ONE® ID Policy

Service Policy

Version: 2.1
Document ID: 1064
Owner: Director, Product Management

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

Table of Contents

1.0 Policy Identification and Purpose

1.1 Service Description

- The ONE® ID Service ("ONE® ID") is a set of identity and access management systems and processes that enables health care providers to access eHealth Ontario ("Agency") services, and is a key element in making those services trusted and secure.

- ONE® ID helps ensure that only Registrants who need secure and reliable access to health-related information, including Personal Health Information, would be Authorized for access. The robust identity validation process uses a person's real-world identity to create a digital identity, which is then used to Authenticate his/her access to an application. ONE® ID also leverages staff in a health care organization or association to ensure that Agency processes are followed in the Registration and identity validation of application users.

1.2 Purpose

- **Conditions and Commitments**

This Policy sets out the conditions, commitments and terms of engagement that apply to the Registration, Service Enrolment and Authentication of the End Users of Services. This Policy also governs Services not managed by the Agency but for which ONE® ID provides Registration and Authentication services (e.g., eNLB).

- **Intended Audience**

This Policy specifies responsibilities and provides direction to:

  - Agency organizational components (e.g. divisions, departments, projects) and personnel, including executives, employees, consultants and contract employees with responsibilities related to ONE® ID.

  - Client Organizations that have signed an Agreement with the Agency for the provision of the ONE® ID Service, including their Legally Responsible Person (LRP).

  - Sponsors, Delegated Sponsors and Local Registration Authorities (LRAs) delegated responsibility by a Client Organization, or Registration Authorities (RAs) delegated responsibility by the Agency.

1.3 Objectives

This Policy helps ensure that:

- Accountabilities and responsibilities for Sponsorship, Registration, Enrolment and Authentication are identified and carried out in a consistent manner, using well-defined, reliable and secure processes.

- Appropriate processes are implemented to Authenticate the identity of Registrants to a defined Level of Assurance.

- Security practices are enabled to protect the information accessed through ONE® ID and prevent unauthorized access.

- End Users comply with acceptable use requirements for the ONE® ID service, in accordance with the ONE® ID service agreement.

2.0 Legal Authority, Scope and Application

2.1 Legal Authority and Responsibilities

- Provision of Services

  The Agency is legally authorized and responsible to collect, use and disclose Personal Information and Personal Health Information, if necessary, for the provision of Services. [Subsection 4(7), Ontario Regulation 43/02 as amended, made under the *Development Corporations Act*.]

- Allowed Activities

  The Agency is legally authorized and responsible to collect, record, use and disclose Personal Information in order to: (a) Register persons to use the Agency's Information Infrastructure; (b) verify the identity of persons Registering or Registered to use the Agency's Information Infrastructure; and (c) maintain and administer the Registration of such persons. The Agency is prohibited from using or disclosing Personal Information for any other purpose. [Subsection 16, Ontario Regulation 43/02 as amended, made under the *Development Corporations Act*.]

- FIPPA and PHIPA

  The Agency is responsible for ensuring that the collection, recording, use and disclosure of Personal Information and Personal Health Information comply with the provisions of the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Health Information Protection Act* (PHIPA).

2.2 Scope and Applicability

- Requirements

  This Policy sets mandatory, minimum requirements for the ONE® ID Service.

- ONE® ID Standards

  This Policy is supported by ONE® ID standards, including:

  - *ONE® ID Identity Assurance Standard*
  - *ONE® ID Alternative Registry Standard*

- *ONE® ID End User Identification and User Name Standard*
- *ONE® ID Password Standard*
- *ONE® ID Challenge Questions Standard*

- **Delivery of Services**

This Policy applies to the delivery of all Services where Registration, Service Enrolment or Authentication is managed by ONE® ID.

- **Collection, Storage, Use and Disclosure of Personal Information**

This Policy applies to the collection, storage, use and disclosure of Personal Information related to the Registration of: (a) End Users of the Agency's Information Infrastructure; and (b) Agency staff (employees/consultants), Registration and Local Registration Authorities, etc. involved in the management and administration of ONE® ID.

- **ONE® ID Service Agreements**

This Policy applies to ONE® ID Service Agreements and their related Service Modules and Service Schedules signed between the Agency and any Client Organization.

- **Scope of Application**

  - All organizational components and personnel of the Agency, including executives, employees, consultants and contract employees with responsibilities related to the provision of ONE® ID.
  - Any third-party service provider, including employees of the service provider, retained by the Agency to assist in the delivery of ONE® ID.
  - Sponsors, Delegated Sponsors and Local Registration Authorities delegated authority by a Client Organization, and the Certificate Authority and Registration Authorities delegated authority by the Agency.
  - Service Owners who use ONE® ID for accessing Service(s) provided through the Agency's Information Infrastructure.
  - Client Organizations that have signed a ONE® ID Services Agreement and Schedule or Module, as the case may be, with the Agency, including the Legally Responsible Persons, employees, consultants, service providers or other Representatives of the Client Organization.

