ONE® ID

Identity Assurance Standard

Ontario
eHealth Ontario

Document Control

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

Table of Contents

1.0 Description

The ONE®ID Program at eHealth Ontario (the "Agency") provides a Registration and Authentication service that facilitates Registrants' access to Healthcare Applications. These Registration and Authentication processes must attain to one of three defined Levels of Assurance, each with requirements that are based on the sensitivity level of the information being accessed.

2.0 Purpose

This Standard sets out the Levels of Assurance as defined by the Agency and the Registration requirements corresponding to each Level of Assurance.

3.0 Scope of Application

This Standard applies where a Level of Assurance needs to be assigned to a Registrant or when a Level of Assurance is specified for accessing a Healthcare Application.

3.1 Link to *ONE® ID Policy*

This Standard is incorporated by reference into the Agency's *ONE® ID Policy*.

4.0 Responsibilities

4.1 Approval

4.1.1 Authority

This Standard is issued under the authority of the Senior Director, Integrated Solutions & Services.

4.1.2 Revision, Review and Approval

This Standard follows the Agency's coordinated method for the revision, review and approval of Agency policies and standards.

4.1.3 Effective Date

This Standard is effective on the date of its publication, and on the date(s) set as it may be amended from time to time.

4.2 Administration and Interpretation

4.2.1 Responsibility

The Senior Director, Integrated Solutions & Services, is responsible for the administration and interpretation of this Standard.

4.2.2 Interpretation

This Standard shall be interpreted in accordance with the provisions of the *ONE® ID Policy*.

4.2.3 Exceptions and Waivers

The Senior Director, Integrated Solutions & Services, is responsible for making all decisions regarding Clients' requests for exceptions or waivers to the requirements in this Standard.

Any Client who seeks an exemption from the requirements in this Standard shall submit a written application to the Agency, which shall include reason(s) for the request. The Agency shall review all applications and determine whether a waiver may be granted on a case-by-case basis.

5.0 Levels of Assurance

5.1 General

A description of the three Levels of Assurance assigned by ONE® ID to individual Registrants is set out in the *ONE® ID Policy*.

5.2 Selecting the Level of Assurance

Application Owners shall determine the minimum Level of Assurance required for access to their Healthcare Applications. This determination shall take place in collaboration and, where required, negotiations with the ONE®ID Program.

5.2.1 ONE®ID Guidelines

When determining the minimum Level of Assurance required for access to their Healthcare Applications, Application Owners shall consider their business requirements, as well as the applicability and appropriateness of the definitions and requirements of the different Levels of Assurance as set out in the *ONE® ID Policy*.

5.3 Minimum Level of Assurance

5.3.1 General

To obtain access to a Healthcare Application, an individual's identity shall be validated by a Registration process whose rigour attains to the Level of Assurance required for access to that Healthcare Application. This Level of Assurance shall then become associated with the individual's identity (e.g. user ID) in the ONE®ID system.

5.3.2 Multiple enrolments

Before gaining access to certain Healthcare Applications, a Registrant may need to be enrolled in another Healthcare Application. For example, a Registrant who is enrolled in the Drug Profile Viewer application would also need to be enrolled in the eHealthOntario.ca portal. Where a Registrant is being enrolled into multiple Healthcare Applications, his/her Level of Assurance must be equal to or greater than the highest Level of Assurance required by the Healthcare Applications in which he/she is being enrolled.

5.3.3 Assigning a Level of Assurance

Individuals must be assigned a Level of Assurance when they are being Registered into the ONE ®ID service.

The real-world identity of a potential Registrant must be validated by a RA or LRA. Once validated, the RA / LRA shall establish a unique electronic identity (e.g. user ID) for the individual, which shall be associated with an assigned Level of Assurance.

Note: In accordance with the *ONE® ID Policy*, a Health Card number from any province, including Ontario, must not be accepted to validate the identity of an individual Registering in Healthcare Applications, including the ONE®ID service.

5.4 Registrar's Level of Assurance

A registrar (e.g., RA or LRA) must have an AL2 or higher to Register individuals at an AL2 or higher. A registrar may not Register an individual at a Level of Assurance that is higher than his/her own Level of Assurance, regardless of the means used to validate identity.

6.0 ONE®ID Registration

6.1 Registration Requirements

ONE® ID's general Registration requirements (as they correspond to each Level of Assurance) are set out below.

6.1.1 AL1

a. The Registrant must be sponsored.

b. The Registrant must be personally involved in the Registration process.

c. The Registrant shall not be required to provide any identification evidence and any supplied identity information may be taken at face value.

d. The Registrant must be 14 years of age or older.

