Ontario Health

Federation Identity Provider Standard

Version: 1.7

Document ID: 3525

Document Control

Next Review Date: Every two years or otherwise established by the Connecting Security Committee.

Approval History

APPROVER(S)	APPROVED DATE
OH Digital Services VP & CISO, Technology Planning & Information Security	2017-11-07
Connecting Security Committee	2018-03-26
OH Digital Services VP & CISO, Technology Planning & Information Security	2020-04-23
Connecting Security Committee	2021-03-18

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.1	August 5, 2014	Final version (v.1.1) with changes from the Privacy Office and Security team	Clara Wong
1.2	January 30, 2015	Updated section related to system logs and amended Part II to include the EHR security policies	Alan Douthwaite
1.3	June 22, 2015	Consolidated and updated definition of "Remote Access Session" in Glossary.	Clara Wong
1.3	June 26, 2015	Incorporated comments from Security team.	Clara Wong
1.31	Nov 10, 2016	Updated password reset frequency to allow up to 1 year for password reset frequency and adjusted the retention requirements authentication logs.	Clara Wong
1.40	March 28, 2017	Updated Standard to align with EHR Security Policies. Merged in content from the Local Registration Authorities Practices Policy and included periodic account audit requirements.	Raviteja Addepalli
1.41	Nov 7, 2017	Update to include Provincial Two Factor Authentication requirements	Marianne White
1.5	March 16, 2018	Update standard to include Patient access to the EHR and NIST password recommendations (NIST 800-63B)	Geovanny Diaz / Ola Edidi
1.6	March 31, 2020	Update standard into new template and made minor revisions for clarity.	John Limarzi

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.7	2021-01-21	Review of the document with minor changes, updated references and the review cycle to biennially.	Ana Fukushima

Federation Identity Provider Standard

Purpose

This Standard establishes the mandatory, minimum requirements applicable to Identity Providers (the "IDP") to be accredited to provide Identity and Authentication Services ("IA Services") in the Ontario Health Federation ("Federation").

Specifically, this Standard governs the Registration and Authentication by the IDP of End Users' access to electronic health services, applications, information and resources (collectively "Federated Services") that are accessible over Ontario Health's Federated System – a technology infrastructure comprising applications, systems, registries, databases, files, portal applications and tools.

Information concerning this document may be obtained from Ontario Health Connecting Security: oh-ds_connecting.security@ontariohealth.ca.

Scope

This document applies to all IDPs that Ontario Health accredits to provide IA Services in the Federation and to their Representatives

The Federation is a network whose members either provide or access Federated Services over Ontario Health's Federated System.

Ontario Health's ONE® ID Program is the Federation Operator of the Federation—a "broker" that relays End Users' access requests for Federated Services, together with identity validations from their IDPs, to enable Application Providers to make informed Authorization decisions.

This Standard and any relevant agreement pursuant to it will be interpreted in such manner as to be effective and valid under applicable Laws and Regulations, including:

- Development Corporations Act and Ontario Regulation 43/02 as amended
- Personal Health Information Protection Act, 2004 (PHIPA) and Ontario Regulation 329/04 as amended
- Freedom of Information and Protection of Privacy Act (FIPPA)

Where there is a discrepancy or gap between this Standard and applicable Laws and Regulations, Laws and Regulations shall take precedence.

Definitions

Acceptable Use Policy: Ontario Health requirements regarding acceptable use of the Federated System or the Federated Services, as modified from time to time.

Application Provider: An organization that provides one or more electronic health application(s) available for consumption over Ontario Health's Federated System as Federated Service(s).

Authenticate or Authentication: Any process that validates the electronic identity of an End User against his/her real-world identity.

Authoritative Party: A third-party individual or, organization or process through whom/which that is accepted by an accredited IDP for corroborating End Users' real-world identity can be corroborated (e.g., employers could be an Authoritative Party for their employees).

Authorize or Authorization: Any process that determines whether access to Federated Services is granted or denied based on specific business rules determined by Application Providers. Services.

Challenge Questions: Questions that an End User is required to select from a drop-down list and answer during Registration, which is used subsequently to Authenticate that End User.

Core Identity Information: The minimum Registration information that the IDP is required to collect in order to perform the IA Services, as more specifically defined in this Standard.

Credential: Information that is issued and attached to an End User through a Registration process to facilitate Authentication. Credentials include, but are not limited to, a User ID (login ID), password, token, public key certificate (PKI certificate), or any combination of these.

Ontario Health Federation (Federation): A computer network whose members either deliver or access Federated Services over Ontario Health's Federated System.

