Local Registration Authority Procedures Manual

ONE ID Business Support | 2024-03-25

Ontario Health

Ontario Health

Table of Contents

Ontario Health

About this Document

This document for Local Registration Agents (LRAs) describes the various roles, responsibilities, and functions of an LRA for supporting ONE ID processes within their organization on behalf of Ontario Health.

It describes the procedures, guidelines, and functions that an LRA can perform for ONE ID. This includes the process of registering and enrolling individuals and communicating with others within the organization about ONE ID processes.

Audience

This document is intended for LRAs that have been authorized to execute ONE ID processes on behalf of Ontario Health and their organization(s). An LRA should have an intermediate level of understanding of registration, service enrolment, and change management concepts.

Reference Material

This manual provides the necessary instruction and background information for LRAs to fulfill their duties. The documents listed below provide additional information:

- ONE ID Policy and Standards: These documents provide the conditions and requirements of ONE ID pertaining to registering, enrolling and authenticating individuals, in which an organization is bound to as part of an Agreement with the Agency.
- ONE ID Implementation Package: This document serves as an overview and guide to implement ONE ID within an organization.
- Privacy FAQs: This document addresses some basic questions about Privacy and Security practices endorsed by the Agency.
- ONE ID Local Registration Authority User Guide: This document provides LRAs detailed step- by-step procedures of registration functions they can perform in the ONE ID System.
- ONE ID Registrant Reference Guide: This document provides the registrant with detailed step-by- step procedures to self-manage their ONE ID account.
- ONE ID Acceptable Use Policy: This document must be agreed to by all ONE ID registrants (including LRAs).

Additional supplemental and service specific reference material can be found on the ONE ID Registration Community and should be reviewed as necessary.

Introduction

ONE ID is a set of systems and business processes that provides secure and trusted access to health care applications and services to healthcare providers in Ontario. ONE ID enables registration, authentication, and authorization for access to digital health services offered by Ontario Health and its partners.

The purpose of the ONE ID System is to ensure that individuals who are authorized to electronically access personal health information (PHI) under the control of Ontario Health are permitted to do so.

ONE ID leverages employees at health care organizations to perform registration and enrolment duties on behalf of Ontario Health. These individuals are known as Local Registration Authorities (LRAs) and are registered, sponsored and trained on the ONE ID processes, policies and system.

Prior to leveraging ONE ID services, organizations must enter a legal agreement with Ontario Health for the provisioning of services, products or technologies as well as nominate individuals to fulfill the Authorized Representative, Sponsor, and LRA roles. These roles and the ONE ID business processes are described in detail in this manual.

LRAs are the primary ONE ID support contact for individuals within their organization and must have an understanding of ONE ID policy and processes to fulfill their role. This includes:

- Validating identities and registering and enrolling individuals in the ONE ID system
- Ensuring that individuals receive appropriate authorization prior to granting them access to any services.
- Protecting the privacy and security of the personal information they must access in the course of their duties
- Communicating with staff in their organization and Ontario Health
- Fulfilling and/or submitting ONE ID requests made by their organization to Ontario Health

Ontario Health has Registration Agents (RAs) who are the experts on the ONE ID service. LRAs can contact ONEIDRegistrationAgents@ontariohealth.ca for additional support in any ONE ID registration activity.

The LRA Role

The Local Registration Authority (LRA) role is assumed by individuals who have been nominated by their organization(s) and approved by Ontario Health to perform ONE ID registration, enrolment, change, and support requests on behalf of their organization(s).

LRAs take part in authenticating, authorizing, user management, and following auditing requirements established by the provincial government, your organization, and Ontario Health.

Qualifications

The following qualifications must be met in order to become a ONE ID LRA:

- Willing to fulfil all duties described in this manual
- Familiar with their organization's onboarding practices, accountability structure, and local record keeping
- Familiar with Privacy & Security principles and best practices as they pertain to handling personal information
- Registered by Ontario Health at Assurance Level 2
- Nominated by their organization's Authorized Representative
- Approved by the Ontario Health Registration Authority

Duties and Responsibilities

The following list summarizes the responsibilities of an LRA. Additional details can be found throughout the LRA Procedures Manual.

- Providing guidance to other LRAs and registrants within their organization
- Communicating and maintaining a list of sponsors and registered users for their organization
- Validating the identity of individuals and sponsors
- Registering other LRA's and individuals and adding service enrolments to authorized accounts
- Liaising with Ontario Health on registration issues
- Responding to Ontario Health requests to validate the identity of individuals

Sponsorship

Sponsorship is the first step in the registration and enrolment process. It is the means by which organizations identify an individual's authorization to access services and their privileges within those services under that organization's authority. While organizations are accountable for this authorization, they are represented by individuals fulfilling the Authorized Representative and/or Sponsor roles.

Authorized Representative Role

The Authorized Representative (AR) is identified during the Agreements process when an organization first engages with ONE ID and/or when an established AR submits an Authorized Representative Delegation Form. An Authorized Representative will be accountable for the registration and enrolment processes for their organization.

The AR is authorized to:

- Engage Ontario Health for access to eligible services (such as ConnectingOntario).
- Engage Ontario Health regarding changes to their ONE ID implementation (e.g. evaluating their internal identity validation process)
- Nominate new LRAs via submission of a Local Registration Authority Nomination Form.
- Identify new Sponsors (see below)
- Fulfill the Sponsor and/or LRA roles as required (i.e. If no other LRA or Sponsor is nominated, then the Authorized Representative must fulfill these responsibilities)

Sponsor Role

The Sponsor's role is to authorize individuals to be enrolled for services under the authority of their organization. This role is managed internally within their organization and Sponsors should be familiar with the service(s) for which they are authorizing users.

Sponsors are responsible for:

- Confirming that registrants have a legitimate reason to access the service(s) in support of the organization.

- Confirming that registrants have met the specific access criteria for the respective service(s)
- Confirming that additional approvals/pre-requisites imposed by their organization are received/met
- Identifying the role(s) (access privileges) that registrants should receive in a given service
- Updating and/or rescinding authorization as warranted by changing circumstances
- Communicating sponsorship information to their organization's LRAs for entry into ONE ID

Obtaining and Tracking Sponsorship

LRAs should follow their own organization's internal request and approval process for obtaining and tracking sponsorships. If there is no such process, the LRA should develop a system with the organization's management. Refer to General Guidelines for more information.

Sponsors and LRAs

Best practices require separation of duties with respect to Identity and Access Management, i.e. the individual authorizing users should not be same individual that captures the authorization in the system. That said, resource constraints may require that the same individual fulfill both the Sponsor and LRA roles for their organization.

The key difference between Sponsors and LRAs is that Sponsors authorize user access, whereas LRAs complete and execute ONE ID support processes and serve as the main point of contact for staff requiring additional support.

A Sponsor or an LRA cannot authorize or make legal changes to their own account. It must be approved by the Authorized Representative, another Sponsor, or LRA.

The responsibilities of each role are depicted in the table below.

Roles and Responsibilities	Sponsor	LRA
Identifies prospective registrants	✓	
Documents the user's entitlement to access a service	✓	
Responsible for the registration processes		✓
Responsible for adhering to the ONE ID policies	✓	✓

Maintains list of sponsors per service and assists other LRAs		✓
Conducts identity validation and processes the Registration & Service Enrolment Requests		✓
Processes changes to service enrolments		✓
Processes changes to registration information		✓
Answers registration and service enrolment questions from registrants		✓
Liaises with Ontario Health on Identity and Access issues		✓

Identity Validation

ONE ID's Registration Process relies on an individual's real world identity to create a digital identity, which is then used to authenticate their access to applications. "Real world identity" is reflected in ONE ID by capturing the user's **core identity information** (legal name and date of birth) and validating this information to a prescribed level of assurance.