6.1.2 AL2 or AL3

a. The Registrant must be sponsored.

b. The Registrant must be personally involved in the Registration process.

c. The Registrant's identity must be validated through an Agency-approved method, see section 7.0.

d. Relevant details of the identity validation shall be recorded.

e. The Registrant must be 16 years of age or older.

7.0 ONE®ID Registration Methods

Where an AL2 or AL3 is required for accessing a Healthcare Application, the following are the methods that may be used to validate identity / Register an individual for a ONE®ID account:

Primary Identity Check		Secondary Identity Check	Actioner
Primary document (section 7.3 and Appendix B) **OR**	**AND**	**Secondary document** (section 7.3 and Appendix B); **OR**	RA, LRA, Notary Public
		Registration number with the College of a regulated health profession (section 7.1.1) **OR**	RA, LRA
		Practice location (supplementary verification, section 7.2.2); **OR**	RA, LRA
		Prior relationship with LRA (supplementary verification, section 7.2.3)	LRA

		OR	
Remote Registration by phone or videoconference (section 7.5)	**AND**	**Remote Registration** by phone or videoconference (section 7.5)	RA

7.1 Documentary Identity Validation

The following requirements apply where an individual's identity is validated or is being Registered into ONE®ID **solely** by documentary evidence:

a. The Registrant must provide TWO pieces of identification, one of which must contain a photograph bearing a true likeness of the Registrant.

b. The second document[1] may be issued by any type of institution that is approved by the Agency.

For a list of primary and secondary documents, see Appendix B.

All identity documents presented must comply with the documentary requirements in section 7.3 and the process requirements in section 7.4.

7.1.1 Secondary Document – Alternative Evidence

Instead of providing a secondary identity document, potential Registrants may provide evidence of the following for review by a RA or LRA (but not a Notary Public):

a. Registration number with a College of a regulated health profession in Ontario (e.g. CPSO registration number).

Note:

A College Registration number is different from a "current registration document from the college of a health profession under the *Regulated Health Professions Act*", which is currently a recognized secondary identity document (see Appendix B). A College Registration number on its own may be presented by the Registrant to the RA or LRA. The RA or LRA shall verify the number, either in the ONE®ID system or via the respective College website before accepting it.

[1] See section 7.1.1 for alternative evidence that may be accepted in place of a secondary document.

7.1.2 Registration by Notary Public

Subject to ONE®ID Program approval, identity validation / Registration that is performed using **solely** documentary evidence may proceed in an in-person meeting with a Notary Public in place of a RA or LRA.

See the guide titled "Registration Using a Notary Public" for further details.

7.2 Supplementary Verification

Identity may be proved by relying on one primary document (see Appendix B), which is supplemented by one (or more) contextual factor(s) as set out below.

7.2.1 General Conditions

7.2.1.1 Photo ID

In order to rely on supplementary identity verification, a potential Registrant must present at least ONE identity document that contains a photo bearing a true likeness of the individual.

7.2.1.2 Minimum Mandatory Identification Information

All minimum mandatory identification information of the Registrant, as defined in the *ONE® ID Policy* (e.g. legal name, gender and date of birth), shall be validated by documentary evidence.

7.2.1.3 Professional Designation

Where applicable, a potential Registrant's professional designation(s) and license number(s) must also be validated as part of the required minimum mandatory identification information specified in the *ONE® ID Policy* by, wherever possible, a secondary document. Contextual evidence may be relied on if necessary or appropriate.

For example, if a physician presents his Driver's Licence as a primary document, it would validate his legal name, gender and date of birth. The physician's professional designation and license number would also need to be validated. It is preferred that, whenever possible, this is achieved by the presentation of a secondary document. However, where necessary or appropriate, a RA may rely on contextual evidence to validate this information (e.g. where Registration takes place at the physician's office and a LRA is able to validate this information by reviewing the practice certificate hanging on the wall).

7.2.2 Practice Location and Role

Where Registration is conducted at a potential Registrant's practice location, a RA or LRA may rely on this as a second piece of evidence to validate the individual's identity, provided that:

i) The practice location (address) must be in the public domain, as confirmed by one or more authoritative source(s) accepted by the ONE®ID Program, e.g. practice location registered with the CPSO;

ii) The RA/LRA has confirmed that the practice location conforms to an address of record (e.g. CPSO registration record), or that the practice location is not a forged address; and

iii) The RA/LRA has confirmed or otherwise has reasonable grounds to believe that the Registrant has or is undertaking a legitimate role of providing or assisting in the provision of health care at that practice location (e.g. the LRA observes that a Registrant is in the process of seeing patients; confirmation by administrative assistant).