End-User: An individual who is authorized to access one or more Federated Service(s), usually as a Representative of a Sponsoring Organization.

End-User Information: All information used for Registration of the End User, including the End User's User ID and Core Identity Information. End-User Information may include Personal Information.

Enroll or Enrolment: The process of giving End-User access to specific Federated Service(s).

Federation Operator: In the context of the Federation means Ontario Health.

Federated Service: The electronic health services, resources and information that are accessible over the Federated System.

Federated System: The technology infrastructure of the Federation comprising applications, systems, registries, databases, files, portal applications and tools.

Health Information Custodian: Has the same meaning as in the Personal Health Information Protection Act, 2004 [Section 3(1)].

Identity Access and Management System (IAMS): The IDP's computer system, applications and associated practices, policies and procedures for creating, maintaining, securing, validating, asserting verifications, and managing electronic identities.

Identity and Authentication Services (IA Services): The electronic services provided by an IDP that include validating End-User identity, issuing Credentials, and sending Authentication information.

Identity Provider (IDP): An organization that provides IA Services within the Federation.

Laws and Regulations: The Personal Health Information Protection Act, 2004 and all statutes, regulations, codes, ordinances, decrees, rules, municipal by-laws, judicial, arbitral, 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 and/or Ontario.

Level of Assurance: The degree of confidence that can be placed in or that is required from the Registration and Authentication of an End User's electronic identity.

Patient Portals/Applications: Applications (HIC or non-HIC affiliated) that facilitate Patient access to the EHR. These applications may be:

- Provider-Gated (Provider facilitates communication with Patient)
- Direct-to-Patients (Patient has direct access to EHR)
- Patient-Gated (Patient delegates access to a Substitute Decision Maker/additional delegates (i.e. family member, physician)

Personal Health Information (PHI): Has the same meaning as in the Personal Health Information Protection Act, 2004 [Section 4 (1)].

Personal Information (PI): Has the same meaning as in the Freedom of Information and Protection of Privacy Act [Section 2 (1)].

Privacy Breach: A Privacy Breach includes:

- A contravention of PHIPA and its regulation, including:
    - Any collection, use or disclosure of PHI that is not in compliance with PHIPA and its regulation
    - Any retention, transfer or disposal of PHI that is not in compliance with PHIPA and its regulation
    - Any circumstances where PHI is stolen, lost, used or disclosed in an unauthorized manner or accessed by unauthorized persons
    - Any circumstance where records of PHI are subject to unauthorized copying, modification or disposal
- A contravention of FIPPA, including:
    - Any collection, use or disclosure of PI that is not in compliance with FIPPA and its regulations
    - Any retention, transfer or disposal of PI that is not in compliance with FIPPA and its regulations
    - Any circumstances where PI is stolen, lost, used or disclosed in an unauthorized manner or accessed by unauthorized persons
    - Any circumstance where records of PI are subject to unauthorized copying, modification or disposal
- A contravention of the privacy policies, procedures or practices implemented by Ontario Health

- A contravention of the privacy provisions in agreements which Ontario Health enters into with external stakeholders and third-party service providers, including the privacy provisions in PHIPA agent agreements, data sharing agreements, confidentiality and non-disclosure agreements and agreements with third-party service providers retained by Ontario Health.

Privacy Breaches can be intentional or inadvertent.

Privacy Impact Assessment (PIA): A detailed assessment undertaken to evaluate the effects of a new or significantly modified service to determine its actual and potential impact on the protection of PI/PHI included in the service. PIAs measure compliance with applicable privacy law and broader privacy implications. A PIA addresses all technological components, business processes, flows of personal information, information management controls and human resource processes associated with a service and identifies ways in which privacy risks associated with these may be mitigated.

Privilege: Assigned to accounts to confer enhanced rights within a system or application. Typical rights include the ability to override system or application controls, manage End User accounts, alter or manage content, write to system files, or perform maintenance.

Register or Registration: The process by which a unique electronic identity is established for any End User, which is associated with a Level of Assurance.

Representative: In the case of Ontario Health or a Participant, any of its directors, officers, employees, agents, consultants, subcontractors or service provider to Ontario Health or that Participant, as well as the directors, officers, employees, agents, subcontractors or service providers of each such party.

Risk-Based Authentication (RBA): An Authentication system that takes into consideration the profile of the user requesting access to a system, as well as which system that the user is attempting to access, which determines the risk profile for that access attempt. The risk profile is then used to determine the nature of the challenge. Risk-Based Authentication allows the application to challenge the user for additional Credentials only when the risk level is appropriate.