Granting an account online access to personal health information requires a minimum level two of assurance (**AL2**). Individuals must present one piece of government issued photo ID and one piece of corroborating evidence in a face-to-face (in person or video conference) meeting. This may occur prior to (Identity Validation by Organization) or during (Identity Validation by ONE ID Process) the Registration and Enrolment process.

As an LRA, you must be satisfied with the legitimacy of the means used to validate the individual's identity. If you have any cause to doubt the veracity of an individual's identity, you may request to review an additional identity document or reject the registration.

Identity Validation by Organization

Identity validations performed by your organization (typically as part of onboarding) may be relied upon to create ONE ID accounts at AL2. Your organization's processes must be confirmed to meet ONE ID requirements before they can be used for this purpose, contact OneIDBusinessSupport@ontariohealth.ca to initiate the evaluation process.

As an LRA, you are responsible for confirming that Registrants have completed your organization's identity validation process and that the information entered in ONE ID aligns with what is captured in your system. How this information is shared varies between organizations, but may include any or all of:

- Participating in the employee onboarding process
- Referring to company directory
- Referring to a Human Resources Information System
- Review of the Registrant's Employee ID Badge

"Express Registration" refers to the processes and supporting functionality used to register and enroll users that have previously completed an identity validation within their organization as part of the hiring process. **Local Registration Authorities (LRAs) may use this functionality in lieu of performing a face-to-face identity validation**.

Capturing Identity Information

Once you have confirmed that the Registrant's identity has been previously validated, complete the registration and enrolment in ONE ID, select the appropriate options to indicate your organization as the source of identity validation and enter:

- Legal First and Last Names
- Email Address

Self-Registration Invitations

After entering identity information, select the appropriate enrolment(s) and issue a registration invitation. The system will send an email with a unique link to the registrant and generate a random Invitation Code for you to provide via another channel.

The Registrant will enter the remaining account information when completing the invitation. You can direct the Registrant to the ONE ID Express Self-Registration Guide for instructions on how to self-complete the invitation.

Refer to the Express Registration Agent Procedures Guide and the Registration and Enrolment Process for more information.

Federated Identities

ONE ID integrates with other identity providers (Local IDPs) to provide a single-sign-on experience between local (e.g. an HIS [Health Information System]) and Provincial (e.g. a Clinical Viewer) applications. In this scenario, the local IDP performs the identity management function for end users while ONE ID identifies the IDP system. Please see Communication Guidelines and Ontario Health Identity Federation for more information.

Identity Validation by ONE ID Process

To expedite the user onboarding process and reduce the administrative workload, it is recommended that users be validated internally within your own organization. If your organization's processes do not meet the requirements for AL2, identity validation must be

completed via review of acceptable evidence in a face-to-face meeting (in person or video conference) with an LRA.

Acceptable Evidence

Evidence must include at least one document from the Primary Identity Document list and one form of corroborating evidence. The Primary Identity Document serves to confirm the user's core identity information while the corroborating evidence may be an additional document and/or circumstantial evidence that serves to increase assurance that the Primary Document is genuine.

REVIEWING DOCUMENTARY EVIDENCE

At least one document presented must be on the Primary Identity Document list. Secondary documents may be reviewed in conjunction with a Primary Document as a form or corroboration. See Appendix A for a complete list of acceptable documents.

When reviewing Identity Documents, the following requirements apply:

- Document must be original, photocopies are not accepted.
- Document must be current, i.e. not expired.
- The document must contain a photo or be reviewed in conjunction with another approved document that contains a photo
- E.g., if birth certificate is used, secondary piece of evidence must include photo
- The document, on its own or combined with a second identity document, must confirm the individual's legal name and date of birth.

REVIEWING CONTEXTUAL EVIDENCE

The context of a registration can corroborate the identity of an individual when used in conjunction with a Primary Identity Document. The following contexts are considered acceptable to support the identity of a Registrant:

- **Prior Professional Relationship:** If the LRA has known the individual professionally for more than 12 months, they may rely on this relationship as a form of identity validation. Professional Relationship includes those with coworkers, colleagues, and patients.
- **Employment by the Sponsoring Organization:** Employment may be confirmed by reference to an employee directory or as advised by organization leadership.
- **Registration at Practice Location:** Meeting the Registrant and their medical practice location can serve to corroborate their identity. This form of evidence is only applicable for LRAs registering individuals outside of their own organization.

The means of supplemental identity validation used must be recorded in the ONE ID System.

PROFESSIONAL LICENSE VALIDATION

When presented, medical professional credentials qualify as a secondary form of documentary evidence of identity. If not presented, credentials may still serve as a form or corroborating evidence when validated by an LRA against an authoritative source. Professional License credentials may be inputted into the system during the identity validation process, self-registration, or any time after the ONE ID account has been created and set up.

The ONE ID System automatically validates credentials for Physicians, Nurses, and Dieticians (Refer to the *ONE ID Local Registration Authority User Guide* for details). To validate other credentials, refer to the issuing Regulatory College website to confirm that the registrant's identity aligns with their license number.

Capturing Identity Information

> It is recommended that you capture identity information in ONE ID as you conduct identity validation. In the event that you record identity information outside the system (e.g. on a registration form), such records should be destroyed or archived in accordance with your organization's document retention policies after being entered into ONE ID.

Within the ONE ID system, you must record the registrant's:

- Legal First and Last Names
- Preferred First and Last Names
- Date of Birth
- The Evidence presented to validate identity including the type and number of documentary evidence
- Healthcare Professional License Information

Capturing Account Information

Additional information regarding the registrant must be captured at the time of registration, including:

CONTACT INFORMATION

Contact Information (email and phone number) may be used by Ontario Health to alert users regarding changes to their account, help resolve technical issues with the account and/or in the event that the account is involved in a suspected security breach.

CHALLENGE QUESTIONS

During the registration and self-completion process, individuals are required to provide answers to five (5) challenge questions. These are questions to which only individuals know the answers and are collected for the purposes of verifying their identity via phone or internet, to safeguard the integrity of the system.

Individuals will be asked to provide answers to **two (2) Service Desk Challenge** questions collected for support purposes. Service Desk Challenge Questions may be asked when registrants call Ontario Health Service Centre (e.g., cannot reset their password online, forget their Login ID and password, or have lost their temporary password) to verify their identity.

Individuals will need to self-complete their registration process online in which they are required to select and answer **three (3) Online Challenge Questions**. These questions are used by the ONE ID system for self-recovery (e.g., Forgot Login ID, Forgot Password) and for knowledge-based authentication (KBA).

ENROLMENT INFORMATION

Enrolment information (e.g., roles and attributes) may need to be collected for select services. As this information may determine the registrant's level of access within a service, it must be provided or confirmed by the authorized sponsor.

Identity Validation for Previously Registered ONE ID Users

Users who have an existing ONE ID account have had their identity previously validated and do not need another validation for the purpose of enrolment. Other account modification requests may require identity validation as follows:

Modifying Identity Information

If there are legal changes that need to be made to the account (e.g., Legal name change), specific documentary evidence is needed to confirm the validity of the change. If it is a non-legal change (e.g., email, change in phone number), the user should be directed to modify their own account via self-management.

DOCUMENTARY EVIDENCE

The specific document that shows the legal change must be validated before modifying the required identity information in the account.

If modifications need to be made to the Users account, depending on the type of change (e.g. Legal name change), documentary evidence is needed and must be validated before making the required changes. Please refer to the section “Modifying ONE ID accounts” for more details.

