

eHealth Ontario

ONE ID Registering Organizations

Local Registration Authority User Guide

Version: 3.0

Copyright Notice

Copyright © 2013, eHealth Ontario

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Table of Contents

1.0	About This Document	1
1.1	Purpose.....	1
1.2	Scope.....	1
1.3	Audience.....	1
1.4	Approach.....	1
1.5	Reference Material.....	1
2.0	Introduction	2
2.1	ONE® ID Overview.....	2
2.2	ONE® ID Registering Organizations.....	2
3.0	Registration Process Overview	3
3.1	Sponsorship.....	3
3.2	Identity Validation.....	3
3.3	Record Applicant Information.....	3
3.4	Enrolment.....	4
3.5	Credential Distribution.....	4
3.5.1	Temporary Passwords – In Person Distribution.....	4
3.5.2	Temporary Passwords – Distribution via eHealth Ontario Service Desk.....	4
3.5.3	RSA Tokens – In Person Distribution.....	4
4.0	Identity Validation via Client Managed Registration Process	5
4.1	Understand the Organization’s Registration Process.....	5
4.1.1	Process Details.....	5
4.1.2	Unique Identifier.....	5
4.2	Validate Applicant’s Relationship with Organization.....	5
4.3	Collect Applicant Information.....	6
4.3.1	Confirm the Applicant’s Identity Before Collecting Personal Information.....	6
4.3.2	Applicant Information May be Taken at Face Value.....	7
5.0	ONE® ID System for Registering Organizations	8
5.1	Add Employee Identifier.....	8
5.2	Documents Tab.....	8

1.0 About This Document

1.1 Purpose

This document provides step-by-step procedures for Local Registration Authorities (LRAs) to leverage their own organization's managed registrations process as a source of identity validation for its employees.

1.2 Scope

This document addresses the changes roles, responsibilities and functions of LRAs who manage the registration and service enrolment process within Registering Organizations as compared to those described in the Local Registration Authority Procedures Manual.

1.3 Audience

This document is intended for LRAs who have been given the authority to perform these tasks on behalf of eHealth Ontario and their organizations. It is assumed that the audience in question has an intermediate level of understanding of the concepts surrounding registration, service enrolment, and change management and has thoroughly reviewed the Local Registration Authority Procedures Manual.

1.4 Approach

This document outlines detailed procedures for the various functions that are unique to LRAs operating within a Registering Organization, including a brief description of the function and why it is required, followed by detailed steps on how to perform the function.

1.5 Reference Material

Detailed information on the various functions that can be performed by all LRAs is described in the Local Registration Authority Procedures Manual.

Detailed information on the functionality of the ONE® ID System available to all LRAs is described in the ONE® ID Local Registration Authority User Guide.

2.0 Introduction

2.1 ONE[®] ID Overview

ONE[®] ID is a set of systems and business processes that provides trusted and secure access to eHealth applications and services to healthcare providers registered with eHealth Ontario.

ONE[®] ID assigns an Identity Assurance Level to each user account corresponding to the rigour taken in validating that user's "real world" identity. Establishing Identity Assurance increases security and trust during the transmission of Personal Health Information.

A minimum of Assurance Level Two (AL2) is required for an account to be granted access to PHI. ONE[®] ID meets the requirement through a robust registration process requiring an in person meeting between perspective users and an LRA in which their identity is validated through the review of identity documents and contextual evidence.

2.2 ONE[®] ID Registering Organizations

ONE[®] ID also supports the use of other registration processes as a source of identity validation where they meet the minimum requirements for AL2. Use of an organization's own managed registration process prevents unnecessary duplication of effort, reducing the administrative overhead required for registration and providing a better user experience.

If an organization wishes to leverage its own registration process to validate the identity of ONE[®] ID users, that process must first be assessed and approved by the ONE[®] ID Program as meeting the requirements for AL2. This guide is intended for LRAs working at organizations that have already completed this approval process and are an authorized "Registering Organization" for ONE[®] ID.

If your organization is interested in becoming a Registering Organization, please contact the ONE[®] ID Business Support Team at ONEIDBusinessSupport@ehealthontario.on.ca.

3.0 Registration Process Overview

Within a Registering Organization, the high level ONE® ID Registration and Enrolment process remains unchanged, That is:

Sponsorship

- Requests must be authorized by an appropriate sponsor before the process can proceed.
- You may engage the sponsor directly to approve the request or redirect the user

Identity Validation

- The applicant's identity must be validated via an approved method
- You may combine multiple validation methods in order to establish identity to the required level of assurance.

Record Applicant Information

- The applicant's core identity information must be entered into ONE® ID
- Information about the identity validation method must also be recorded in ONE® ID at the time of account creation

Enrolment

- The new account will need to be granted access via the ONE® ID System
- Alternatively, access can be requested via email

Credential Distribution / Completion

- The applicant's credential must be distributed to them in a secure manner and they must complete the process to activate it

The detailed process for each step is unchanged from that described in the LRA Procedures Manual except as described in this section.

