be communicated. Refer to The Sponsorship Model for more details.

Submitting authorization requests

LRAs submit user authorization requests to the Ontario Health by email. Refer to Section 5.3 for more details.

Submitting revoke requests

LRAs must submit revoke requests to the Ontario Health for end users who are no longer authorized for access, either because they have left the organization, changed roles, are on extended leave, etc. It is critical that revoke requests be submitted in a timely manner to ensure alignment between the Federation Authorization Service and local systems. Refer to Section 5.6 for more details.

Tracking requests

LRAs should maintain records of user sponsorships, authorizations, and revokes for audit purposes. Ontario Health maintains a record of all user authorizations, but maintaining independent local records allows for verification of system data. Refer to Section 6 for more details.

4.3. Identity Management Responsibilities

The individuals that support entitlement management on behalf of HICs are not necessarily the same individuals who perform identity management, although both functions fit the broad definition of "Local Registration Authority." LRAs acting on behalf of an IDP validate the identities of end users and assign them credentials. The ONE® ID LRA Procedures Manual defines these processes for ONE® ID while other Identity Providers define their processes locally. Individuals performing Identity Management need only be nominated to Ontario Health when their duties require interaction with Ontario Health systems and/or personnel.

For convenience, organizations will often nominate the same individual to support both entitlements and identity management. If this is not the case, the HIC's LRA must have an understanding of the IDP's practices sufficient to perform their own duties. This includes:

Confirming the validity of user credentials

LRAs must recognize the format of the respective IDP's credentials and have a means of confirming their legitimacy, i.e. that the credential is valid and belongs to the user in question. This may include checking employee badges, referring to a company directory, or receiving confirmation from the IDP.

The credential submitted in entitlement management requests for federated services must correspond with the one sent by the IDP during authentication, identified by the "userloginname" attribute in the authentication message. In most cases, this is the "friendly" login ID entered by the user (e.g. JOHN.SMITH@HIS) but some IDPs must use a

different value due to technical constraints. The LRA must be aware if friendly names are not being used by their IDP and have a means of determining the correct value to submit for each user.

Familiarity with the IDP support practices

Users may expect LRAs to be able to manage their credentials and LRAs should be able to redirect them to the appropriate resources.

Visibility into the IDP revocation process

Revocation of user credentials should align with revocation of entitlements. LRAs should be aware of staff turnover and submit revoke requests accordingly.

4.4. Ontario Health LRA System Roles

Ontario Health provisions system roles to LRAs based on the level of access required for them to execute their duties. All system roles fall under the broad definition of "LRA" and have authorization to manage entitlements on behalf of their respective HIC. System roles may enable functionality beyond entitlement management (e.g. identity management in ONE® ID) and may have requirements beyond nomination (e.g. mandatory training).

ONE® ID LRA

ONE® ID LRAs support their sponsoring organization's use of ONE® ID as an Identity Provider. They have received the requisite training and system access to register & enroll users in the ONE® ID system and have access to system functionality to support suspend, revoke, and change processes. ONE® ID LRA processes are consistent with those described in this manual and are further detailed in the ONE® ID LRA Procedures Manual.

ONE® ID ERA

ONE® ID Express Registration Agents (ERAs) support their sponsoring organization's use of ONE® ID as an Identity Provider. They have received the requisite system access to issue registration & enrolment invitations to end users from the ONE® ID system but do not have access to system functionality to support suspend, revoke, and change processes. ONE® ID ERA processes are consistent with those described in this manual and are further detailed in the Express Registration Procedures Guide.

Federation Agent

Federation Agents (FAs) support their organization's use of the Federation Authorization Service. They execute the processes defined in Section 5 on behalf of their sponsoring organization. The FA role is limited to managing user entitlements, though the individual fulfilling it may also support identity management for one or more identity providers.

Test LRA

Test LRAs (AKA Partner LRAs) manage access to services in Ontario Health's DTE-Partner environment for the purposes of testing. They have access to the ONE® ID system in the DTE-Partner environment to register and enroll users for the purposes of testing. They also have the ability to reset user passwords within the DTE-Partner Environment.

4.5. The Sponsor and LRA Roles

Many organizations find it more efficient to have the same individual fulfill both the Sponsor and LRA roles. This is acceptable, but the organization should be mindful of the fact that these roles have distinct responsibilities; it is the sponsor who has the authority to approve (or disapprove) user access while it is the LRA that manages access requests. The size and structure of the organization should be considered when identifying Sponsors and LRAs. The chart below illustrates the distinction between these roles.

Activity	**Sponsor**	**LRA**
Authorize new user for access	X	
Approve modification of an existing user's access, e.g. enable a new role	X	
Revoke authorization for access	X	
Validate end user's credential		X
Submit access request to Ontario Health		X
Submit revoke request to Ontario Health		X
Maintain records of the organization's authorizations and revokes		X

Table 2 - LRA & Sponsor Roles

Entitlement Management Procedures

The procedures defined in this section capture the mandatory requirements for entitlement management requests. Many of these requirements are also likely to be met by a HIC's established business processes and organizations are encouraged to leverage these synergies where possible.