Correcting Identity Information

Cases where identity information was previous captured incorrectly are distinct from changes to identity information, e.g., a typo in a legal name vs assuming a married name. Correcting errors in identity information can be based on previously reviewed documentary evidence and/or your professional relationship with the user. If neither of these are sufficient to confirm the correct information, you must review a piece of documentary evidence.

Modifying Challenge Information

Users that are locked out of their ONE ID account and are unable to authenticate over the phone may require LRA assistance to update their Service Desk Challenge Questions. To mitigate the risk of identity fraud, you must validate the requestor as follows:

ESTABLISHED PROFESSIONAL RELATIONSHIP

If you have a professional relationship with the user for at least 1 year, you may use this contextual evidence to make the required changes.

DOCUMENTARY EVIDENCE

The user’s identity information (legal name and birth) must be validated using the documentary evidence that matches what is listed in the account before modifying challenge information.

Missing Challenge Information

In some cases, previous ONE ID accounts may not have had Challenge Questions captured. After verifying the user’s identity (same process as above), add 2 service desk challenge questions on their behalf.

The user will call Service Desk at **1-866-250-1554** and be verified using the service desk challenge questions. The user will then be permitted to obtain a temporary password to reset their account and input their own Challenge Questions.

General Guidelines

This section provides high level guidance on how to perform your duties as an LRA and is intended to help you establish practices to support these duties when they do not already exist within your organization. You are encouraged to leverage all or your organization's internal polices, processes, tools, etc. where applicable. If you believe that these guidelines (or any of the content of this manual) conflicts with your organization's practices, please contact ONEIDRegistrationAgents@ontariohealth.ca

As part of the ongoing support and maintenance of ONE ID, you should periodically review how these practices are working for your organizations and refine as needed.

Information Management

You are responsible for communicating the information management practices outlined in this guide to registered individuals within your organization. Components of information management include:

- Information collection
- Information storage and retention

These practices are necessary to safeguard the privacy of personal information (PI) (including PHI) that is collected, transmitted, stored, or exchanged by and through the information infrastructure to ensure the privacy and security of that information.

If you have any questions or require further information about the collection described above, please contact the Ontario Health Chief Privacy Officer at:

Email: privacy@ontariohealth.ca

Phone: 1-877-280-8538

Mail: Chief Privacy Officer

525 University Avenue, 5th Floor

Toronto, ON M5G 2L3

Information collection

Information collected in the course of your duties as an LRA is necessary for the creation and/or maintenance of ONE ID accounts and enrolments and **must not be used for any other purpose**. You must advise users of this fact when collecting their information.

When collecting information, you must:

- Ensure the privacy the collection process, i.e., it is limited to you and the Registrant and relies on a secure channel
- Obtain it directly from the source (the registrant and/or your organization's records) and not via an intermediary
- Ensure the accuracy of the information you record as compared to the source

See Compliance and Assurance for more information on Privacy and Security Practices.

Information Storage and Retention

Any user registration information **must not be kept or recorded anywhere outside of the ONE ID system**. In the event that this information is captured outside of the system, these records should be properly retained and/or disposed of in accordance with your organization's Privacy, Security, and Data Retention policies.

Transient records (e.g., paper forms) used to support your organization's internal process **must be stored in a secure location** (e.g., locked file cabinet) until the information has been entered into the ONE ID System. Thereafter, these documents should be handled in accordance with your organization's Data Retention, Privacy, and Security Policies.

Incident Management

Incident management addresses what needs to be done in the event that an individual's Personal Information (PI) is compromised or used in a manner that is unrelated to registering or enrolling individuals into Ontario Health services.

Examples of incidents include but are not limited to:

- Personal Information is stolen or misplaced
- Personal Information is used to perpetrate identity theft
- Personal Information is used for purposes other than registration, such as updating an HR contact database

Reporting an incident

In the event of an actual or suspected privacy incident, please contact the Ontario Health Service Desk at **1-866-250-1554** immediately so that it will be actioned as soon as possible. Please ensure that you recount the incident in detail, which may include the time the incident occurred, and the parties involved. For more information on the practices for incident management, refer to **Compliance and Assurance**. You are responsible for ensuring your organization complies with these practices.

Communications and Training within the Organization

As an LRA, you will be interacting with different groups and are responsible for the following:

- **New LRAs**: Training and support for other LRAs within your organization.
- **Individuals and Registrants**: Ensuring that all registrants understand the Ontario Health Acceptable Use Policy and Notice of Collection.
- **Sponsors**: Understanding who the Sponsors and Authorized Representatives are
- **Staff within your organization**: Communicating how the registration and enrolment processes will work within your organization or care team.
- **ONE ID staff**: Communicating changes to delegates or users

Interacting with New LRAs

You are responsible for registering, training and monitoring the activities of new LRAs within your organization. This includes:

- Ensuring that the nomination has come from the Authorized Representative (**AR**).
- Submitting the LRA Nomination Form to ONEIDRegistrationAgents@ontariohealth.ca

NEW LRA TRAINING PLAN

The types of questions you may want to address as you develop the LRA training plan include:

- Has the LRA read and understood the LRA Procedures Manual?
- Do you want the new LRA to shadow an experienced LRA for a certain period? If so, for how long?
- How will you note that the LRA has been trained?
- How will you ensure that the LRA is fulfilling the duties and responsibilities of the position especially within the first few weeks, and provide feedback?

When enrolling new LRAs, direct them to the Registration Community to take the mandatory ONE ID LRA Training Module. You will be responsible for documenting the answers to these questions and communicating them within your organization and to Ontario Health if required (such as, in support of an audit), and for ensuring that your organization is in compliance. See Compliance and Assurance for more information.

As part of the ongoing support and maintenance, you may also want to revisit how the process is working for your organizations and refine as needed.

Interacting with Individuals and Registrants

When and how LRAs interact with users is heavily dependent on your organization's structure and request management protocols. Questions you may want to consider include:

- Which individuals/groups will require access?
- Does your organization have multiple ONE ID protected services? What is the overlap between the user groups?
- How high is the turnover in your user group(s)? How many registrations/revokes/suspends/reinstates will need to be processed on a monthly basis?

Identity confirmation is a key component of all interactions with users, not just registration. **Always confirm a registrant's identity before updating their account information or providing information regarding it.** If you previously registered or otherwise know the registrant, you may rely on this knowledge as confirmation of their identity. You may also, at your discretion, request to review an identity document to confirm their identity.

Interacting with Sponsors

How LRAs interact with Sponsors is heavily dependent on your organization's structure and request management protocols. At a minimum, all LRAs should be aware of who in their organization fulfills the Sponsor and Authorized Representative roles. More specific questions to consider include:

- Has a process been established for your organization as to how you will be notified of new sponsors?
- How will the list of sponsors be communicated amongst the LRAs within your organization; how will the list be updated?

- Will an email from a sponsor or memo be acceptable as proof of sponsorship?
- Is there an established authorization process that can/should be leveraged for ONE ID sponsorship?

You will be responsible for documenting the answers to these questions and communicating them within your organization, and to Ontario Health if required (such as, in support of an audit), and for ensuring that your organization is compliant. See Section X: Compliance and Assurance for more information.

Interacting with "Staff"

Depending on your organization, there may be other departments you can work with to ensure that the processes and policies that you are developing are in keeping with federal or provincial legislation and your organization's operations. For example, if your organization has a Human Resources division, you may want to exchange information when individuals have been hired or have left the organization.

Interacting with ONE ID

ONEIDRegistrationAgents@ontariohealth.ca should be your primary communication channel for ONE ID related matters, including submitting requests for action, reporting errors in the ONE ID system, and asking for guidance on process/policy interpretation.