3.0 ONE® ID Policies

3.1 General Policy Requirement

- End Users[1]

  All End Users must be Sponsored, Registered, Enrolled and Authenticated in accordance with this Policy in order to access any Service provided or managed by the Agency.

- Registration and Enrolment Processes

  All End Users must participate in the Registration and Enrolment processes by:

  - Registering in the ONE® ID service upon receipt of an invitation from a Sponsor.
  - Receiving notification of the legal authority and purpose(s) for the collection, recording, use and disclosure of Registrant information, including Personal Information.
  - Consenting to the collection, recording, use and disclosure of Registration information.
  - Agreeing to abide by the Agency's *Acceptable Use Policy*, as amended from time to time.
  - Accepting any additional terms and conditions of the Service(s) being accessed.

3.2 Sponsorship

- **Service Owners**

While the Agency has defined standards for Registration, Enrolment and Authentication, a Service Owner who has a different business requirement from the standard processes may approach the Agency to request a change, through the Business and Architecture Review Committee (BARC) process (or equivalent), which may be applied to the ONE® ID Service as a whole or implemented for that specific Client only.

Every Service Owner has the responsibility to:

- Specify the Level of Assurance required for a Registrant to be Enrolled in a Service it provides.

[1] See the Glossary for the definition of capitalized terms.

- Designate Client Organizations that may act as Sponsors for a Service.

- Appoint at least one Representative to act as a Sponsor on its behalf.

- **Agency**

The Agency has the responsibility to:

- Provide Services to Client Organizations and deliver a variety of Services, products and technologies, including the ONE® ID Service, in order to meet the business requirements that are defined by Service Owners.

- Sign a ONE® ID Service Agreement and Service Module or Service Schedule, as the case may be, with each Client Organization that qualifies as a sponsoring Client Organization of one or more Services.

- Inform Client Organizations of the eligibility requirements for Registration or Enrolment in a Service.

- Complete service planning and implementation processes to enable End Users to be Registered, Enrolled into and receive Authentication Credentials for accessing Services through the Information Infrastructure.

- **Client Organizations, Legally Responsible Persons and Sponsors**

Every Client Organization that has signed a ONE® ID Agreement shall appoint a Legally Responsible Person and shall designate at least one Representative to act as a Sponsor.

- **Legally Responsible Person's Responsibilities**

The Legally Responsible Person shall:

- Have the authority to sign a ONE® ID Agreement with the Agency.

- Be the primary contact with respect to any matters relating to the Agreement.

- Have overall responsibility for the performance of the Client Organization's obligations under the Agreement.

- Have the authority to approve and grant access to the Service(s).

- Provide notices to the Agency in accordance with the Agreement.

- As necessary, perform the duties and responsibilities of a Sponsor and/or LRA for a Client Organization.

- **Sponsor Responsibilities**

Sponsors are responsible for the following:

- Identifying End Users who are eligible to be Registered and Enrolled into Service(s), including ONE® ID, for which the Sponsor has been given authority to act as a Sponsor.

- Attesting that Registrants meet the eligibility requirements to be Registered or Enrolled in Service(s) for which the Sponsor has been given authority to act as a Sponsor.

- Receiving notification from the Agency that an End User has been Registered in or accessed the ONE® ID service.

- Confirming, verifying, supplying and recording the information required for Registration and Enrolment in a Service to the Agency.

- Obtaining any necessary consents required by applicable Laws and Regulations before collecting, using or disclosing the Personal Information (and Personal Health Information, if any) of a Registrant.

- Approving an End User's Registration and Enrolment in a Service, including the ONE® ID service;

- Informing an End User that his/her Registration and Enrolment(s) are complete and, as applicable, upgrading the End User's Level of Assurance to AL2 (see section 3.4).

- Informing the Agency if any Registrant sponsored by the Client Organization no longer: (a) has a legitimate business requirement to be Enrolled in any Service; or (b) meets the eligibility requirements.

- As necessary, performing some or all of the duties and responsibilities of a Local Registration Authority for the Client Organization.

- **Changing Sponsors**

  A Client Organization may change its Sponsor(s) at any time, subject to its reporting obligations below.

- **Reporting**

  Upon the request of the Agency, Client Organizations shall provide reports as follows:

  - Listing each present and past Sponsor and Delegated Sponsor, along with the Service(s) for which each of them has or had sponsorship authority.

  - Listing all current or former Registrant(s) that each Sponsor, Delegated Sponsor or LRA has Enrolled in any Service(s).