All entitlement management procedures are reliant on authorized individuals (usually LRAs, though LRPs and their Delegates may also perform this function) submitting entitlement information to Ontario Health. The submitter acts on behalf of a HIC and attests that all information provided has been validated. The means of validation may vary as HICs seek to leverage their established processes and tools to support user entitlement management. The means of submission may vary as services provide different templates, systems, and communication channels (see Appendix A for more details) to improve efficiency. Such changes are acceptable, so long as the entitlement management requirements continue to be met.

The workflows in this section are presented in isolation, presuming no integration with client systems/processes and no use of service-specific templates or systems. As such, they may be used to manage entitlements under any circumstances. The requirements that each process seeks to meet are identified at the outset to help identify potential integration points with local processes/systems.

5.1. Legally Responsible Person Delegation Procedure

This procedure identifies the individual assuming the LRP Delegate Role to provide oversite for their organization's Entitlement Management for eHealth services.

Triggers

The LRP Delegation Procedure may be initiated when:

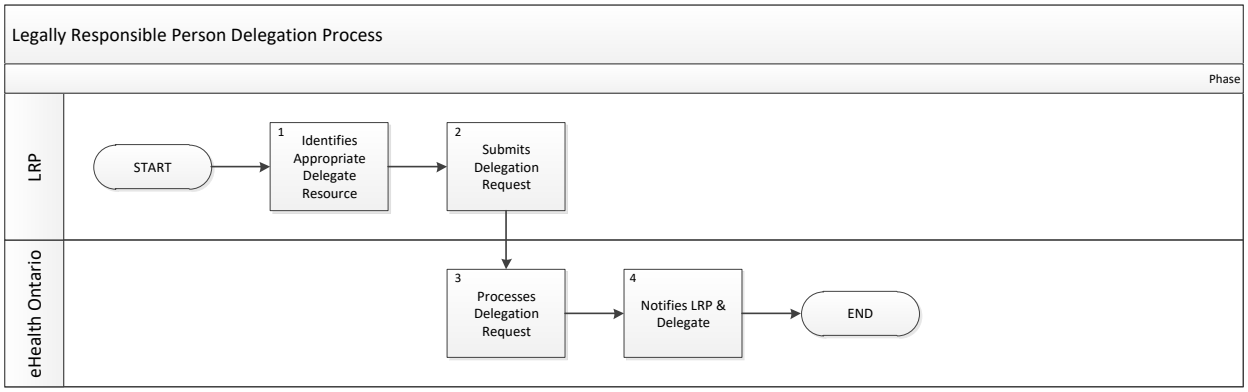
- The LRP determines that another resource would be better able to provide Entitlement Management oversite.
- The organization implements a new service and must identify appropriate resources to support it
- An existing Delegate leaves the organization or changes roles and must be replaced

Requirements

A known and authorized resource must submit a request to Ontario Health indicating:

- **The LRP Delegate's Name and Contact Information** – the Delegate must be identified as a point of contact for Ontario Health
- **Confirmation that the LRP has authorized the individual as a Delegate** – an explicit statement is required indicating which individual is being authorized as the HIC's Delegate

Workflow



Process Steps

#	Step	Actor	Description
1	Identifies Appropriate Delegate Resource	LRP	Identifies the resource with the necessary skills and authority to fulfill the role of LRP Delegate. Refer to Section 2 for more details regarding the role.
2	Submits Delegation Request	LRP	Submits an LRP Delegation Request to ONEIDBusinessSupport@OntarioHealth.ca including: • The name and contact information of the LRP Delegate • A clear statement indicating that this individual has been assigned the role of LRP Delegate.

			The LRP Delegation Form should be used to capture and submit this information.
3	Processes Delegation Request	Ontario Health	eHealth records are updated to reflect the new oversite contact for the organization.
4	Notifies LRP & Delegate	Ontario Health	LRP & Delegate are advised via email that the organization record has been updated.

5.2. Local Registration Authority Nomination Procedure

This procedure identifies the resources authorized to act as LRAs on behalf of the respective Health Information Custodian. The LRP/Delegate is relied on as the organization's only authorized contact if no LRA has been nominated.