Registration may be completed during or after the on-site meeting.

Note: all requirements in section 7.2.1 apply.

7.2.3 Prior Professional Relationship with LRA

Where a LRA has known a potential Registrant in a professional capacity for a minimum of 12 months before the date of Registration, the LRA may rely on this as contextual evidence in place of a secondary document to validate the Registrant's identity.

Note: all requirements in section 7.2.1 apply.

7.3 Documentary Evidence of Identity

Regardless of the method(s) used to Register an individual for a ONE®ID account, the following requirements apply to an identity document that is presented in support of an identity claim:

a. The document must be of an approved type (see Appendix B).

b. The document must be an original or a notarized copy.

c. The document must indicate the full name of the Registrant.

d. The document must be valid at the time of Registration.

e. The document must either contain a photo which bears a true likeness of the Registrant, or it must be reviewed in conjunction with another approved identity document containing such a photo.

f. The document must either:

- Include all minimum mandatory identification information of the Registrant, as set out in the *ONE®ID Policy* (e.g. legal name, gender and date of birth); OR
- Be reviewed in conjunction with at least one approved identity document (e.g. primary document) that contains any unconfirmed minimum mandatory identification information. In other words, any unconfirmed identification information must not be confirmed by contextual evidence (e.g. through supplementary verification).

g. The minimum mandatory identification information as shown on all identity documents being reviewed in conjunction with one another must correspond.

7.4 Process Requirements

Regardless of the method(s) used to Register an individual for a ONE®ID account so as to enable his/her access to Healthcare Applications, all identity documents presented must be reviewed and validated in accordance with the following process requirements:

a. The document(s) must be presented by the Registrant to a registrar through:

- An in-person meeting; OR
- A remote channel (telephone or videoconference) approved by the ONE®ID Program. See section 7.5 for detailed requirements on remote Registration.

b. The registrar may be a RA, LRA or notary public. See section 7.1.2 for requirements on Registration by a notary public.

c. The document(s) must be validated using the appropriate method(s) that attain to the Level of Assurance required for accessing a Healthcare Application, as follows:

- Where **AL2** is required, all document(s) must be verified (confirming a document's authenticity by reviewing its contents);
- Where **AL3** is required, all document(s) must be verified (as for AL2) and corroborated (confirming a document's authenticity with an authoritative source or third-party, e.g. a document's issuing agency).

d. The document must be reviewed in conjunction with:

- Another approved identity document from the primary or secondary documents list (see section 7.1 for detailed requirements on documentary identity validation);
- An accepted alternative to a secondary document (see section 7.1.1); OR
- An approved form of contextual evidence (see section 7.2 for details on supplementary identity verification).

e. The registrar must record the types of all documents reviewed and the number of at least one primary document as part of the validation process.

7.5 Remote Registration

7.5.1 Videoconferencing

Subject to ONE® ID Program approval, Registration for the ONE®ID Service may proceed by videoconference. This option may be used where an in-person meeting with a RA/LRA is impractical. The Registrant must consent to conducting [or completing] ONE®ID registration by videoconference with a RA.

The entire Registration videoconference must:

i. Be a secure point-to-point connection to a verified email address or telephone number;
ii. Occur in real-time, independent of location;
iii. Use only videoconference software / equipment that has been approved by ONE®ID;
iv. Be conducted as a mutually authenticated protected session, OR the transaction must consist of time-stamped or sequenced messages signed by their source and encrypted for the recipient. In either case, cryptography approved by ONE®ID must be used;
v. Use technology that:
   - Allows the combined use of video and audio capabilities to facilitate the review of identity documents; and
   - That has an image quality or resolution that is sufficiently high to verify the authenticity of the identity documents presented (e.g., providing [30] frames per second at a [1280 by 720] display resolution).

A RA must verify the identity of a potential Registrant before proceeding with any Registration by videoconference. For example, a potential Registrant may present two identity documents, whose types and numbers shall be recorded in the ONE® ID database.

7.5.2 Phone Registration

Subject to ONE® ID Program approval, Registration for the ONE®ID Service may proceed by telephone. This process may be used where a face-to-face meeting with a RA or LRA is impractical. The in-person meeting is replaced with a phone call[2] from ONE®ID to a potential Registrant. The potential Registrant must also consent to conducting [or completing] Registration and receiving notifications from ONE®ID by telephone.