ONEIDBusinessSupport@ontariohealth.ca is the appropriate communication channel regarding any changes to AR/ LRA delegates and user statuses, sponsorship attestation requests, and changes to ONE ID process/policies/systems.

Communications Plan

The types of questions you may want to address as you develop an effective communications plan for your organization include:

- Will you use posters or send emails to educate the organization about the framework and process?
- How will you communicate the process(es) the sponsor or applicants need to follow
- What information will be requested of them, why the information is required, and how the information will be used?
- How will you communicate changes to the processes?

Record Keeping

All LRAs are accountable for their own and other LRAs transactions within the organization. Upon request, the ONE ID Program can provide you with a report of registrants sponsored by your organization and transactions performed by the LRAs. However, it is recommended that you maintain your own records as a point of comparison.

The following are records to maintain by the organization's LRAs:

- Registrations performed
- Service enrolments
- Updates performed
- Sponsorship requests (electronic or hard copy) received

Do not keep any personal identity information other than the name of the person for whom the transaction was performed, the transaction date, and the transaction type.

Your internal request management tools/processes may already incorporate sufficient record keeping. If this is not the case, we recommend using the Registration and Enrolment Audit Log Template

Communication Guidelines

In the course of you fulfilling your responsibilities as an LRA, you will need to communicate with end users, Ontario Health, and other stakeholders. It is assumed that communication will be via email, though these guidelines can be applied to any communication method. Note that your organization's communication and privacy/security standards may provide additional guidance.

Privacy Considerations

Transmission of any PI via email is against Ontario Health's policy and will result in a security incident being raised. **Do not submit any PI about users via email, including Gender, Date of Birth, and Identity Document Information**. Registrants should be identified in email only by their name, Login ID, and Professional Designation number (if applicable).

General Guidelines

Consider the nature of the request when sending communications. Ontario Health will always make efforts to engage the appropriate support teams, but starting with the appropriate communication channel will ensure faster service. Specific guidelines for submitting ONE ID account management requests are provided below. Other communication can be directed as follows:

- Incident reporting and general inquiries regarding Ontario Health services should be directed to servicedesk@ontariohealth.ca or, for immediate assistance, you can call 1-866-250-1554 (eHealth help desk).
- For assistance with ONE ID processes, policies, or system, please email ONEIDRegistrationAgents@ontariohealth.ca.
- For inquiries regarding adopting a new Ontario Heath service, please go to https://ehealthontario.on.ca/en/health-care-professionals/digital-health-services and complete the appropriate webform.

Submitting ONE ID Requests to via Email

The ONE ID System is the primary method for executing all Registration, Enrolment, and Account Maintenance requests. However, requests related to select services cannot be processed directly in the online system and require the intervention of Ontario Health. In such cases, LRAs can submit requests via email.

Note: Submitting requests via email creates delays in the process and increases the risk of errors due to miscommunication. For these reasons, Ontario Health may reject email requests that could be completed using the ONE ID Online system.

Sender's Email

Email requests must clearly identify you as the LRA (either in the body of the email or your signature) and be sent from the email account entered in your ONE ID Account. Ensure that your contact information in ONE ID is up to date and correct.

Subject

The subject line of your email should indicate the type of request (Enroll / Suspend / Reinstate / Revoke), the relevant service, and the Login ID (FIRSTNAME.LASTNAME@ONEID.ON.CA) of the relevant user, e.g.: "HSI Enrolment Request for JOHN.SMITH@ONEID.ON.CA."

Request Statement

The body of your email should contain an explicit statement of the request being made, including:

- **Type of request** (Enroll/Suspend/Reinstate/Revoke Enrolment / role or Revoke user registration)
- **Login ID of the Registrant** (FIRSTNAME.LASTNAME@ONEID.ON.CA)
- **Service Enrolment** (Connecting Ontario, ONE Labs Clinician, etc.)
- **Relevant Role(s)** (As applicable per service)
- **Enrolment Attributes** (as applicable per service)
- **Expected Return Date** (only applicable for suspend requests)
- **Reason** (only applicable for revoke and suspend requests), select from:
    - The registrant no longer requires access to the service

- The registrant's level of assurance no longer meets the minimum required for the service
- The registrant is no longer associated with the sponsoring organization

Example email:

> Hi,
>
> As the LRA under the authority of Kingston Health Sciences Centre, please REVOKE the Connecting Ontario Enrolment from the account JOHN.SMITH@ONEID.ON.CA as they are no longer associated with the sponsoring organization.
>
> Thanks,

In lieu of including these details in the body of your email, you may instead complete one of the email enrolment form templates located at the Registration Community.

Sponsorship Assertion

The LRA must include an explicit statement of sponsorship, indicating that the request has received proper authorization, e.g. "This request has been authorized under (insert Sponsoring Organization name)."

The organization must be one for which the LRA has been authorized to act on behalf of and the individual sponsor must have appropriate authority therein.

Federated Authorization Request

Once IDs are setup for access at your organization, they need to be submitted to us at OneIDBusinessSupport@ontariohealth.ca by an LRA. Individual Federated Authorization Requests (requests for local rather than ONE ID accounts) should follow the same format as ONE ID Requests. Federated Authorization requests may be submitted in bulk using the request template. Email requests should include the following information:

- LRA Submitting request
- Organization the request is for; e.g West Parry Sound Health Centre
- Type of Request; Add or Revoke
- Environment e.g. PROD, PST

See Appendix C for more information on Federated Authorizations.

ONE ID Registration and Enrolment Process

This process details the steps required to Register and Enroll end users for access to ONE ID protected applications.

This process may be initiated as part of a broader service implementation process or independently.

Preconditions

- The ONE ID Organization Setup process has been completed for the organization and it is authorized to sponsor end users for access to the respective service(s).
- An LRA must be authorized by the sponsoring organization before registering and enrolling registrants.

Triggers

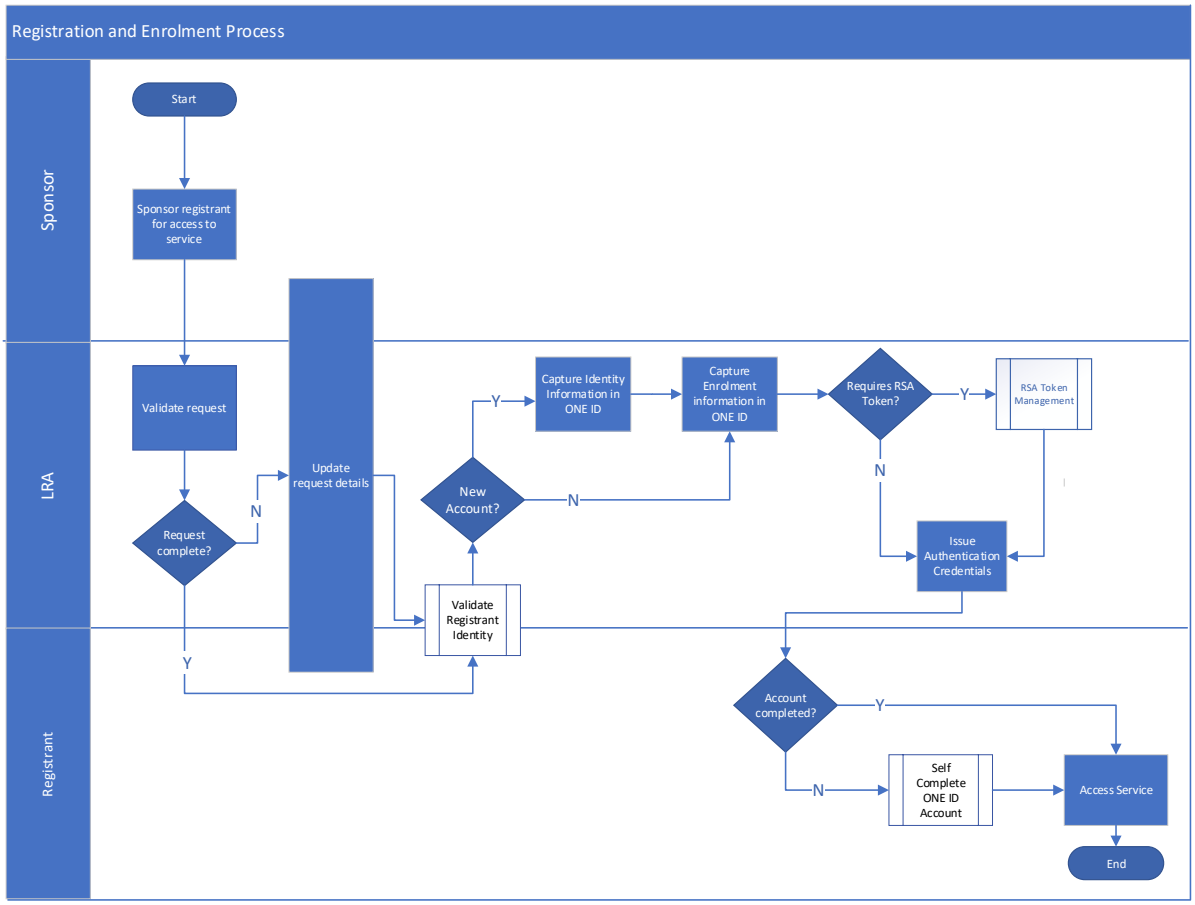
This process may be triggered in any of the following circumstances.