Triggers

This process may be initiated when:

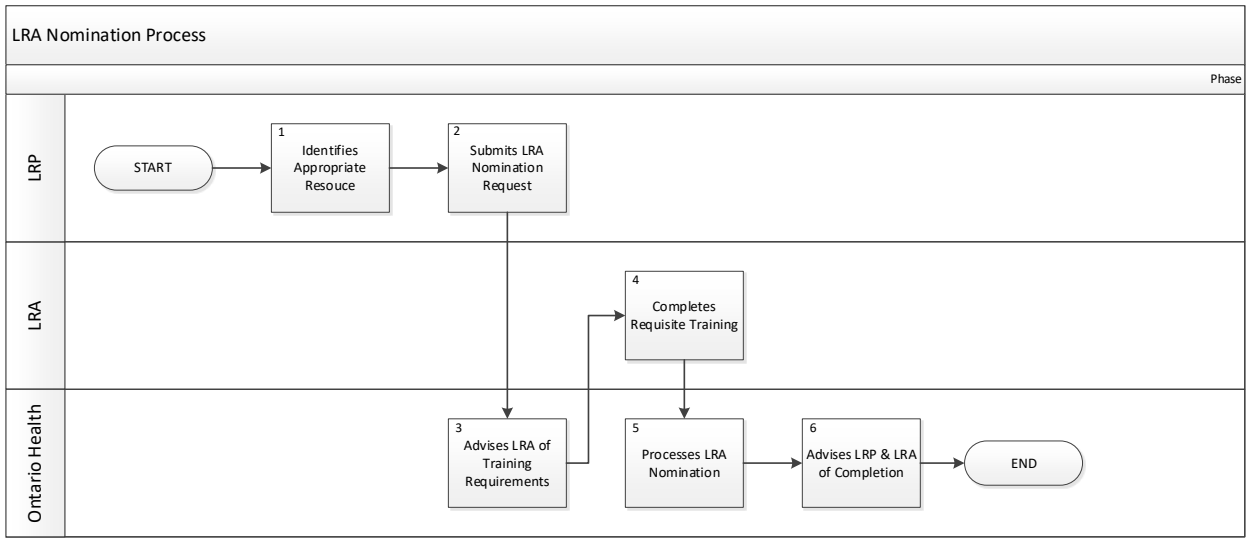
- The organization implements a new service and must identify appropriate resources to support it
- The organization's expands its use of an existing service and a new LRA must be identified to support the new user group
- An existing LRA leaves the organization or changes roles and must be replaced

Requirements

A known and authorized resource must submit a request to Ontario Health indicating:

- **The LRA's ONE® ID Login** – the LRA must be registered in the ONE® ID system at Identity Assurance Level 2 in order to validate their identity.
- **Confirmation that the respective HIC's LRP/Delegate has authorized the LRA** – an explicit statement is required indicating that the LRP has provided authorization.
- **Confirmation of the LRA system roles required** – an explicit statement indicating which system roles are required for the LRA
- **Confirmation that the LRA has completed all requisite training** – training requirements may vary, depending on the system roles requested

Workflow



Process Steps

#	Step	Actor	Description
1	Identifies Appropriate Resource	LRP	Identifies the resource with the necessary skills and authority to fulfill the role of Local Registration Authority. Refer to Section 4 for more details regarding the role.
2	Submits LRA Nomination Request	LRP	Submits an LRA Nomination Request to ONEIDBusinessSupport@ontariohealth.ca including: • The ONE® ID Login ID of the LRA • A clear statement indicating that this individual has been nominated for the LRA Role. • A clear statement of which system roles are required The LRA Nomination Form should be used to capture and submit this information.
3	Advises the LRA of Training Requirements	Ontario Health	Prospective LRAs are advised to complete training as per the requirements of their system role(s). Refer to Section 4 for more details regarding LRA training requirements.
4	Completes Requisite Training	LRA	LRA training may be provided via an in person session, webinar, or online module; method and/or content may vary depending on the system role(s) required.
5	Processes LRA Nomination	Ontario Health	Organization records are updated to incorporate LRA information and system access is provisioned as appropriate.
6	Advises LRP & LRA of Completion	Ontario Health	Notification of process completion is sent to the LRP & LRA via email.

5.3. User Authorization Procedure

This procedure captures a user's authorization to access a Delivery Channel and/or Service under the authority of a particular Health Information Custodian.

Triggers

This process may be initiated when:

- A new service is implemented and the user group must be granted access
- An employee joins the organization and/or assumes a role that requires them to have access to the service
- The organization expands its use of the service such that additional staff require access