3.1 Sponsorship

In addition to user authorization, you may also rely on Sponsorship as a source of truth regarding the applicant's relationship with the Registering Organization, i.e. a Sponsor *may* confirm whether or not a user is an employee of the organization. Refer to [Section 4](#) for more details.

3.2 Identity Validation

While identity validation should be significantly faster and easier when relying on a previously executed registration process, LRAs are still required to perform due diligence in validating the applicant's identity. Refer to [Section 4](#) for detailed process steps for relying on an organization's registration process for identity validation.

3.3 Record Applicant Information

In lieu of identity documents, the applicant's Unique Identified assigned by the Registering Organization (e.g. Employee #) must be entered into the ONE® ID System. Refer to [Section 4](#) for specific details regarding system functionality.

All other applicant information must be recorded in the ONE® ID System as per the Local Registration Agent Procedures Manual and the ONE® ID Local Registration Agent User Guide.

3.4 Enrolment

There are no special considerations when enrolling users within Registering Organizations. Standard processes outline in the Local Registration Authority Procedures manual should be followed.

3.5 Credential Distribution

While a face-to-face meeting is not required for the registration process, user credentials must be distributed directly from the LRA to the User in a secure manner.

3.5.1 Temporary Passwords – In Person Distribution

Temporary passwords should never be distributed via email. When distributing temporary passwords in person to users, you must first confirm their identity. If you know the user through an established relationship, you may rely on this knowledge as confirmation of identity. Otherwise, you must review a photo ID document prior to distributing credentials.

3.5.2 Temporary Passwords – Distribution via eHealth Ontario Service Desk

If it is not possible to distribute the temporary password in person, users should be given their ONE® ID Username and asked to call the eHealth Ontario Service Desk to obtain a temporary password.

3.5.3 RSA Tokens – In Person Distribution

Only LRAs and the user to whom a token is assigned are authorized to handle RSA Tokens. For this reason, RSA tokens should be distributed in person and not via inter-office mail.

4.0 Identity Validation via Client Managed Registration Process

While the ONE® ID Team has previously validated that your organization's internal registration process is sufficient for validating the identity of Users to Assurance Level Two, it is still your responsibility as an LRA to verify that the individual you are registering has previously undergone this process. How this is accomplished may vary between organizations.

4.1 Understand the Organization's Registration Process

LRAs must be familiar with their organization's registration process. Even if they are not directly involved in its execution, the LRAs should be sufficiently familiar with the process to recognize when it has or has not been completed. eHealth Ontario is unable to provide training on an organization's internal processes. It is the responsibility of LRAs and their respective organizations to ensure that the requisite training is provided.

4.1.1 Process Details

In particular, LRAs should be aware of:

- **When the process is executed.** Are employee identities validated as part of the hiring process? On their first day? Some other time?
- **Any exceptions to the process.** Are all employees required to undergo the process or just Full Time Staff? What about temporary or contract workers? Co-op students?
- **How process completion can be validated.** If there are exceptions to the process, how are the indicated (e.g. different Employee # format for temp staff)? This requirement may impact what means the LRA must rely on to validate the Applicant's relationship with the Registering Organization.

4.1.2 Unique Identifier

The Applicant's Unique Identifier is a unique number, string, or code which identifies them in the Registering Organization's Registration System. It is most commonly an Employee Number assigned by the organization but it may also be the applicant's license number if they are a member of a Regulated Health Professional College (e.g. a doctor with hospital privileges).

Whether the Identifier is an arbitrary code or a license number, what is required is that it correspond to the applicant's identity record captured in the Registration System. LRAs should be aware of what types of numbers may be used by applicants within their organization and which of them (if any) may constitute an exception to their organization's identity validation process.

4.2 Validate Applicant's Relationship with Organization

Depending on the size of the organization and the nature of its registration process, the means of confirmation an LRA relies on may vary. LRAs must be mindful of any exceptions to their organization's registration process and ensure that the means they rely on can account for them. Acceptable means include:

Staff Directory – Where available, LRAs may rely on their organization's directory to confirm that an applicant is affiliated with the registering organization.

Employee ID Badge – A Photo ID Badge issued by the registering organization presented by the applicant may be accepted as confirmation of employment.

Professional Relationship – LRAs who have an established working relationship with the applicant may rely on their own knowledge as confirmation that they are affiliated the organization.

Sponsorship – Where applicable, Sponsors may serve as a source of truth regarding an applicant's relationship with a sponsoring organization. In such cases, sponsorship requests should contain not only an explicit statement authorizing the applicant for access, but one confirming the applicant's relationship to the organization. LRAs must be diligent in ensuring that the Sponsor's role within the organization makes them such a source of truth, e.g. they are the applicant's manager.

Authoritative Confirmation – There may be other authoritative sources of confirmation besides the Sponsor (e.g. HR Department). Such sources should be known to the LRA and consulted as necessary.

If you are unable to confirm an applicant's relationship with the registering organization through any combination of the above means, you should rely on the standard ONE[®] ID Identity Validation Process described in the LRA Procedures Manual.