Security Breach: A Security Breach includes:

- A contravention of the security policies, procedures or practices implemented by Ontario Health
- A contravention of the security provisions in agreements which Ontario Health enters into with external stakeholders and third-party service providers, including the security provisions in PHIPA agent agreements, data sharing agreements, confidentiality and non-disclosure agreements and agreements with third-party service providers retained by Ontario Health

Security Breaches can be intentional or inadvertent.

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.
Sponsoring Organization An organization (usually a Health Information Custodian) that has the right to access one or more Federated Service(s) for the purpose of delivering health care or to assist in the delivery of health care in Ontario.

Threat Risk Assessment (TRA): A process designed to identify and analyze threats and risks to I&IT processes, programs, infrastructure, and applications, leading to recommendations of appropriate safeguards to protect assets and information from loss, theft, destruction, modification, or corruption.

User ID: Electronic information comprising of a string of characters that uniquely identifies an End User in an information system.

Shall/Must: Used for absolute requirements, i.e., they are not optional.

Should: Used when valid reasons exist in certain circumstances not to implement the requirement; however, the implementer must understand the implications before choosing a different course and must consider implementing compensating controls.

May: The requirement is only a recommendation, or provided as an implementation example and is not intended on being exhaustive.

Standard Requirements

1. Accreditation

1.1. Accreditation Requirements

During the accreditation process, Ontario Health will review the Identity Access Management System (IAMS) of the IDP.

The IDP must:

- Attest that it has the necessary authority, personnel and technical resources necessary to provide IA Services
- Assist in Ontario Health review by providing the documentation or other information required
- Advise Ontario Health of any changes to its IAMS and Registration or Authentication policies, practices, processes or technologies
- Agree to comply with and assist Ontario Health in complying with all Applicable Laws and Regulations, such as the PHIPA and the FIPPA
- Agree to comply with all applicable agreement(s)
- Respond to any recommendation made by Ontario Health or its delivery partners for remedial action to address any gaps identified by its reviews
- Designate one or more Representatives to liaise with Ontario Health.

1.2. Exemptions

In exceptional cases, an IDP may request an exemption from one or more requirement(s) in this Standard in writing to Ontario Health, which must state the reason(s) for the request. All requests shall be submitted to Ontario Health prior to the IDP providing or continuing to provide any IA Services. All requests shall be reviewed and must be approved by the appropriate stakeholder(s). Ontario Health shall work with the IDP and may make a recommendation(s) that would bring the IDP into compliance. Such recommendation(s) may be subject to conditions, including requiring that compliance be achieved within a time period that is determined by Ontario Health, in accordance with the agreement between Ontario Health and the IDP.

If the IDP does not implement the recommended changes or does not implement the recommended changes in accordance with any stated condition(s), Ontario Health shall:

- Not accredit the IDP; nor
- Undertake such other measures in accordance with the agreement between Ontario Health and the IDP.

1.3. Additional Information

Ontario Health may collect, record, use or disclose information for the purposes of Registration and/or Enrolment into any Federated Services, so as to reflect, for example, changing business needs or to comply with applicable Laws and Regulations.

1.4. Changes to an Accredited IAMS

The IDP must notify Ontario Health of any subsequent changes to an IAMS that Ontario Health had accredited and to any of its Registration or Authentication policies, practices, processes or technologies, in accordance with the terms of the agreement(s) with Ontario Health or as soon as reasonably practicable, and prior to implementing any changes where they may require Ontario Health approval.

1.5. Repeated Review(s)

Ontario Health may repeat all or part of the accreditation review as required, for reasons including their modification or to audit for compliance with any Federation policy or standard.

Ontario Health shall conduct or repeat a review if, at any time, it is advised, suspects or otherwise detects that significant changes have been made to an IAMS or the Registration and Authentication policies, practices, processes or technologies of an IDP.

1.6. Termination

The use of an IAMS may be terminated by Ontario Health or an IDP with reasonable notice, in accordance with the terms of the agreement(s) between them.

2. Suspension and Revocation

2.1. Suspension

2.1.1. General Suspension Rules

The IDP may suspend an account if:

- Information is discovered or revealed suggesting a reasonable likelihood that the information, documentation or any other matter provided or done to establish the Registration was misleading, false or fraudulent;
- An End User has failed to comply with any Federation policy, standard, agreement or the terms and conditions of any Federated Service; or
- The suspension is requested by an IDP or End User for any reason (e.g., leave of absence).

Please also see requirements on suspending accounts when passwords remain unused for the periods specified in section 4.3.4.