Requirements

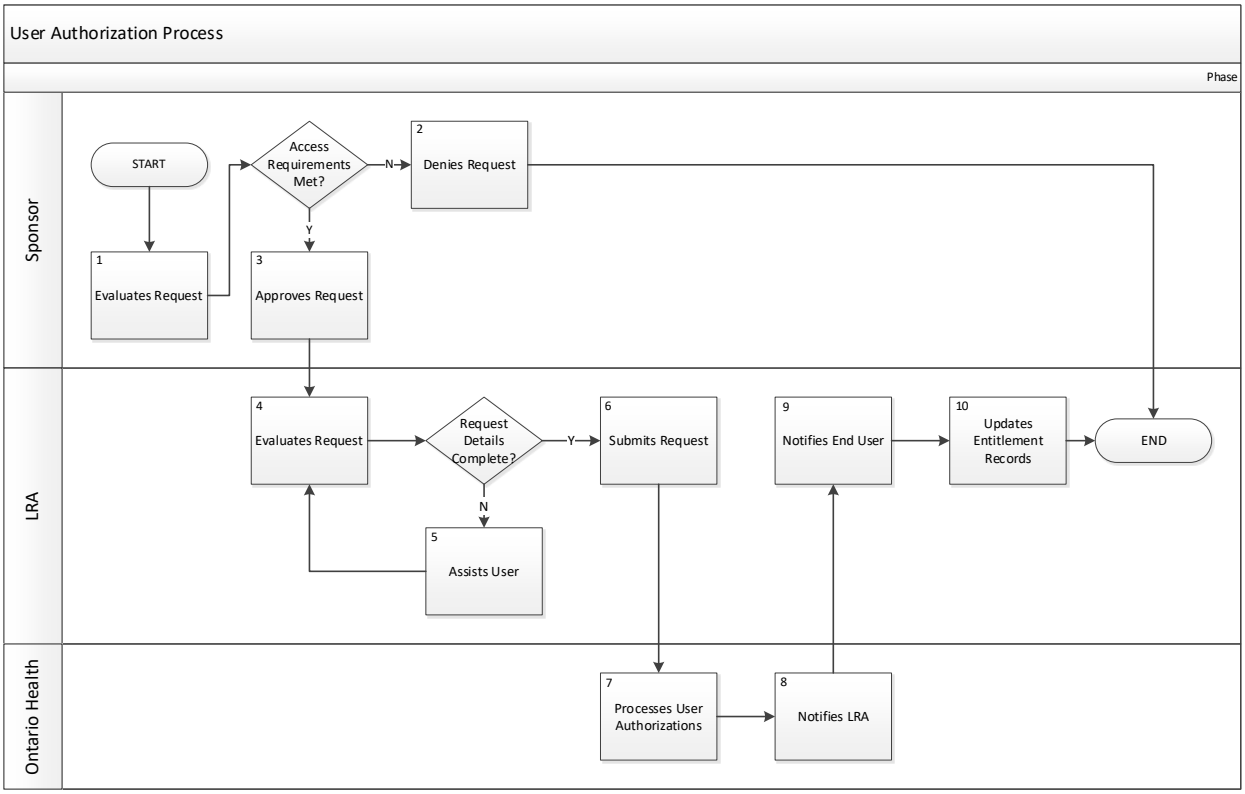
A known and authorized resource must submit a request to Ontario Health indicating:

- **The individual user credential** – the LRA must ensure that the credential being submitted is valid and belongs to the individual being authorized
- **Confirmation that the user has met all service-specific access criteria (e.g. training requirements)** – the request itself is taken as confirmation
- **Confirmation that the respective HIC has authorized the user** – an explicit statement is required indicating which HIC has provided authorization
- **Any service-specific information required to process the request (e.g. role)** – specifics will vary depending on the service, refer to Appendix A for more details
- **The name and contact information of the LRA submitting the request** – Ontario Health must validate that the request has come from a known and authorized individual.

Additional requirements this procedure seeks to meet include:

- **Authorization Tracking Requirements** – See Section 6 for more details

Process Workflow



Process Steps

#	Step	Actor	Description
1	Evaluates Request	Sponsor	Evaluates the request to confirm: • The user has met all service access criteria • The user is authorized to act as the HIC's agent when accessing the service If Access Requirements have been met, go to step 3 If Access Requirements have not been met, the go to step 2
2	Denies Request	Sponsor	Denies the access request and advises the user of the reason. The request may be reinitiated when/if the user meets the requirements
3	Approves Request	Sponsor	Approves the authorization request and forwards to the LRA
4	Evaluates Request	LRA	Evaluates the request to confirm: • The appropriate Sponsor has provided authorization to access the service • A valid credential has been captured for the user • Requisite service-specific details have been captured If the request is complete and valid, go to step 6 If the request is incomplete or invalid, go to step 5

5	Assists User	LRA	Assists user to close any gaps in the authorization request, this may include: • Redirection to an IDP to have a credential confirmed or validated • Redirection to the appropriate Sponsor for approval • Redirection to a training team to ensure access criteria are met The LRA returns to step 4 once gaps have been addressed.
6	Submits Request	LRA	Submits request via email to ONEIDRegistrationAgents@ontariohealth.ca. Requests must include: • The individual's Login ID • A clear statement of which HIC has authorized or revoked the individual for access. This must be explicitly stated in the email body; an implicit statement (e.g. the name of the organization in the email signature) cannot be relied upon for authorization. • Requisite information regarding the DC/Service(s) required, refer to Appendix A for more information. • The name and contact information of the LRA (may be included in the email signature) • Example email text: "Please grant JANE.DOE@ABCHOSPITAL.CA access to ConnectingOntario as per authorization from ABC Hospital."
7	Processes Authorization Request	Ontario Health	eHealth's entitlement records are updated as per the authorization request
8	Notifies LRA	Ontario Health	Replies to the request email confirming that the authorization has been processed
9	Notifies End User	LRA	Advises end user that the request has been processed and that they can now access the service
10	Updates Entitlement Records	LRA	The HICs records are updated to capture the user entitlement details. Refer to Section 6 for more information

Consolidated Authorization Requests

Authorization requests may be consolidated is cases where request details are common for all users, i.e. an LRA may submit a list of Login IDs in a single request if all users have received the same service authorization. Up to 10 users may be consolidated in a single email request. A Bulk Authorization Request (see below) is required if more than 10 users must be authorized at the same time.