  - The report must be prepared in a format and include such detail as may be required or accepted by the Agency (acting reasonably).

  - The Agency may provide electronic systems to assist in recording and reporting Sponsor and Delegated Sponsor information.

3.3 Registration

Several identity validation methods may be used to Register in the ONE® ID Service, in certain cases subject to ONE® ID Program approval. Please refer to the *ONE®ID Identity Assurance Standard* for detailed requirements.

- **Registrants**

  A Client Organization or the Agency must Register sponsored individuals.

  - Individuals may be Registered as a:
    - Registration Authority of the Agency; or
    - Legally Responsible Person, Sponsor, Delegated Sponsor, Local Registration Authority or End User of a sponsoring Client Organization.
  - A Legally Responsible Person may delegate responsibilities to a Sponsor, Delegated Sponsor and/or LRA. Written or electronic notice of the delegation shall be given to the Agency, which should include the name and contact information of the individual to whom responsibility is being delegated and a description of the scope of that delegation.
  - The Agency shall provide each Registration Authority or Local Registration Authority with a copy of the Registration Authority Procedures Manual or the Local Registration Authority Procedures Manual, as the case may be.

- **Items Assigned to Registrants**

  Every Registrant shall be assigned the following:

  - A unique identity and User ID conforming to the *ONE® ID End User Identification and User Name Standard*.
  - A Level of Assurance conforming to the *ONE® ID Identity Assurance Standard*.
  - The information required to set and maintain a password in conformity with the *ONE® ID Password Standard*.

- **User ID**

  No Registrant shall knowingly be Registered with more than one unique identity or User ID except when:

  - The previously existing Registration has been revoked.
  - A probable unique identity has been discovered for the Registrant but it cannot be determined with sufficient assurance that the identity belongs to the Registrant.

- The Registrant is Enrolled for more than one Service and one of these requires establishing a unique identity separate and distinct from any other.

- **Duplicate Identities**

Where it is discovered that duplicate identities have been inadvertently established, the duplicate Registration(s) must be revoked:

- The duplication shall be resolved as quickly as possible in favour of the earliest active Registered identity.

- The retained identity shall be updated to reflect the most accurate, complete and comprehensive Registration information available, including the assigned Level of Assurance and active Enrolment(s).

3.4 Levels of Assurance

- **Defined Levels of Assurance**

An individual shall be assigned a defined Level of Assurance by ONE® ID at the time of Registration.

ONE® ID shall use the following standards when assigning a Level of Assurance to an individual, based on the classification of the information that will be accessed:

Level of Assurance	Information Classification	Description of Level of Assurance
AL1	AL1 is appropriate for information that has a sensitivity level of "unclassified", and is normally used for public information and internal communications, such as internal documents and unclassified communications, normally intended for communication between staff. If compromised, this information could reasonably be expected to cause no significant injury or losses to the parties involved and would require only administrative action for correction.	An unverified identity: An individual supplies all identification information, which is taken at face value. No assurance needed as to veracity of identification claim.

Level of Assurance	Information Classification	Description of Level of Assurance
	AL1 is insufficient when Personal Health Information or Personal Information will be accessed.[2]	
AL2	AL2 is appropriate for information that has a high sensitivity level within eHealth Ontario or the health sector environment, and that is intended for use by specific and Authorized individuals only. If compromised, this information could reasonably be expected to cause serious injury or financial losses to one or more of the parties involved or would require legal action for correction.	A verified identity: An individual is uniquely identified through a managed Registration process and identification claim is verified with documentary evidence and / or authoritative source(s), which may be supplemented by contextual evidence in appropriate circumstances.
AL3	AL3 is appropriate for information that is extremely sensitive and of the highest value within eHealth Ontario or the health sector environment. This information is intended for use by named and Authorized individuals only. To decide whether an AL3 is required, the Agency shall consider: • Whether any circumstance(s) or the context surrounding the access or use of the information require(s) additional confirmation of identity than AL2.	A corroborated identity: An individual is uniquely identified through a managed Registration process and identification claim is verified using at least two separate methods (e.g. multi-factor), and / or corroborated with authoritative source(s) (e.g. the issuer of the documentary evidence presented).

- **Assigning a Level of Assurance**

The Agency shall assign a Level of Assurance to the Registration of each individual corresponding to the degree of effort taken to validate the Registrant's identity, including the rigour of the Registration process involved and strength of the evidence offered to support the identity. The *ONE® ID Identity Assurance Standard*

[2] This is subject to exception(s) relating to access from sponsored accounts pursuant to a delegation arrangement.

should be consulted when assigning a Level of Assurance to the Registration of each individual.