The following requirements apply to Registration by telephone with a RA:

i. Potential Registrants must be contacted at a phone number that is recognized/approved by ONE®ID. In order to meet the requirements for AL2, Registration by telephone must also involve confirming the potential Registrant's identity via an out-of-band mechanism or through email to a recognized/approved email address.

ii. Where a phone number has recently changed or the number presented has not yet been established as the Registrant's phone number of record, a RA must not proceed with registration by telephone.

iii. Before proceeding with a phone Registration, a RA must first Authenticate the identity of the Registrant using a process that is defined by the ONE®ID program;

[2] Other out-of-band tokens (e.g. text message or mobile push methods) may also be used.

iv. A phone Registration may not proceed if any call-forwarding feature or answering machine is in use at the scheduled time.

7.6 Alternative Registries and Managed Registration Processes

Subject to the requirements of the *ONE® ID Policy* and the *ONE® ID Alternative Registry Standard*, the Agency may allow the use of an alternative registry or approved managed Registration process of a Registering Organization to validate individuals' identity for the ONE®ID Service.

See the *ONE® ID Alternative Registry Standard* for detailed requirements.

8.0 References and Associated Documents

Reference	Location
Certification Policy Manual, Version 1.1	http://www.ehealthontario.on.ca/
Government of Ontario Corporate Policy on Electronic Identification, Authentication and Authorization (IAA), v.0.8, July 2012	Ministry of Government Services, I&IT Corporate Security Branch
Government of Ontario Policy for Public Facing Electronic Identification, Authentication and Authorization, V.8.1, April 21, 2010	Ministry of Government Services, Office of the Corporate Chief Information Officer, I&IT Strategy, Policy and Planning Branch
ONE® ID Alternative Registry Standard	http://www.ehealthontario.on.ca/
ONE® ID Policy	http://www.ehealthontario.on.ca/

Appendix A: Glossary

Term	Description
Agency	The corporation formerly known as the Smart Systems for Health Agency, which is continued under the name of the Agency in English and cyberSanté Ontario in French.
Authenticate or Authentication	Any process designed to verify the identity of an individual or any other entity, or to establish the validity of a transmission, message, or originator.
Challenge Question	Questions that a Registrant is required to select from a drop-down list and answer during the ONE® ID account activation (self-completion) process. These questions are then used to Authenticate him/her when he/she accesses the ONE® ID system or contacts the eHealth Ontario Service Desk for assistance.
Client or Client Organization	Any organization, which includes Registering Client Organizations, that has entered into any form of agreement with the Agency for accessing and using one or more Healthcare Applications.
College	The college of a health profession under the *Regulated Health Professions Act* in Ontario.
Healthcare Application	The various electronic health information or information management and technology services the Agency provides to a Client and used by a Client pursuant to an agreement.
Level of Assurance	The degree of confidence that can be placed in the Registration (identity validation) or Authentication of an individual
Local Registration Authority	An individual that has been delegated responsibility by a Client Organization for the performance of tasks associated with identifying, Authenticating, Registering, enrolling, and managing Registrants which are within the scope of his or her authority.
Registrant	An individual affiliated with a Client who, or which, has or requires access to one or more Healthcare Applications.
Registe r or Registration	The process by which a unique electronic identity and associated Level of Assurance is established for a Registrant.
Registration Authority	An individual who has been delegated responsibility by the Agency's Certificate Authority for the performance of tasks associated with identifying, Authenticating, Registering, enrolling, and managing Local Registration Authorities and Registrants.
Application Owner	An organization that provides or hosts one or more Healthcare Applications to be made available over the Agency's information infrastructure to one or more Client Organizations.

Appendix B: Primary and Secondary Identity Documents

This section of the document provides a list of the documents that are accepted as primary or secondary documents, and in some cases, a description of the document. Primary documents require the Registrant to prove their identity using more stringent criteria; secondary documents are issued by an institution that has been approved by the Agency.

Primary 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 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, Chiropractic, Dental Hygiene, Dental Technology, Dentistry, Denturism, Dietetics, Massage Therapy, Medical Laboratory Technology, Medical Radiation Technology, Medicine, Midwifery, Nursing, Occupational Therapy, Opticianry, Optometry, Pharmacy, Physiotherapy, Psychology, and Respiratory Therapy)
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 Card

Acceptable Secondary Identity Documents	
15	Union Card
16	Other Federal ID Card, including Military
17	Ontario Ministry of Natural Resources Outdoors Card
18	Judicial ID Card
19	Student Identification 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*

Unacceptable Documents

The following two documents cannot be used for identity verification during the registration process due to legal or statutory regulations.

Unacceptable Secondary Identity Documents	
1	Health Cards
2	Social Insurance Cards