Bulk Authorization Requests

LRAs should contact the Business Delivery Team at ONEIDBusinessSupport@ontariohealth.ca in circumstances where individual email requests are impractical (e.g. during service implementation when the initial user group must be added). As with consolidated requests, authorization details must be consistent for all users. Bulk Authorizations are processed according to a mutually agreed upon schedule.

5.4. User Revocation Request Procedure

This procedure revokes an individual's authorization to access a Delivery Channel and/or Service under the authority of a particular Health Information Custodian.

Triggers

This process may be initiated when:

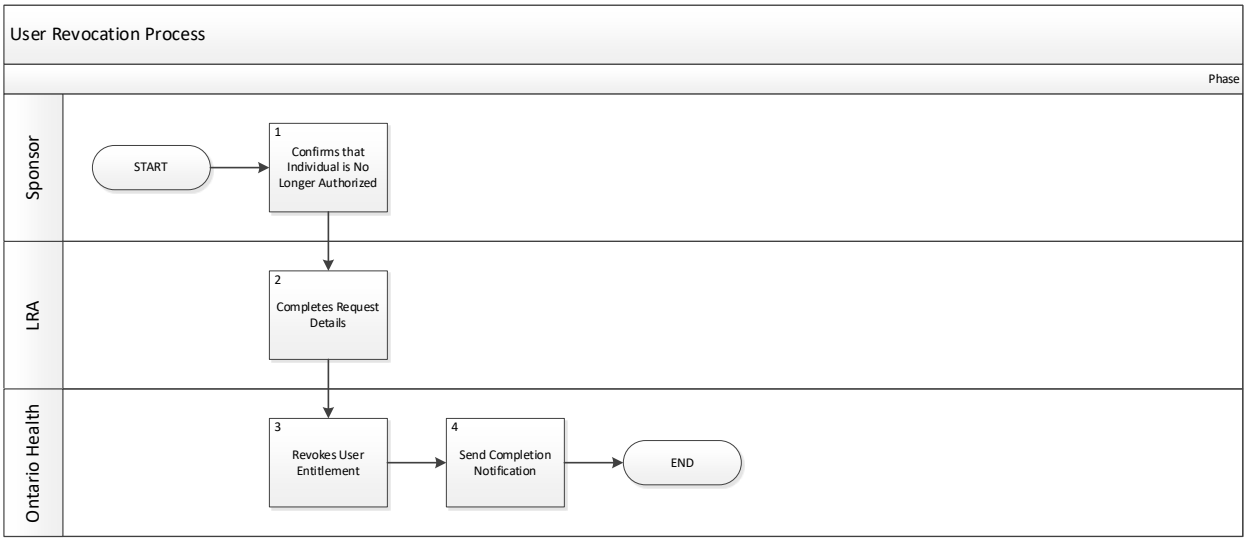
- A user exits the organization
- A user assumes a new role and no longer requires access to the service

Requirements

A known and authorized resource must submit a request to Ontario Health indicating:

- **The individual user credential** – the LRA must ensure that the correct credentials are indicated in the revoke request
- **Confirmation that the user is no longer authorized by the sponsoring organization** – the revoke request itself is taken as confirmation that the user is no longer authorized

Workflow



Process Steps

#	Step	Actor	Description
1	Confirms Individual is No Longer Authorized	Sponsor	Determines that the individual should no longer be authorized for access to the service
2	Completes Request Details	LRA	Ensures that the revoke request contains: • The individual's Login ID • The specific services/roles to be revoked

3	Revokes User Entitlement	Ontario Health	Updates entitlement records to remove the authorization indicated
4	Sends Completion Notification	LRA	Notifies LRA that the request is complete

Consolidated Revocation Requests

Revocation requests may be consolidated is cases where request details are common for all users, i.e. an LRA may submit a list of Login IDs in a single request if all users are losing authorization for the same service/role. Up to 10 users may be consolidated in a single email request. A Bulk Revocation Request (see below) is required if more than 10 users must be revoked at the same time.

Bulk Revocation Requests

LRAs should contact the Business Delivery Team at ONEIDBusinessSupport@ontariohealth.ca in circumstances where individual email requests are impractical. As with consolidated requests, revocation details must be consistent for all users. Users can be revoked in bulk according to a mutually agreed upon schedule.

Compliance and Audit

User Entitlements for eHealth Services must be managed in accordance with the policies and standards of the Ontario Health Identity Federation as well as those of the respective Delivery Channel and/or Service.