- **Access to Sensitive Information**

Access to any Service containing Sensitive Information, including Personal Information and Personal Health Information, shall not be provided unless a Registrant has been assigned an AL2 or AL3.[3]

3.5 Required Identification Information

- **Minimum Mandatory Identification Information**

  - The minimum mandatory identification information required for an individual includes: legal name, gender and date of birth. Where applicable, the professional designation and license number are required.

  - **Note:** A Health Card number from any province, including Ontario, or a Social Insurance Number, must not be accepted to confirm the identity of an individual who is Registering in any Service(s).

- **Additional Information**

In addition to the minimum mandatory identification information, the Agency may collect, record, use and disclose other information as specified in the *ONE® ID End User Identification and User Name Standard*.

- **Changes to Identification Information**

Every Registrant must advise the Agency of any changes to the required identification information.

  - In some instances, e.g., changes to legal name, the Agency may require the submission of supporting documents.

- **Acceptable Use Policy**

Every Registrant shall agree to be bound by the Agency's *Acceptable Use Policy*, as amended from time to time.

  - A Registration Authority or Local Registration Authority shall not Register or Enrol a Registrant in any Service if a Registrant does not agree to be bound by the Agency's *Acceptable Use Policy*.

---

[3] *Ibid.*

3.6 Alternative Registry

In order to facilitate or expedite Registration in the ONE® ID service, the Agency may use an alternative registry that has been developed or managed by an organization that:

i. Is not a Health Information Custodian; and

ii. Demonstrates a documented and verifiable relationship with an acknowledged health sector regulatory body, administrative agency or other health sector organization designated by the Agency.

An alternative registry approved by the Agency shall comply with this Policy and the *ONE® ID Alternative Registry Standard*.

If a Registrant has previously been identified in an alternative registry using processes and systems that has been reviewed and approved by the Agency as being comparable and equivalent to those used by the Agency, and there have been no changes to the information presented, ONE® ID may use this privately shared information to validate the Registrant's identity.

3.7 Managed Registration Processes of Registering Client Organizations

The Agency may review and approve the use of a managed Registration process that has been developed or is maintained by a Registering Client Organization in order to expedite or facilitate Registration. A Registering Client Organization must be a(n):

i. Organization that provides health care or assists in the provision of health care in Ontario; or

ii. Health Information Custodian.

Detailed requirements are set out in the *ONE®ID Alternative Registry Standard*.

3.8 Authentication

- **Processes**

The Agency shall establish processes to validate the association between End Users' real-world identity and their Credentials as established during the Registration process. Any interaction between the Information Infrastructure and End Users will only be allowed after successful Authentication.

- End Users shall be required, at a minimum, to present a User ID and a password prior to engaging in any interaction with the Information Infrastructure.

- End Users shall comply with the requirements of the *ONE® ID Password Standard*.

- Where the Client requests it, hardware tokens or other Authentication methods may be used in some situations.

- From time to time, the Agency may, at its sole discretion, revise its Authentication methods, giving written notice of the revision to the Client.

- The use of Authentication methods involving the collection of Challenge Questions shall comply with the requirements of the *ONE® ID Challenge Questions Standard*.

- In addition to the presentation of a User ID and a password, the use of hardware tokens or other Authentication methods may be used to validate an out-of-province interaction between the Information Infrastructure and an End User.

3.9 Enrolment

- **Eligibility Criteria**

The Agency shall Enrol Registrants into Service(s), provided that the Registrant is sponsored and meets the eligibility criteria, including the Level of Assurance, specified by the Service Owner.

- A Registrant may be sponsored for Enrolment into one or more Services by one or more Client Organizations.

- A Registrant may be Enrolled into the same Service multiple times based on sponsorship by different Client Organizations.

- **Timing**

Enrolment may occur at the same time as Registration, for a first-time Registrant.

- Every Enrolment shall be recorded and maintained independently and distinctly from any other.

- Information concerning a Registrant's Enrolment(s) shall not be communicated across Client Organizations.

- Information that has been recorded for a Registrant (e.g., professional designation, contact information, etc.) as a result of an Enrolment may be reused in connection with a new Enrolment without being collected and recorded again.

- **Additional Information**

The Agency may collect, record, use and disclose additional information required for Enrolment in a Service.

3.10 Suspension

- **General Rules**

A Registration or Enrolment may be suspended and access temporarily disabled if:

- At the Agency's discretion, the Registrant has not actively used his/her ONE® ID account or a specific Enrolment has not been used for a period in excess of six (6) months.
- Information is discovered or revealed suggesting a reasonable likelihood that the information, documentation or any other matter provided or done to establish the Registration or Enrolment was misleading, false or fraudulent.
- The Registrant has failed to comply with the *Acceptable Use Policy* or the terms and conditions of a Service.
- Suspension is requested by a Client Organization for any reason (e.g., leave of absence) for a period not exceeding two years.