- A new staff member has joined the organization and requires access to services protected by ONE ID.
- A current staff member has assumed a new role and requires access to services protected by ONE ID.
- A new service has become available via ONE ID and must be enabled for end users.

Post-Conditions

- User's ONE ID account can be used to access requisite services.

Workflow



Process Steps

#	Name	Description	Role
1	Sponsor registrant for access to service	Sponsor validates that the Registrant meets the criteria for accessing the service and is authorized to do so under the authority of the Sponsor's organization. Note: Access criteria varies depending on service, refer to service-specific documentation for details.	Sponsor
2	Validate Request	Review the request to ensure that the organization's internal authorization process has been followed and	LRA

		that requisite data elements (e.g. service role) have been included. • If the request is incomplete or inaccurate, go to step 3. • If the request is complete/accurate, go to step 4. Note: Requisite data varies depending on type of service, refer to service documentation for details.	
3	Update Request Details	Coordinate with Sponsor and/or Registrant to complete the request.	Sponsor, LRA, Registrant
4	Validate registrant identity	Complete the identity validation process as prescribed by your organization and ONE ID. Process details may vary depending on circumstances, refer to Identity Validation for details.	LRA, Registrant
5	Capture identity information in ONE ID	Enter the registrant's identity information into the ONE ID system. Information requirements are determined by the identity validation method used. Refer to the ONE ID LRA User Guide and/or Express Registration Agent User Guide for details.	LRA
6	Capture Enrolment information in ONE ID	Add enrolments/roles as per sponsorship request. • If enrolment service requires RSA token, go to step 7 • If the service does not require an RSA token, go to step 8	LRA
7	RSA Token Management	Assign an RSA token to the registrant using the RSA console. Refer to RSA Console User Guide for Local Registration Authorities and Local Registration Authority User Guide.	LRA

		Refer to RSA Token Management Process for more details.	
8	Issue Authentication credentials	Provide authentication credentials to registrant. This includes the Login ID and (if applicable) temporary password/invitation code.	LRA
9	Self-complete ONE ID account	The Registrant completes an online process to activate their account. Refer to the ONE ID Registrant Reference Guide for further information on this functionality.	Registrant
10	Access service	The registrant verifies access to the respective service(s) by logging in for the first time.	Registrant

RSA Token Management Process

This process details the steps required when assigning, enabling/disabling/replacing/revoking tokens, and resetting token pins. Please see the RSA token User Guide and the Registration and Enrolment Process for more details.

If you must assign a token and do not have one available, please contact the Registration Agents.

Preconditions

- LRA has an RSA Token and has access to the RSA console.
- Registrant has a ONE ID account and has been sponsored and enrolled in a service that requires a token.

Triggers

This process may be triggered in any of the following circumstances.

- Registrant needs a token to access a service enrolment.
- Registrant's token needs to be enabled/disabled/replaced or needs a pin reset.
- The Registrant no longer requires an RSA Token

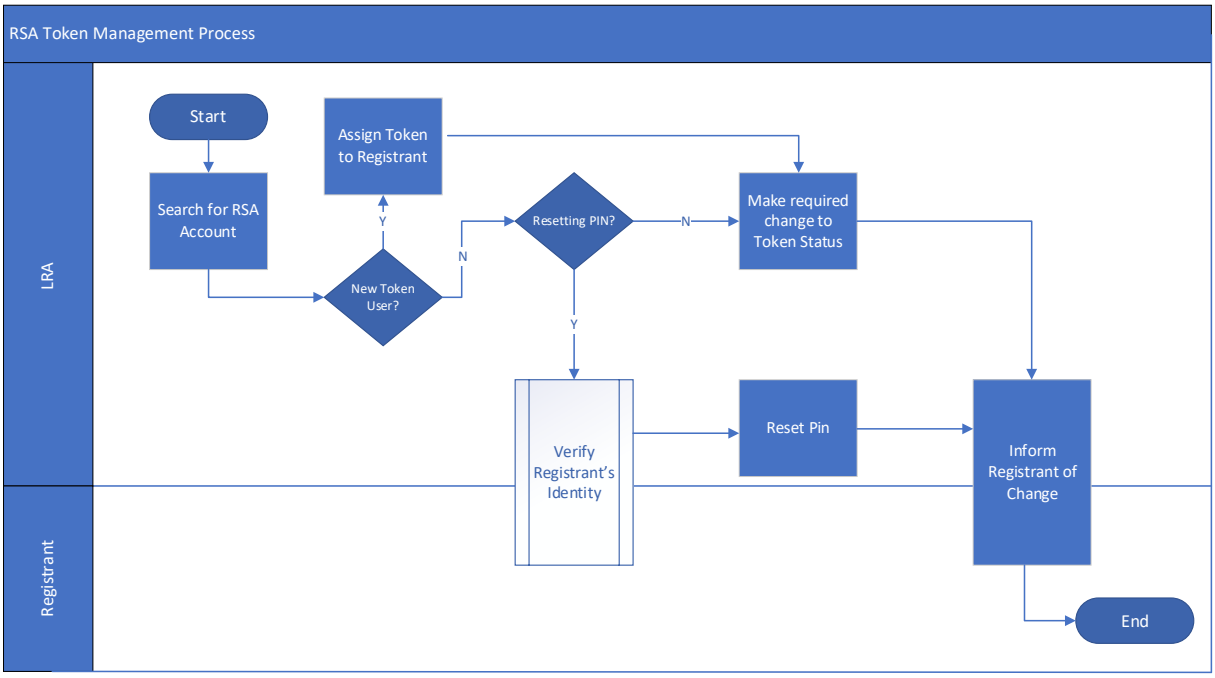
Post-Conditions

- Registrant has an active RSA Token and has access to the service enrolment.