This section provides additional guidance regarding an LRA's responsibility for policy compliance and authorization tracking.

6.1. Privacy and Security Requirements

Beyond assuring compliance with the specific processes and policies they support, LRAs have responsibilities with respect to maintaining Privacy and Security. Requirements are described here but LRAs must also receive training from their organization or Ontario Health when assuming the role.

Personal Health Information

LRAs should not have access to Personal Health Information (PHI) in the course of performing their duties, but they do help manage end user access to PHI and should be aware of their obligations under the *Personal Health Information Protection Act*. The Act sets rules for the collection, use and disclosure of personal health information and provides individuals with the right to access and to request a correction of their personal health information.

Prior to leveraging an eHealth Service, an organization must implement practices which assure that they are in compliance with the Act. LRAs are Agents of a Health Information Custodian as defined in the Act and are accountable to their organization for their actions.

Personal Information

The *Freedom of Information and Privacy Act* deals with privacy protection with respect to an individual's right to control his or her own personal information and the privacy rules governing the collection, use, disclosure, retention, and disposal of personal information. Personal information that is collected for the purpose of identity validation and/or handled in the course of executing other LRA responsibilities is covered by the Act.

Prior to leveraging an eHealth Service, an organization must implement practices which assure that they are in compliance with the act. LRAs are primarily accountable to the respective IDP with respect to the handling of personal information.

6.2. Privacy and Security Incidents

Awareness of Privacy and Security requirements will assist LRAs in identifying when/if a Privacy or Security Incident has occurred.

Privacy Incident

A privacy incident includes circumstances where:

- A contravention of (or about to be):

    - A provision of the *Personal Health Information Protection Act, 2004* or its regulations and/or the *Freedom of Information and Privacy Act*;
    - Applicable agreements' privacy provisions;
    - Privacy policies, procedures and practices implemented;
- Personal health information and/or personal information is lost or stolen or has been or is about to be accessed for unauthorized purposes; or
- Records of personal health information have been or are about to be copied, modified or disposed of in an unauthorized manner

Security Incident

An information security incident is any:

- Violation or imminent threat of violation of information security policies, standards, procedures or practices; and/or
- Information security event that may compromise operations or threaten the security of Ontario's Electronic Health Record or related business process.

LRA Responsibilities

In the event of a suspected privacy or security incident, an LRA is required to:

- **Report** the suspected incident **immediately** to their organization's Privacy Officer or Security Officer.
- Take reasonable and safe measures to **contain** the privacy breach or security incident, e.g. revoking the authorization for an account that may have been compromised.
- Be prepared to **participate** in an investigation as required.

6.3. Identity Management Policy Compliance

Identity Management policies and processes are defined by IDPs, though they must align with Federation Policies and Standards. LRAs should receive sufficient documentation and training on these policies and processes from their respective IDP to ensure compliance within the scope of their duties.

6.4. Entitlement Management Policy Compliance

LRAs are not expected to be "gatekeepers" for user authorizations (that is the Sponsor's role). However, they are expected to be aware of policy requirements and direct users/sponsors accordingly. If an LRA has reason to believe that all requirements for an authorization request have not been met, they should suspend processing it until satisfied. Possible examples of non-compliance include but are not limited to:

Scenario	Action
Service-specific access requirement has not been met, e.g. the user has not yet completed mandatory training.	LRA places request on pending until they receive confirmation that the requirement has been met.
User relays sponsorship to the LRA, e.g. "My manager said I should have access."	LRA should follow up with the Sponsor directly to confirm.
A user is seeking to gain access via an unrecognized credential, e.g. the HIC typically relies on a Local IDP but the user wants access via ONE® ID.	LRA should connect with the IDP to confirm the credential.

Figure 2 - Non-compliance examples

Ontario Health can be engaged to assist in cases where the policy requirements are unclear. Inquiries should be emailed to ONEIDRegistrationAgents@ontariohealth.ca.

6.5. Entitlement Tracking

While Ontario Health tracks data centrally, LRAs must also maintain local records of the authorization and revoke requests they've processed. Local records provide a point of comparison for entitlement data and may be relied on in the event of an audit or security incident to confirm the legitimacy of user entitlements.

Data Elements

At a minimum, the authorization record should include:

- The Login ID of the end user
- The name of the individual Sponsor who authorized their access
- The name of the LRA who processed the request
- The Delivery Channel for which the user has been authorized
- The Service(s) (if distinct from Delivery Channel) for which the user has been authorized
- Any service-specific roles or attributes
- The date on which authorization was requested
- The date on which the authorization was revoked (if applicable)

Depending on the organization-specific implementation, some of these data elements may be consolidated or eliminated, e.g. if the Sponsor and LRA are the same individual then their identity only needs to be captured once.

Tracking Process

Where possible, it is recommended that the audit trail be built into the request process. If an existing electronic workflow system is being leveraged, this should happen automatically. Ontario Health does not prescribe requirements for such a system beyond all data elements being captured.