- **Reactivation**

A Registration that has been suspended because there is no active Enrolment associated with it, a temporary role change, a leave of absence or a failure to comply with the Agency's *Acceptable Use Policy*, may be reactivated through a new Enrolment.

- **Documentation**

A Registration or Enrolment that has been suspended due to possible misleading, false or fraudulent information shall not be used or reactivated unless it has been confirmed that the identity information, documentation or other material facts related to the Registration are accurate.

- **Reason for Suspension**

The reason for a suspension and any resulting actions taken, including an investigation, must be recorded and retained.

- **Written Notice**

The Agency shall provide a Client Organization with written notice of any suspension and the reason(s) for the suspension of a Local Registration Authority pursuant to the terms of the signed Agreement.

3.11 Revocation

- **Enrolments**

An Enrolment shall be revoked when the Registrant no longer requires it or when the Enrolment is no longer Authorized.

- **Registration**

The Registration of an individual shall be revoked if:

- The individual is deceased.
- There has been no active Enrolment for a period exceeding two years.
- It is determined that the Registration concerned is a duplicate.
- It is determined that the identity information, documentation or any other matter provided or done to establish the identity was misleading, false, or fraudulent.
- The identity has been otherwise compromised (e.g., identity theft).
- It was requested by the Registrant for any reason.

- **Subordinate Enrolments**

The revocation of any Registration shall include the revocation of all subordinate Enrolments.

- **Documentation**

The revocation and any resulting actions taken shall be recorded and retained.

- **Client Organizations**

The Agency shall provide written notice to Client Organizations of any revocation of Registration and the reason(s) for the revocation of a Local Registration Authority.

4.0 Operational Policies

4.1 ONE® ID Responsibilities

- **Agency**

The Agency is the root Registration Authority for ONE® ID and is responsible for:

- Developing, maintaining and supporting access management systems for Registration, Enrolment and Authentication.
- Appointing one or more person(s) to carry out the duties of Registration Authority/ies for the Agency.
- Appointing one or more persons, including persons nominated by a Client Organization, to act as Local Registration Authorities for the Client Organization and the Services for which they are appointed.
- The Agency shall provide each Registration Authority or Local Registration Authority with a copy of the Registration Authority

Procedures Manual or Local Registration Authority Procedures Manual, as the case may be.

- **Integrity of Identity Information**

The Agency is responsible for ensuring an appropriate separation of duties to maintain the integrity of the identity information collected, recorded, used and disclosed for ONE® ID.

- In general, the responsibilities of Sponsors, Registration Authorities and Local Registration Authorities should be performed by different individuals.

- A Legally Responsible Person, Sponsor, Registration Authority or Local Registration Authority shall not Register him/herself. Identity validation shall be performed by another RA, LRA or notary public.

- Where a Legally Responsible Person whose identity validation and Registration has been completed by an authorized and different individual, appoints him/herself as the Sponsor for a Client Organization, he or she may Enrol other Registrants as well as him/herself.

- **ONE® ID Agreement**

Every Client Organization that signs a ONE® ID Agreement with the Agency is responsible for carrying out the obligations of that agreement, including the designation of persons who may act as Sponsor(s) for Service(s), and the nomination of one or more persons to carry out the functions of a Local Registration Authority.

4.2 Termination of Agreements

- **Agency**

In the event that any agreement with a Client is terminated, the Agency shall retain and use:

- Registrant information for any individual who has completed a Registration and provided consent for the collection, recording, use, and disclosure of the information.

- Archival information regarding past Registration or Enrolment activity according to legal and policy requirements.

- **Service Owner**

If a Service Owner terminates an arrangement for its Service to be provided through the Agency's Information Infrastructure:

- The Agency shall work with the Service Owner to implement an orderly transition on a case-by-case basis.

- Enrolments in the Service shall cease as of the termination date for the Service.

- No further Enrolments shall occur through ONE® ID for the discontinued Service.

- The Service Owner may receive a copy of the Enrolment information current to the termination date for the Service.

- **Client Organization**

If an Agreement between the Agency and a Client Organization is terminated:

- Any sponsoring information or file provided to the Agency to assist in Registering and Enrolling End Users shall be returned to the Client Organization.

- The Client Organization may not sponsor any further Registration or Enrolment.

- The appointment of any individual as a Local Registration Authority to represent the Client Organization shall be revoked.

- The Client Organization may receive a copy of Enrolment information for its sponsored End Users current to the date of termination.

- **Notification**

The Agency shall provide written notice of the termination of any Agreement pursuant to the terms of the Agreement.

4.3 Responsibilities of Registration and Local Registration Authorities

- **Registration Authority's Level of Assurance**

Registration Authorities who are employees of and act on behalf of the Agency shall be Registered at an appropriate Level of Assurance and issued Credentials required by the Agency to access ONE® ID processes, procedures or systems as required to perform their duties.