4.3 Collect Applicant Information

With the exception of identity documents, all applicant information described the LRA Procedures Manual remains mandatory. However, the LRA need not review any documentation to confirm the applicant's core identity information. The applicant's information may be taken at face value once their relationship with the registering organization has been confirmed.

The following special considerations apply when collecting applicant information within registering organizations:

4.3.1 Confirm the Applicant's Identity Before Collecting Personal Information

While the applicant may have already undergone the organization's registration process, the LRA must still perform due diligence to confirm that the individual they are dealing with is the same one who was registered. This means:

- **Relying on company directories for user contact information.** If personal information is to be gathered via phone (including date of birth, challenge questions, etc.), it must be by an outbound call from the LRA to the applicant at the number in the company directory. The email address in a company directory may be relied on to book an in person meeting, but **personal information should never be exchanged via email.**
- **Recognizing the Applicant.** If the LRA has an established relationship with the Applicant, they may rely on visual (in person meeting) or verbal (phone call within above criteria) recognition as confirmation of identity.
- **Reviewing Photo ID for unknown Applicants.** When registering an Applicant they do not know, LRAs should request to review a photo identity document to confirm that they are the same individual who was sponsored. The purpose of this validation is to

establish the Applicant's identity to the satisfaction of the LRA, not to register the Applicant in ONE® ID.

4.3.2 Applicant Information May be Taken at Face Value

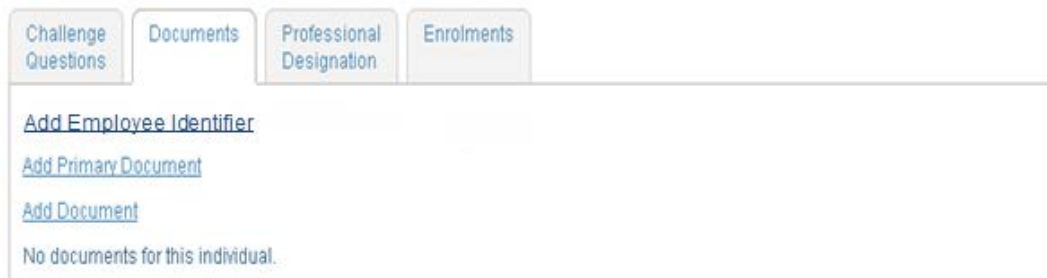
You may obtain information directly from the applicant without needing to review corroborating documentation. This includes both their Core Identity Information and their Unique Identifier. It is necessary that you validate the applicant's relationship with the registering organization, not that you validate the identifier that organization assigned.

5.0 ONE® ID System for Registering Organizations

Registration and Enrolment in the ONE® ID System follows the same basic workflow as when relying on standard ONE® ID Identity Validation. The difference is that the Employee Identifier may be entered in lieu of Primary and Secondary Identity Documents. All other aspects of the process remain the same; refer to Section 4.0 of the ONE® ID Local Registration Authority User Guide for details.

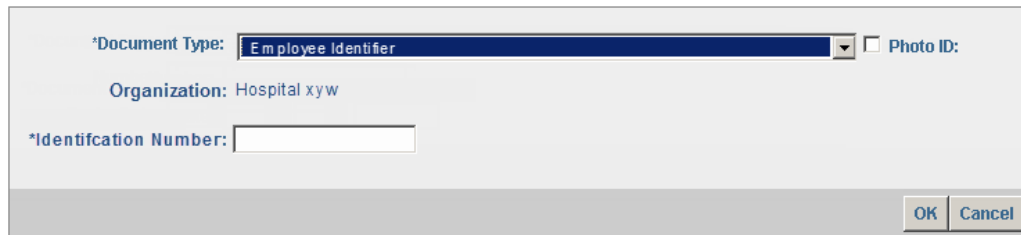
5.1 Add Employee Identifier

The following steps describe the process for adding the registrant’s Employee Identifier to their account.



1. On the **Documents** tab, click **Add Employee Identifier**.

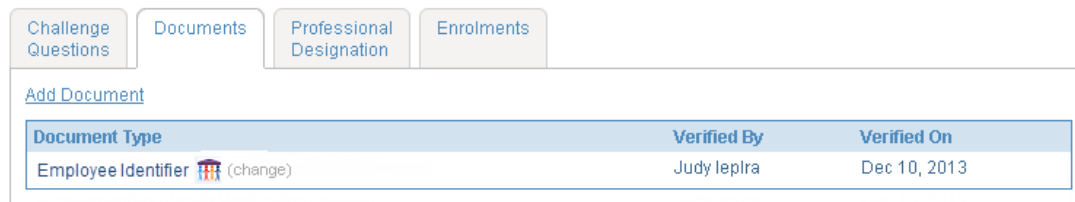
Identity Document



2. The **Identity Document** screen opens with the **Document Type** “**Employee Identifier**” selected. The **Registering Organization Name** is also displayed.
3. Enter the **Identification Number**.
4. Click **OK**.

5.2 Documents Tab

Once added the **Document Type** “**Employee Identifier**” is displayed on the **Documents** tab.



This entry, on its own, is sufficient to grant the user AL2. There is no need to add additional documents.