Or

- The Registrant's RSA Token has been revoked

Workflow



Process Steps

#	Name	Description	Role
1	Search for RSA Account	Search the RSA Console for the user's ONE ID account. • If the user requires a new token to access a service, proceed to step 2. • If the user has an existing token that requires a PIN Reset, proceed to step 3. • If other changes are required, proceed to step 5.	LRA
2	Assign Token to Registrant	Assign Hardware Token you have on hand to the Registrant. Proceed to step 5 to enable the token.	LRA

		Note: For a user to set a new PIN, advise them to login to ONE ID and leave the PIN section blank. The system will then prompt them to create a new PIN.	
3	Verify Registrants identity	Verify the Registrant's identity using the ONE ID Challenge Questions or by reviewing the employee ID. For more details, refer to ONE ID Identity Validation.	LRA, Registrant
4	Reset Pin	To set new pin, advise user to login to ONE ID as per their standard instructions and leave the PIN section blank. For additional assistance, user may contact Ontario Health Service Desk.	LRA
5	Make Required Change to Token Status	Enable/Disable or replace token as required.	LRA
6	Inform Registrant of Change	Inform registrant that the request has been completed. This may involve an update of internal records.	LRA, Registrant

ONE ID Enrolment Management Process

This process details the steps required when suspending, reinstating, and revoking users' service enrolments to ONE ID protected applications. To add a service enrolment, please see the ONE ID Local Registration Authority User Guide and Registration and Enrolment Process for more details.

Suspending: Temporarily taking away access to a registrant's service enrolment. A registrant will still have access to their remaining services even if one of those services are suspended.

Reinstating: Granting a registrant access to an Ontario Health product or service that was previously accessible to the registrant.

Revoking: Permanently rescinding the registrant's access to the service. A registrant will still have access to their remaining services even if one of those services are revoked.

In the event that a Registrant is deceased or retired, please notify Ontario Health. Registration Agents will permanently revoke the registration and all associated service enrolments. Please see Revoking a Registration for more details.

Preconditions

- Suspend
    - The registrant is taking extended leave (e.g. maternity leave, sabbatical) or any other reason the sponsoring organization deems appropriate.
- Reinstate
    - The registrant is returning from extended leave or any other reason the sponsoring organization deems appropriate.
- Revoke
    - The registrant has left the organization or no longer requires access to the service.

Triggers

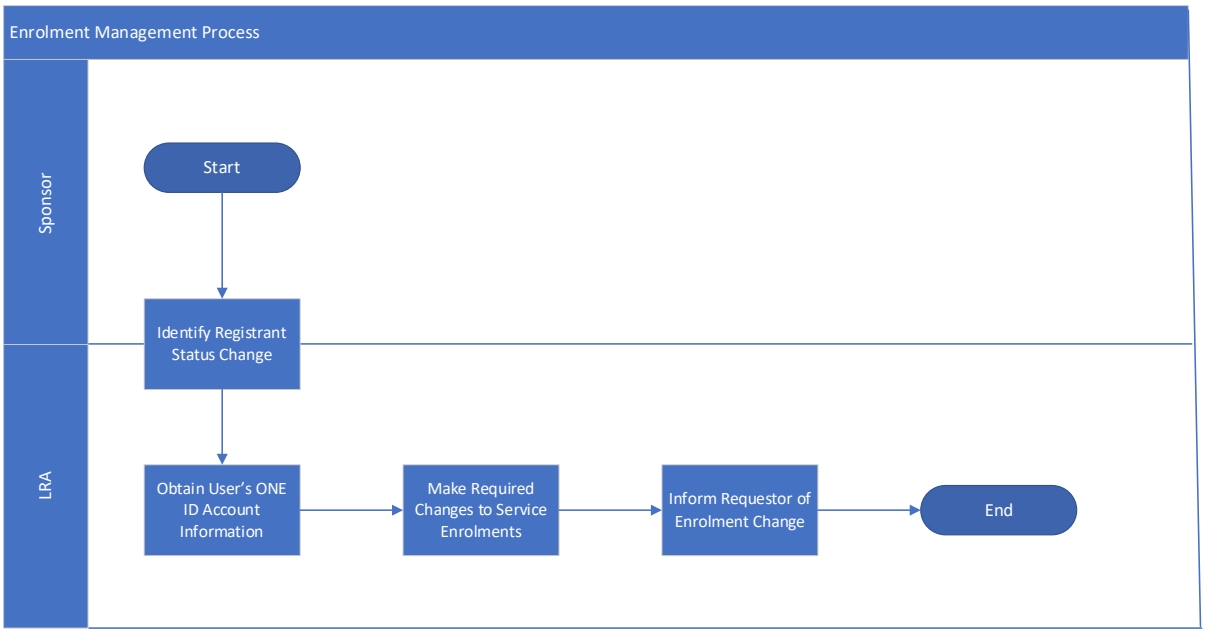
This process may be triggered in any of the following circumstances.

- The sponsor advises that the enrolment should be suspended/reinstated/revoked
- The LRA becomes aware of the employee status change through organizational processes.

Post-Conditions

- Changes to the user's service enrolments have been made.

Workflow



Process Steps

#	Name	Description	Role
1	Identify Registrant Status Change	The LRA is made aware of a change to the registrant's status (initiating or returning from leave, change of employment, etc.). This may be communicated by the Sponsor or raised via internal processes.	Sponsor LRA

2	Obtain User's ONE ID Account Information	Obtain ONE ID login from the Registrant, internal records, or searching ONE ID.	LRA
3	Make Required Changes to Service Enrolments	Suspend/reinstate/revoke the service enrolments in the user's ONE ID account as required For more detailed steps in the enrolment management process, refer to the ONE ID Local Registration Authority User Guide.	LRA
4	Inform Requestor of Enrolment Change	Inform requestor that the request has been completed. This may involve notification to the Sponsor and/or update of internal records	LRA

User Account Information Management Process

This process details the steps required when making changes to a user's ONE ID account information. These include changes to a registrant's legal name, gender, date of birth, and service desk challenge questions.

> Other changes to the user's account profile (contact information, password, etc.) can be self-completed by the registrant. Refer to the Registrant Reference Guide for more information.
>
> For any modifications or updates made to a registrant's account, the ONE ID System will

Preconditions

- The registrant's legal name, gender, or date of birth was entered incorrectly in the registration system or has been legally changed.
- The Registrant cannot remember the answers to their Service Desk Challenge Questions.