- **Registration Authority Acknowledgement**

Every Registration Authority must sign or click through a Registration Authority Acknowledgement with the Agency. The Agency may revise this acknowledgment from time to time, giving written notice of such revisions to the Client.

- **Registration Authority Access Privileges**

Each Registration Authority is granted access privileges to the Agency's identity and access management policies, processes, procedures and systems, and is responsible for:

- Registering sponsored individuals as End Users of the Agency's Information Infrastructure.
- Where applicable, Enrolling Registrants in Services.
- Updating and maintaining Registration and Enrolment information.
- Performing supporting services to Registrants as required.
- Performing these duties in compliance with this Policy, including privacy and security requirements.

- **Local Registration Authority's Level of Assurance**

Local Registration Authorities who are delegated responsibility by a Client Organization's Legally Responsible Person or Sponsor shall be Registered at an appropriate Level of Assurance and issued Credentials required by the Agency to access ONE® ID processes, procedures or systems as required to perform their duties.

- **Local Registration Authority Acknowledgement**

Every Local Registration Authority must sign a Local Registration Authority Acknowledgement with the Agency. The Agency may revise this acknowledgment from time to time, giving written notice of such revisions to the Client.

- **Local Registration Authority Access Privileges**

Each Local Registration Authority is granted access privileges to the Agency's identity and access management policies, processes, procedures and systems, and is responsible for:

- Registering sponsored individuals as End Users of Service(s) and notifying the Sponsor of the completion of a Registration.
- Where applicable, Enrolling Registrants in Service(s) for which his/her Client Organization has been Authorized.
- Updating and maintaining Registration and Enrolment information.
- Providing supporting services to Registrants as required.
- Performing these duties in compliance with this Policy, including privacy and security requirements.

4.4 Customer Service Support

- **Customer Service Representatives**

The Agency shall Register and Enrol customer service representatives to perform the tasks of identifying, Authenticating, and assisting End Users within the scope of their authority, as delegated by the Agency.

- **Level of Assurance**

Customer service representatives must be Registered at an AL2 and provided with the Credentials necessary to access the Service(s) for which they provide support.

- **Access to Information**

Customer service representatives shall be provided with access to the Registrant information required to carry out their assigned duties, including information required for the Authentication of Registrant identity.

4.5 Infrastructure Service Support

- **ONE® ID Service**

The Agency shall Register and Enrol users who require access related to developing, testing, and maintaining the Service(s), including the ONE® ID Service.

- **Level of Assurance**

Users providing infrastructure services must be Registered (at a minimum) at an AL2 and provided with the Credentials necessary to access the Service(s) for which they provide support.

- **Limited Access**

Access for such users may be limited by the time or functionality required for carrying out their duties.

4.6 Monitoring and Audit

- **Logging**

All transactions against the Agency's Information Infrastructure, including its identity and access management system(s), must be logged

- **Processes**

The Agency may implement processes to monitor and audit compliance with this Policy by any persons with operational responsibilities, including Registration Authorities, customer service representatives and infrastructure support users.

  - Client Organizations shall provide information access and assistance that is reasonably required by the Agency for the purposes of conducting any audit.

5.0 Policy Approval and Administration

5.1 Policy Approval

- **Authority**

This Policy is issued under the authority of the Chief Executive Officer of eHealth Ontario.

- **Effective Date**

This Policy is effective on the date set for its publication by the Chief Executive Officer, and on the date(s) set as it is amended from time to time with the approval of the Chief Executive Officer.

- **Approval Method**

The Agency follows a coordinated method for the approval, review, and revision of this Policy.

5.2 Administration

- **Responsibility**

The Senior Director, cGTA, administers this Policy.

5.3 Publication and Notification

- **Availability**

A copy of this Policy is available in electronic format on the Agency's website (www.ehealthontario.on.ca).

- **Audience**

This Policy is intended to be read and made available to Agency staff involved in the ONE® ID Service, as well as ONE® ID Clients (or potential ONE® ID Clients).

- **Modifications**

Client Organizations and End Users should periodically check the Agency's website for notice of modifications to this Policy.

5.4 Interpretation

- **Responsibility**

The Senior Director, cGTA, is responsible for the interpretation of this Policy, including the resolution of any dispute related to it.

- **Applicable Laws**

Each provision of this Policy and any relevant agreement pursuant to it will be interpreted in such manner as to be effective and valid under the applicable laws of Ontario and Canada, including:

  - Ontario Regulation 43/02, as amended

- *Personal Health Information and Protection Act, 2004* and Ontario Regulation 329/04
- *Freedom of Information and Protection of Privacy Act*.