Alternatively, LRAs can retain the email threads between themselves, Sponsors, and Ontario Health as authorization records, though such emails should be stored separately from other correspondence both to ensure clear records and prevent inadvertent disclosure of sensitive information during an audit or investigation.

Manual tracking of authorizations may also be relied on; Appendix B provides a sample template that can be used. This method is not recommended as it is both more labour intensive for the LRA and more prone to human error. It should only be relied on when other options are unavailable.

Authorization Reports

Sponsoring Organizations are required to review their entitlement records at least once per year to ensure that they are accurate and up to date. Ontario Health can provide a report of user authorizations in support of such efforts. LRAs may request such reports by emailing ONEIDRegistrationAgents@ontariohealth.ca.

Appendix A. Service-Specific Authorization

Access criteria are determined by the application provider depending on the information presented and its intended use. Figure 5 maps the eligibility of potential staff roles to various delivery channels/services while the subsections in this appendix provide additional details regarding their respective entitlement management procedures.

Roles	ConnectingOntario Clinical Viewer (Acute Care CDR, OLIS, DHDR)	Connecting Ontario Admin Portal	eHealth Services Portlet (OLIS, Diagnostic Imaging)	OTN Hub	ClinicalConnect (Acute Care CDR, OLIS, DHDR, DICS)
Researchers	NO	NO	NO	NO	NO
Regulated Health Care Practitioners	YES	NO	YES	YES	YES
Health Care Admin staffs (e.g. Ward Clerks)	YES	NO	YES	YES	YES
Resident	YES	NO	YES	YES	YES
Technical Administrators	NO	YES	NO	YES	NO
Local Registration Authorities	NO	NO	NO	YES	NO

Table 3 - Resource Role to Entitlement Mapping

A user may fulfill more than one role in Figure 5 (e.g. they may be both a regulated practitioner and a technical administrator). In such cases, the user must ensure that their use of each authorized service is in alignment with its access criteria and/or acceptable use policy.

• ConnectingOntario ClinicalViewer

The ConnectingOntario ClinicalViewer relies on the Entitlement Management Procedures defined in Section 5. Access to services within the Delivery Channel is managed at the organization level, i.e. all users authorized under the authority of a particular organization will be able to view a common set of services. All organizations receive access to Acute Care CDR data while qualifying organizations also receive access to Ontario Laboratory Information System (OLIS) and/or Digital Health Drug Repository (DHDR) data. **Only the Delivery Channel, "ConnectingOntario", needs to be specified in authorization and revoke requests. No additional attributes are required.**

Access to ConnectingOntario ClinicalViewer requires that all users complete mandatory training delivered by their organization, Ontario Health, or its delivery partner. Regardless of who delivers the training, the respective HIC is accountable for ensuring that all of its users have completed training prior to accessing the service. A copy of the training material can be found here.

Refer to the ConnectingOntario Viewing Guide for more detailed information on ConnectingOntario Access Criteria.

A.2 ConnectingOntario Admin Portal

The ConnectingOntario Admin Portal relies on the Entitlement Management Procedures defined in Section 5, except that user authorization requests should be submitted to ConnectingOntario.Delivery@ontariohealth.ca. The Connecting Ontario Application Registration Form should be used to capture and submit all requisite data.

A.3 eHealth Services Portlet

The eHealth Services Portlet is a service within the eHealthOntario.ca Portal that relies on entitlement management via the ONE® ID system; ONE® ID is the only identity provider that may be leveraged to access this service. ONE® ID enrolment processes align with the procedures defined in this manual but leverage the ONE® ID Web interface instead of email communications. Refer to the ONE® ID LRA Procedures Manual and ONE® ID LRA Users Guide for more details.

A.5 OTN Hub

The OTN Hub is a Delivery Channel for Telemedicine and eLearning Services. OTN Hub relies on the Ontario Health Identity Federation for authentication but not for authorization management, i.e. the Federation Authorization Service is not leveraged and entitlement requests need not be submitted to Ontario Health. Users and/or organizations provide information about themselves and their desired services when requesting access to the Hub and are assigned access as follows:

ROLE	**OTNhub**
Physician – Family Medicine / General Practitioner	eVisit (PCVC and Clinical Ncompass) eConsult (Referrer) Directory
Physician – Specialist	eVisit (PCVC and Clinical Ncompass) Directory
Nurse Practitioner	eVisit (PCVC and Clinical Ncompass) eConsult (Referrer) Directory
Nurse – RN / RPN	eVisit (PCVC and Clinical Ncompass) Directory
Allied Healthcare Professional	eVisit (PCVC and Clinical Ncompass) Directory
Technical Contact, Healthcare Administrator, Telemedicine Coordinator, Other	eVisit (PCVC and Non-Clinical Ncompass) Directory

Table 4 – OTNhub Roles

For more information, go to https://signup.otn.ca/individual-signup/ or https://signup.otn.ca/org-signup/.