Triggers

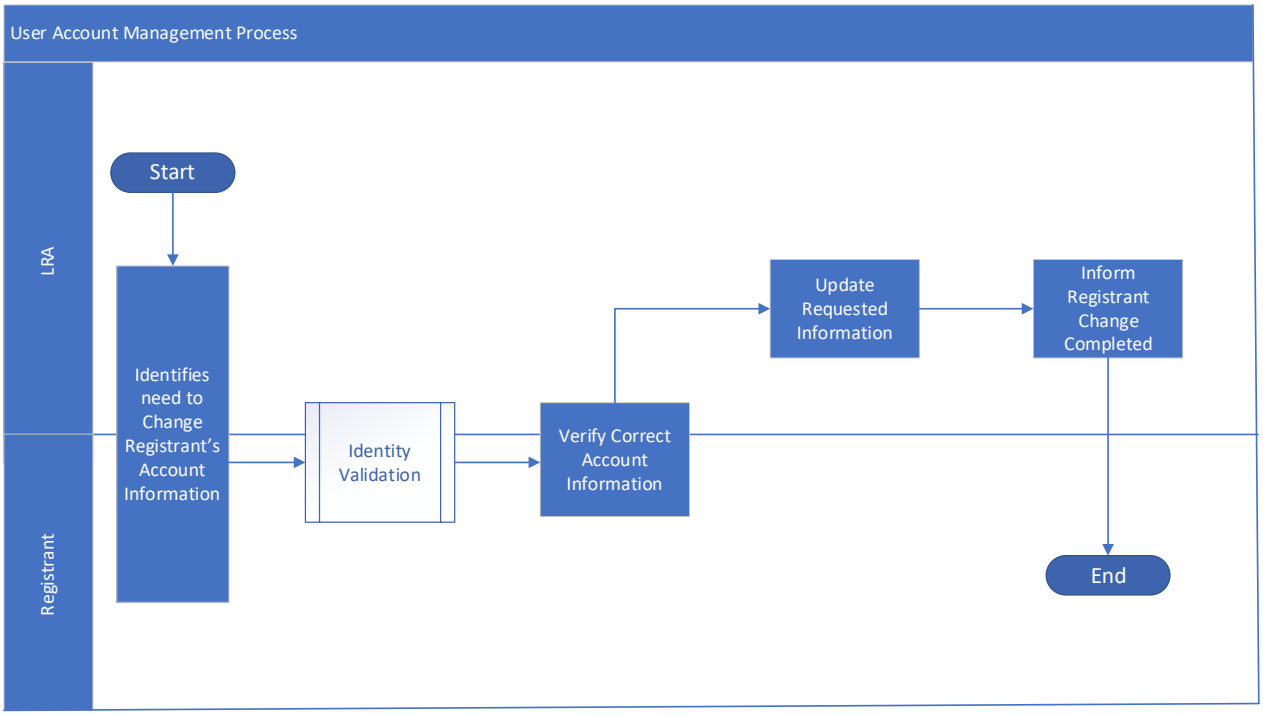
This process may be triggered in any of the following circumstances.

- A registrant advises the LRA of a change to their information.
- The LRA becomes aware of an error in the user's identity information.
- The Ontario Health Service Desk redirects a user to their LRA after their identity cannot be validated over the phone.

Post-Conditions

- Required changes to the user's ONE ID account information have been made.

Workflow



Process Steps

#	Name	Description	Role
1	Identifies need to Change Registrant's Account Information	LRA identifies a need to change Registrants account information. This is likely to be raised by the Registrant themselves, but not necessarily.	LRA, Registrant
2	Identity Validation	Confirm the registrant's identity. If the LRA has previously validated the registrant's identity and/or has an established (>1 year) working relationship with them, they may rely on this knowledge as confirmation of identity. To the discretion of the LRA, they may also ask to review a valid identity document from the registrant.	LRA, Registrant

		Please refer to Identity Validation for more details.	
3	Verify Correct Account Information	Verify the correct information to be entered into ONE ID. Verification requirements depend on the nature of the change, refer to Account Change Documentation Requirements (below) for details.	LRA, Registrant
4	Update Requested Information	Update the requested information change in the user's account. For more detailed steps in the user account management process, refer to the ONE ID Local Registration Authority User Guide.	LRA
65	Inform Registrant Change Completed	Inform Registrant that the request has been completed	LRA

Account Change Documentation Evidence Requirements

Types of Account Change		Evidence Requirements
Legal Change	Legally Changed Name	Primary/Secondary Evidence Document (e.g. Identity document with new name, change of name certificate)
Non-Legal Changes	Service Desk Challenge Questions	Identity not previously validated: • Review Primary/Secondary identity evidence documents Previously validated identity/professional relationship: • No evidence document needed
	Error Corrections	Identity not previously validated:

		• Review Primary/Secondary identity evidence documents Previously validated identity/professional relationship: • No evidence document needed
	Contact Information: (e.g. phone number, email)	No documents needed, Registrant can self-manage in account
	Preferred Name	No documents needed
	Gender	No documents needed

Compliance and Assurance

Ontario Health delegates the responsibilities for identity validation, registration and enrolment to the Sponsoring Organization's LRA(s). LRAs are responsible for adhering to the practices outlined in the LRA Procedures Manual and Ontario Health may request the LRA to assure they are complying with these practices.

Upon request, the LRA should be prepared to confirm the names of all Sponsors, LRAs, and authorized registrants within their organization and to provide documentation regarding their organization's established processes. Please refer to General Guidelines for more information.

A record of all requests must be stored and maintained for reference in the event of an audit. At minimum, records must identify:

- The Registrant
- The LRA
- The Sponsor
- The service(s) being enrolled/revoked

Such records can be maintained in your organization's request management system or an email archive.

Information Collection

The LRA is responsible for adhering to the Privacy and Security practices outlined in this guide regarding information collection and communicating the Privacy and Security practices, such as:

- Advising the individual what information will be requested of them, why the information is required, and how the information will be used.
- Adhering to privacy legislation (Freedom of Information and Protection of Privacy Act).

The LRA must NOT:

- Retain any of the identity documents presented during the registration process.
- Record PHI (such as the state of the individual's health).

- Use any of the PI provided by individuals for any other purpose than to register and enrol them in Ontario Health services.

For questions or concerns about the collection described above, please contact the Chief Privacy Officer at:

Email: privacy@ontariohealth.ca

Phone: 1-877-280-8538

Mail: Chief Privacy Officer

525 University Avenue, 5th Floor

Toronto, ON M5G 2L3

Information Storage and Retention

PI physically documented outside of the ONE ID System as part of the organization's internal process must be stored in a secure location (i.e. locked file cabinet) until the information has been entered into the ONE ID System.

Hereafter, these documents should be handled in accordance to your organization's Document Management, Privacy and Security Policies.

Incident Management

If the LRA or individuals within the organization suspects a security or privacy breach**, immediately report the incident to Ontario Health's Service Centre at 1-866-250-1554**.

Ontario Health will be responsible for investigating the incident and follow through its lifecycle. Security or privacy breaches includes:

- PI recorded during the registration process is stolen or misplaced.
- PI is stolen and used to perpetrate identity theft.
- Someone other than the LRA accesses registrant identity information.
- Information collected during the registration process is used for other purposes, such as updating an HR contact database.

Training of LRA's

As an LRA, you are responsible for ensuring that an LRA training plan has been established for new LRAs. Organizations should have their own internal processes related to onboarding and authorizing staff and how they connect to ONE ID.

- The LRA should be directed to the Registration Authority Community LRA Training section to complete ONE ID LRA Online Training.
- Have the LRA read the documentation regarding the processes around registration, especially those regarding privacy and security. All relevant documentation can be found on the ONE ID Registration Community site.
- Have the LRA shadow an experienced LRA through a few user registrations.
- Allow yourself some time to review the registrations and enrolments processed by the LRA within the first couple of weeks to ensure that the LRA is fulfilling the duties and responsibilities of the position and vis-versa.

Auditing of LRAs

All LRAs are responsible for tracking their own activities within their organization and ensuring they are in compliance with the LRA Procedures Manual.

> It is recommended that the Authorized Representative conduct an internal audit of the LRAs on a yearly basis to ensure their continued compliance.
>
> Ontario Health may request proof of compliance to the procedures and practices outlined in this document.

For auditing purposes, the Authorized Representative may be required to provide evidence that LRAs are trained and complying with the processes defined in this document for ONE ID Registrations and Service Enrolments.

An LRA may be asked to show compliance with the Privacy and Security practices outlined in this procedures guide regarding:

- Information collection
- Information storage and retention
- Incident management

Verifying Registrant Information

Ontario Health may request the assistance of the LRA to confirm the identity of existing registrants in ONE ID due to:

- A Security Incident
- An apparent duplicate account
- Any account information that appears to be incorrect

Ontario Health

Appendix A – Identity Documents

Identity documents are the standard means of validating identity during the ONE ID registration and service enrolment of individuals. They are also used to validate any changes to registration information (such as legal name, date of birth and gender) after the applicant has been registered.