- **Related Policies**

This Policy shall be interpreted in accordance with other Agency policies, including the *eHealth Ontario Privacy and Data Protection Policy*, *eHealth Ontario Privacy Impact Assessment Policy*, *eHealth Ontario Acceptable Use Policy* and *eHealth Ontario Information Security Policy*.

- **Waivers**

The failure of the Agency to enforce at any time any of the provisions of this Policy may not be construed as a present or future waiver of such provisions, nor would it in any way affect the ability of the Agency to enforce each and every such provision thereafter. The express waiver by the Agency of any provision, condition, or requirement of this Policy, and related agreements will not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

- **Agency Name**

A reference to the Smart Systems for Health Agency (SSHA) in any document that provides background or support for this Policy shall be read as referring to eHealth Ontario.

- **References to Sections**

Unless otherwise specified, all references to "sections" refer to the sections of this Policy.

- **Pronouns**

Pronouns, and any variations thereof, include the feminine and masculine, and all terms used in the singular include the plural, and vice versa, as the context may require.

- **"Include" and "Including"**

The words "include" and "including" when used are not intended to be exclusive and mean, respectively, "include, without limitation," and "including, but not limited to."

- **Capitalization**

Capitalized terms used in this Policy have the meaning ascribed to them in the Glossary.

5.5 Contact Details

Information concerning this Policy may be obtained from:

ONE® ID Business Solutions & Support

eHealth Ontario,
415 Yonge Street,
Toronto, Ontario
M5B 2E7

6.0 Appendix A: Glossary

Term	Description
Acceptable Use Policy	The Agency's requirements regarding acceptable use of the Services, as modified from time to time.
Agency	The corporation formerly known as the Smart Systems for Health Agency which is continued under the name of eHealth Ontario in English and cyberSanté Ontario in French.
Agreement	Collectively, the Master Services Agreement or the Agency's Services Agreement together with any Service Module(s), including any attached Service Schedule(s) and any documents incorporated by reference.
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.
Authorized Representative or Legally Responsible Person	The person(s) appointed by the Agency and the Client Organization who will be the primary contact for the other party with respect to any matters relating to the Agreement signed between the Agency and the Client Organization. The Authorized Representative(s) of either party shall: (i) have the overall responsibility for coordinating the performance of their respective obligations under the Agreement; and (ii) have the authority to provide notices to the other party under the Agreement.
Certificate Authority	An individual or group of individuals designated by eHealth Ontario who are responsible for the Registration, Service Enrolment, and Authentication services provided by eHealth Ontario to Clients.
Challenge Question(s)	See Online Challenge Questions and Service Desk Challenge Questions (below)
Client or Client Organization	Any organization that has entered into any form of agreement with the Agency related to the provision of Services for the collection, transmission, storage, use, or disclosure of information about health matters (including Personal Health Information).
Credential	Any credential including, but not limited to, a user identification, password, token public key certificate (PKI certificate), or any combination of these that is issued by the Agency to an End User to allow Authentication of the End User's identity to a system or application.
Delegated Sponsor	An individual Representative of a Client who a Sponsor has delegated to be responsible for determining whether or not a potential Registrant is eligible to be an End User of a Service. The delegation by the Sponsor must be approved by the Client's Legally Responsible Person and the delegation shall be for a limited period of time and be on a service-by-service basis.
End User	Any individual who is a Representative of the Client who has been Authorized to use the Service(s).

Term	Description
Enrol or Enrolment	The process of Enrolling a Registrant as being Authorized to access specific Service(s). Enrolment assumes that Registration has established identity to a specified Level of Assurance and that the due diligence required for Enrolment can be satisfied by the due diligence applied to Registration. A Registrant may be Enrolled for multiple Services.
Health Information Custodian	Has the same meaning as in the *Personal Health Information Protection Act, 2004* [Section 3 (1)].
Information Infrastructure	The Agency's computer networks, hardware, software, facilities, telecommunications, and related equipment, information technology systems and data repositories, for the collection, transmission, storage, and exchange of health-related information (including Personal Health information).
Laws and Regulations	All statutes, regulations, codes, ordinances, decrees, rules, municipal by-laws, judicial, arbitrable, administrative, ministerial, departmental, or regulatory judgments, orders, decisions, rulings, or awards enacted or promulgated by any regulatory body pursuant to any statutory authority or requirements and, in all cases, applicable, binding, and enforceable in Canada.
Level of Assurance	The degree of confidence that can be placed in an identity through Registration or Authentication.
Local Registration Authority Acknowledgment	An Agreement that governs how an individual who has been appointed as a Local Registration Authority shall perform his or her duties as a Local Registration Authority.
Local Registration Authority(ies)	An individual that has been delegated responsibility by a Client Organization's Legally Responsible Person or Sponsor for the performance of tasks associated with identifying, Authenticating, Registering, Enrolling, and managing Registrants that are within the scope of his or her authority.
Online Challenge Questions	Questions that an End User is required to select from a drop-down list in connection with the End User's Registration record. These questions are used to verify an End User's identity over the phone or Internet to safeguard the integrity of the Information Infrastructure.
Personal Health Information	Has the same meaning as in the *Personal Health Information Protection Act, 2004* [Section 4 (1)].
Personal Information	Has the same meaning as in the *Freedom of Information and Protection of Privacy Act* [Section 2 (1)].
Register or Registration	The process by which a unique identity is established for any End User of the Agency's Information Infrastructure with an associated defined Level of Assurance.
Registrant(s)	An individual sponsored by a Client Organization that has or requires access to one or more Service(s).
Registration Authority	An individual that has been delegated responsibility by the Agency's Certificate Authority for the performance of tasks associated with identifying, Authenticating, Registering, Enrolling, and maintaining