2.1.2. Emergency

Ontario Health reserves the right to immediately suspend access to Federated Services by an End User if it reasonably believes that there is an emergency or other circumstance that would warrant such action, including but not limited to a compromise of the Federated Services or the integrity of data therein.

2.1.3. Reactivation

An account that has been suspended by the IDP due to possible misleading, false or fraudulent information must not be used or reactivated unless it has been confirmed that the relevant information, documentation or other material facts are true, accurate and complete.

2.1.4. Documentation

The IDP must document and retain a record of the reason(s) for:

- A suspension
- Any resulting actions taken
- Details of any investigation

2.2. Revocation

2.2.1. General Revocation Rules

The IDP must revoke the account of an End User if:

- The individual no longer needs the account (e.g., he/she is deceased; has resigned or retired);
- It is determined that the account concerned is a duplicate;
- It is determined that the information, documentation or any other matter provided or done to establish the Registration was misleading, false, or fraudulent; or
- The identity has been otherwise compromised (e.g., identity theft).

The IDP may revoke the account of an End User upon request by that End User for any reason.

2.2.2. Documentation

The IDP must document and retain a record of the reason(s) for:

- A revocation
- Any resulting actions taken
- Details of any investigation

3. Registration and Entitlement

3.1. Establishing and Maintaining Local Registration Authorities

Each HIC must ensure that a Legally Responsible Person (LRP) or their delegate identifies at least one or more persons to act as a Local Registration Authority (LRA) to manage the enrollment of its agents and Electronic Services Providers who require access to Federation Services.

The LRP must ensure that a new LRA:

- Has the time and resources required to perform the duties;
- Is stable in his or her current position (not subject to reassignment);

- Meets Level 2 assurance(see section 3.4) qualifications according to the Federation Identity Provider Standard; and
- Understands the importance of policy adherence, especially privacy and information security.

3.1.1. Modifications

Modifications to the status of an approved LRA may be based on a request from the LRP, or at the discretion of the Registration Authority (RA) if it is suspected or discovered that the LRA is non-compliant with relevant policies, procedures or agreements. If the status of an LRA is revoked or suspended, the LRP must submit a request to lift the suspension before the status may be reinstated.

3.1.2. Documentation

Ontario Health or its delegate, acting as a RA, must maintain a copy of all requests to approve, suspend or revoke a person's status as LRA.

3.2. General Registration Rules

The IDP must validate the identity of End Users or their own Representatives during Registration and before issuing Credentials.

The IDP may determine their respective Registration requirements for End Users. However, at a minimum, the IDP must:

- Validate the Core Identity Information set out in section 3.2.1;
- Ensure the method(s) used attain(s) the required Level of Assurance; and
- Ensure that each individual being Registered:
    - Is 16 years of age or older
    - Presents sufficient information to validate identity and positively 'Authenticate' the individual upon subsequent access requests to Federated Services

The End Users must present two pieces of identification, at least one identity document that contains a photograph bearing a true likeness of the End User (see section 13 for a list of Primary Documents and Secondary Documents that are currently accepted for Registration).

However, this would not be required where a prior direct or personal interaction between the IDP and the Registrant has taken place to validate the individual's identity and the IDP has records to support this. In addition, the IDP must not accept a Health Number from any province, including Ontario, or a Social Insurance Number to confirm individuals' identities for Ontario Health products and services, including Federated Services.

In addition, the IDP's Registration requirements are expected to be of comparable or greater stringency than ONE®ID requirements. For further information, please refer to the Ontario Health ONE® ID Policy and associated standards.

Special requirements for Patient Access to Patient Portals/Applications

Identify Validation

1. Patients must register for access in person. Where required, remote registration can be permitted and must be done only over a secure video application (i.e., Skype or WebEx).

2. Under special circumstances (e.g., patient out of the country, extreme illness, excessive travelling distance), registration over the phone is permitted. Users must correctly answer at least the following 6 questions:

    - Date of Birth
    - Address and Postal Code
    - Health Care Number (HCN)
    - Name of Family Doctor
    - Name of Emergency Contact
    - Name of Next Kin

3. Patients must be 14 years of age or older in order to register for an account to access their own medical records.

4. Using a Health Card with a photo is an acceptable Primary ID for a patient to register for access to a Patient Portal/Application.