During identity validation, perform a visual inspection of the document for signs of tampering or forgery. If the document appears to be altered, the LRA may reject at their own discretion.

These lists are available as a separate document on the Registration Community and may be distributed to applicants to help prepare them for the registration and enrolment process.

Primary Identity Documents

Acceptable Primary Identity Documents	
1	Birth Certificate issued by a Canadian Province or Territory
2	Canadian Certificate of Birth Abroad
3	Canadian Certificate of Indian or Metis Status
4	Canadian Permanent Resident Card
5	Certificate of Canadian Citizenship (paper document or plastic card, excluding commemorative issue)
6	Certification of Naturalization (paper document or plastic card, excluding commemorative issue)
7	Citizenship Identification Card issued by a foreign jurisdiction where these exist (e.g., Mexico, Europe)
8	Confirmation of Permanent Resident (IMM 5292)
9	CANPASS (A Remote Area Border Crossing permit allowing the bearer to cross into Canada at certain remote areas without reporting to a port of entry as long as imported goods are declared.)
10	Nexus (A cross-border express pass available to low-risk individuals who have passed a stringent Canadian and American security check, including a fingerprint biometric, photograph, and personal interview with immigration officials. In order to maintain this pass, the individual must reapply every two years.)
11	Firearm Registration License
12	Permanent Resident Card (i.e., Maple Leaf Card)

13	Driver's License (including graduated driver's license)
14	Canadian Passport (currently valid)
15	A valid Passport issued by a foreign jurisdiction
16	Statement of Live Birth from Canadian Province (Certified Copy)
17	Immigration Canada – Refugee Claimant ID Document
18	Ontario Photo Card

Secondary Identity Documents

Acceptable Secondary Identity Documents	
1	Any document listed as an Acceptable Primary Identity Document except for the Primary Identity Document being recorded in the Registration Management System.
2	Old Age Security Card
3	Certificate issued by a government ministry or agency (e.g., Marriage, Divorce, Adoption)
4	Canadian Convention Refugee Determination Division Letter
5	Canadian Employment Authorization
6	Canadian Minister's Permit
7	Canadian Immigrant Visa Card
8	Canadian Student Authorization
9	Record of Landing (IMM 1000)
10	Document showing the registration of a legal change of name accompanied by evidence of use of prior name for the preceding 12 months.
11	Current Registration Document from the College of a Health Profession under the Regulated Health Professions Act, 1991. (Audiology and Speech-Language Pathology, Chiropody and Podiatry, Chiropractic, Dental Hygiene, Dental Technology, Dentistry, Denturism, Dietetics, Homeopathy, Kinesiology, Massage Therapy, Medical Laboratory Technology, Medical Radiation Technology, Medicine, Midwifery, Naturopaths, Nursing, Occupational Therapy, Opticianry, Optometry, Pharmacy, Physiotherapy, Psychology, and Psychotherapy, Respiratory Therapy and Traditional Chinese Medicine and Acupuncture)
12	Current Professional Association License/Membership Card (for any Regulated Health Profession, including the following: Association of Ontario Midwives, Denturist Association of Ontario, Nurse Practitioner Association of Ontario, Ontario Association of Medical Radiation Technologists, Ontario Association of Naturopathic Doctors, Ontario Association of Orthodontists, Ontario Association of Speech Language Pathologists and Audiologists, Ontario Chiropractic Association, Ontario Dental Association, Ontario Medical Association, Ontario Nurses Association, Ontario Opticians Association, Ontario Pharmacists" Association, Ontario Physiotherapy Association, Ontario Podiatric Medical Association, Ontario Society of Chiropodists, Ontario Society of Medical Technologists, Registered Nurses Association of Ontario, Registered Practical Nurses Association of Ontario, or Respiratory Therapy Society of Ontario)

13	Federal, Provincial, or Municipal Employee Card
14	Current Employee Identification or Identifier from a Sponsoring Organization
15	Union Card
16	Other Federal ID Card, including Military
17	Ontario Ministry of Natural Resources Outdoors Card
18	Judicial ID Card
20	BYID Card (Formerly Age of Majority Card)
21	CNIB Photo Registration Card
22	Canadian Police Force Identification Card
23	Identification Card issued under the *Blind Persons Rights Act*

Appendix B – LRA Acknowledgement

This form is intended for your review only. Acknowledgement is made via the ONE ID Online System.

Form of Local Registration Authority Acknowledgement

I, _____, understand that I will be registered in Ontario Health ("**Ontario Health**") ONE ID and appointed as a Local Registration Authority ("**LRA**"). Local Registration Authority means an individual that has been delegated responsibility by a Client Organization or the Ontario Health Certificate Authority for the performance of tasks associated with identifying, authenticating, registering, enrolling, and managing registrants who are within the scope of his or her authority as delegated by a Client Organization or the Ontario Health Certificate Authority. "**Certificate Authority**" or "**CA**" means an individual or group of individuals designated by Ontario Health that are responsible for the registration, service enrolment, and authentication services provided by Ontario Health to clients.

As an LRA I will be obligated to:

1. Read and adhere to Ontario Health's LRA Procedures Manual as amended from time to time.

2. Complete such training, including security and privacy training, related to Ontario Health's registration and appointment processes and technologies used for authentication as Ontario Health may reasonably require and provide from time to time.

3. Take reasonable steps to keep my Authentication Credentials provided by Ontario Health secure and confidential at all times. "**Authentication Credentials**" means any credential including but not limited to a user identification, password, token, or any combination of these, that is issued by Ontario Health to an registrants to allow the authentication of the registrant's identity to a system or application. I understand that I am responsible for any unauthorized or inappropriate use of my Authentication Credentials. Should I suspect or become aware that my Authentication Credentials have been compromised, or unauthorized access has been made of any computer terminal or other device connected to Ontario Health's infrastructure, I will immediately notify Ontario Health by calling the support number provided by Ontario

Health in the LRA Procedures Manual or by any other method set out in LRA Procedures Manual.

4. Read and abide by Ontario Health's Acceptable Use Policy, as amended from time to time. A copy of Ontario Health's current Acceptable Use Policy can be found at www.ehealthontario.on.ca.

5. Not exceed the scope of authority delegated to me by Ontario Health including but not limited to registering and enrolling only individuals, (as defined in the LRA Procedures Manual) and Computer Applications (as defined in the LRA Procedures Manual) that have been sponsored and the identity of the individual or validity of the Computer Application, as the case may be, has been verified as set out in the LRA Procedures Manual.

6. Obtain any necessary consent required before collecting, using, or disclosing personal information as set out in the LRA Procedures Manual.

7. Safeguard confidential and personal information collected or received by me in connection with my duties as an LRA and meet privacy requirements as set out in the LRA Procedures Manual.

8. Perform my duties as an LRA fully, responsibly, and diligently, in a professional and competent manner.

9. Immediately notify a Local Registration Authority within my organization or Ontario Health when the organization identified below no longer requires me to act as an LRA or I no longer wish to act as an LRA for any reason.

I understand that:

- My appointment as an LRA is not approved unless Ontario Health provides me with Authentication
- Credentials signifying Ontario Health's acceptance of me as an LRA;
- Ontario Health may suspend me from acting as an LRA or terminate my designation as an LRA for any reason, including but not limited to, my failure to comply with the obligations set out above;
- My actions as an LRA may be subject to an audit from time to time to ensure compliance with the obligations set out above; and

- My appointment as an LRA is subject to the obligations set out above and by signing below I acknowledge that I have read and understand these obligations and commit to adhere to same.

Appendix C – Ontario Health Identity Federation

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.

> Note: 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.

ENTITLEMENT PREREQUISITES

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.

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.

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.

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.