Term	Description
	Registrants which are within the scope of his or her authority as delegated by the Certificate Authority. Registration Authorities are authorized to Register Local Registration Authorities.
Representative(s)	In the case of the Agency or the Client, any directors, officers, employees, agents, consultants, or subcontractors (including service providers) to the Agency or the Client, as the case may be, as well as the directors, officers, employees, or agents of any subcontractor, of each such party.
Sensitive Information	Information that if released without authorization would cause harm, embarrassment or unfair economic advantage, i.e., breach of the duty of confidentiality or the duty to protect the privacy of individuals with respect to their PHI or PI.
Service	Any electronic service, application or other resource that: (i) a Client may access over the Agency's Information Infrastructure; (ii) is made available to the Client by the Agency, or is provided by an organization other than the Agency but for which ONE® ID performs Registration and Authentication (e.g., eNLB); and (iii) used by a Client in accordance with the terms and conditions of an Agreement between the Client and the Agency. Service(s) include(s) electronic health service(s) that enable(s) a Health Information Custodian to use electronic means to collect, use, modify, disclose, retain or dispose of Personal Health Information.
Service Desk Challenge Question(s)	Questions that an End User is required to set up to facilitate account activation. These questions are then used to identify an End User when he/she calls in for support. An End User is free to provide his/her own questions, subject to certain conditions.
Service Module	The individual service Agreement(s) between the Agency and the Client that govern the provision of specific information management and technology services to the Client by the Agency. These Service Agreements are executed by the parties and incorporate by reference the terms and conditions of the Master Services Agreement.
Service Owner	A Client Organization that has entered into an agreement with the Agency for the provision or hosting of Services that collect, store, use, or disclose health-related information, including Personal Health Information, to the End Users of one or more Client Organizations.
Service Schedule	The individual Service Schedule(s) between the Agency and the Client governing the provision of specific information management and technology services to the Client by the Agency. These schedules are incorporated by reference in the Agreement.
Sponsor	An individual Representative of a Client who the Client has designated as being responsible for determining whether or not a potential Registrant is eligible to be an End User of a Service.
User ID	Electronic information comprising a string of characters, uniquely identifying an End User of an information system.

7.0 Appendix B: References and Associated Documents

Reference	Location
Development Corporations Act, R.S.O. 1990, Chapter D10 Ontario Regulation 43/02 as Amended to Ontario Regulation 54/05	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90d10_e.htm
Personal Health Information Protection Act	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm
Freedom of Information and Protection of Privacy Act	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
eHealth Ontario Acceptable Use Policy	http://www.ehealthontario.on.ca/pdfs/ProgramsServices/AUP.pdf
eHealth Ontario Privacy and Data Protection Policy	http://www.ehealthontario.on.ca/pdfs/Privacy/Privacy_Data_Protection_Policy.pdf
eHealth Ontario Information Security Policy	http://www.ehealthontario.on.ca/pdfs/Privacy/Information_Security_Policy.pdf
eHealth Ontario Enterprise Security & Privacy Incident Management Operating Directive	http://www.ehealthontario.on.ca/pdfs/Privacy/ESPIM_Operating_Directive.pdf
Certification Policy Manual, Version 1.1, January 25, 2005	http://www.ehealthontario.on.ca/pdfs/ProgramsServices/CP_Manual.pdf
ONE® ID Identity Assurance Standard	https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_15337_6244_717_23647_43/do/document/overview?projID=129869
ONE® ID Alternative Registry Standard	https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_15337_6244_717_23647_43/do/document/overview?projID=129869
ONE® ID End User Identification and User Name Standard	https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_15337_6244_717_23647_43/do/document/overview?projID=129869
ONE® ID Password Standard	https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_15337_6244_717_23647_43/do/document/overview?projID=129869
ONE® ID Secret Challenge Questions Standard	https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_15337_6244_717_23647_43/do/document/overview?projID=129869