A.6 ClinicalConnect

Clinical Connect is a Delivery Channel for practitioners in Ontario's South West region. It is managed by Hamilton Health Sciences and relies on both the Federation Authorization Service and local access management. For this reason, entitlement management requests must first be processed by the DC before being reflected in the Authorization Service. Processes align with those described in this manual, but LRAs submit requests to Hamilton Health Sciences who, in turn, submit them to Ontario Health. Click here for more information regarding an LRA's responsibilities in supporting ClinicalConnect.

Appendix B: Authorization Tracking Template

This template is provided to illustrate the tracking that LRAs must perform as part of the authorization process. It is recommended that tracking be performed via internal workflow management software and/or other established tools within the organization in order to reduce administrative overhead and improve accuracy. This template may be leveraged in cases where such tools are unavailable.

Tracking_Template.xlsx

Appendix C. Glossary

Agent: In relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agency is being remunerated. For example, an agent may be an organization, employee or contractor that validates identities of users on behalf of a HIC; an Agent may perform data correction services for a HIC on their data contribution endpoint.

Application Provider (AP): An organization responsible for the ehealth services consumed end users. APs establish their own access criteria and may need to establish relationships with Delivery Channels and Health Information Custodians independent of their relationship with Ontario Health. Examples include OLIS, DHDR, DIViewer, etc.

Delivery Channel (DC): Delivery Channels (DCs) provide an online interface (e.g. a Portal) through which end users may access one or more applications/services. DCs make access decisions and present services to users. Examples include ConnectingOntario ClinicalViewer, ClinicalConnect, and OTN Hub.

Ontario Health Identity Federation (Federation): A business and technology framework which establishes trust amongst member organizations with respect to end user identity validation and authentication. Members are bound by a common set of agreements, policies, and standards to create an infrastructure of trust within the Federation.

Entitlement Management: The policies, standards, technology, and procedures which establish, control, maintain, and track an individual's entitlements to access electronic services. An individual's entitlements to access services may also be referred to as their "authorizations," "enrolments," "access privileges," or "permissions"

Health Information Custodian (HIC): An organization responsible for collecting, using, and disclosing Personal Health Information in support of the provision of healthcare in Ontario.

Identity Provider (IdP): An Organization that creates and maintains credentials for end users based on their real world identities. IDPs authenticate end users for access to Federated Services and pass validated data to the Federation Hub.

Local Registration Authority (LRA): A person who has been authorized by a HIC to manage the registration and/or enrolment process for its Agents and Electronic Service Providers to obtain access to services. LRAs must be registered with Ontario Health when their duties require them to interact with the Agency's systems or personnel for the purposes of supporting Identity and Access Management.

Legally Responsible Person (LRP): A signing authority for an organization responsible for overseeing its Identity and Access Management processes. The LRP is responsible for authorizing Sponsors and LRAs to act on behalf of the HIC.

Legally Responsible Person (LRP) Delegate: An individual delegated responsibility for overseeing an organization's identity and access management processes. The LRP Delegate has all the authority of the LRP with respect to these processes, although they are not necessarily a signing authority.

Sponsor: A representative of a HIC with the authority to identify individuals as its agents and authorize them to access services under its authority.

Appendix D. References

The materials listed below are linked in line throughout this document and/or provide further details on its content. They are consolidated here for ease of reference:

Reference	Location
Ontario Health Acceptable Use Policy	https://ehealthontario.on.ca/files/public/support/AcceptableUsePolicy_EN.pdf
Ontario Health Identity Services Schedule	https://ehealthontario.on.ca/files/public/support/Identity_Services_Schedule_v1_7_(Nov_2016)(no_signature_block).pdf
Ontario Health Identity Federation Identity Provider Policy	https://ehealthontario.on.ca/files/public/support/Federation_Identity_Provider_Policy_EN.pdf
Ontario Health Identity Provider Standard	https://ehealthontario.on.ca/files/public/support/eHealth_Ontario_Federation_Identity_Provider_Standard_EN.pdf
Ontario Health Information Security Policy	https://ehealthontario.on.ca/files/public/support/Information_Security_Policy_EN.pdf
Ontario Health Personal Health Information Privacy Policy	https://ehealthontario.on.ca/files/public/support/Privacy/PHI_PrivacyPolicy_EN.pdf
Ontario Health Personal Information Privacy Policy	https://ehealthontario.on.ca/files/public/support/Privacy/PI_PrivacyPolicy_EN.pdf
Ontario Health Privacy and Data Protection Policy	https://ehealthontario.on.ca/files/public/support/Privacy/Privacy_and_Data_Protection_Policy.pdf
ONE®ID Policy	https://ehealthontario.on.ca/files/public/support/ONE_ID/Registration_Community/one_id_policy.pdf
ONE®ID LRA Procedures Manual	https://ehealthontario.on.ca/files/public/support/ONE_ID/Registration_Community/one_id_lra_procedures_manual.pdf
Privacy & Security LRA Training	https://ehealthontario.on.ca/support-topics/lra-privacy-security-training/story.html