Self-completion phase of Registration

5. Upon a successful identity validation, the patient may receive a PIN for self-registration purposes. The PIN:

    - Must be unique, random and at least six characters long
    - Requires no complexity
    - Is valid only for 30 days; beyond that, PIN regeneration is require

6. The patient portal/application must prompt patients to provide at least the following information when completing the self-registration phase:

    - PIN
    - Date of Birth
    - Patient's Medical Record Number (MRN)

Substitute Decision Maker (SDM) Access to a Patient's Record

7. Where a Substitute Decision Maker requests access to a Patient's record, the following documentation must be provided in person:

    - A fully filled and signed delegate form provided by [the EHR Solution] Program Office.
    - One identity document that contains a photograph bearing a true likeness of the SDM (see section 13 for a list of Primary Documents and Secondary Documents that are currently accepted for Registration).
    - Supporting documentation such as a long-form birth certificate, power of attorney documents, will and death certificate, or other acceptable court documents.

Note: For auditing purposes, the application must capture and store data on confirmation of identity verification, the provider who performed the identification, and any supporting documentation.

3.2.1. Core Identity Information

The following is the Core Identity Information the IDP must collect in order to Register an End User:

- Legal name (The End User's first name and last name are mandatory fields. The IDP may enter a null value as an End User's middle name)
- Where applicable, all professional designations and license numbers of the individual

Where the organization leverages the ONE ID Provincial 2 factor authentication service the telephone number of the End User must be recorded and maintained securely.

3.3. Assigned Information

During Registration, the IDP must assign every End User the following:

- A unique User ID (see below);
- The information required to set and maintain credentials (see section 4.2); and
- A Level of Assurance (e.g., AL1, AL2, AL3) during the Registration of each End User corresponding to the rigours of the Registration process involved and the strength of the evidence offered to support the identity.

The IDP must ensure that End Users are assigned a User ID that uniquely identifies the End User within the Federated System.

User IDs must be in a format approved by the IDP.

NOTE: ONE®ID's standard format of User IDs for individuals is:

- [preferred firstname].[preferred lastname]@[ONEID.on.ca], e.g., John.Doe@ONEID.on.ca

3.4. Levels of Assurance

3.4.1. Definition

A Level of Assurance refers to the level of confidence that can be placed in an identity claim. The Level of Assurance required for access to a Federated Service is determined by Ontario Health based, among other things, on Application Providers' business requirements and the applicability and appropriateness of the identity requirements corresponding to different information classification, as set out below:

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. AL1 is insufficient when Personal Health Information (PHI) or Personal Information (PI) is accessed.	An unverified identity: An individual supplies all identification information, which is taken at face value. No assurance needed as to the veracity of the identity claim.
AL2	AL2 is appropriate for information that has a high sensitivity level within Ontario Health and 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 identity claim is verified with documentary evidence, 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 Ontario Health and the health sector environment. This information is intended for use by named and authorized individuals only. To decide whether an AL3 is required, Ontario Health and Application Providers 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 the identity claim is verified and corroborated with an authoritative source(s) (e.g., the issuer of the documentary evidence presented).

The IDP should consult the ONE® ID Identity Assurance Standard for further requirements relating to Levels of Assurance.

3.4.2. Minimum Level of Assurance

Ontario Health typically requires all End Users' electronic identities to attain a minimum of AL2 in order to access Federated Services with PI or PHI. Accordingly, the IDP must be capable of Registering and Authenticating End Users to AL2, at a minimum.

Where an AL3 is required, the IDP must implement more rigorous Registration or Authentication measures such as:

- Setting more stringent requirements for End User Credentials
- Requiring a greater number of Authentication factors

Access to some Federated Services may require End Users to be provisioned with access to other Federated Service(s). When multiple Enrolments are required, an End User's AL must be greater than or equal to the highest AL required by the Federated Services.

3.5. Process Requirements for AL3

Identity must be corroborated where an AL3 is required. Identity corroboration may either be by:

- Direct verification by an Authoritative Party (e.g., Vital Statistics Agency, Revenue Canada); and/or
- A trusted third-party professional (e.g., lawyer, doctor, minister)

It may also involve the exchange or confirmation of shared secrets—information that is known by the corroborator about a potential Registrant. For example, as in the passport model, a third-party may be required to confirm the length of time a potential Registrant has continuously resided in Canada.

Authoritative Parties

Some examples of Authoritative Parties accepted by Ontario Health are listed below, corresponding to the categories of End Users:

- Employees (e.g., the employer or a Canadian Police Information Centre (C.P.I.C.) check during the hiring process)
- Corporations (e.g., a Corporate Registry)
- Doctors (e.g., the College of Physicians and Surgeons)
- Citizens (e.g., the Vital Statistics Agency, Citizenship and Immigration, Revenue Canada or Revenue Quebec)

If in doubt, the IDP is advised to consult Ontario Health on whether a third-party would be accepted as an Authoritative Party for the purpose of identity corroboration.

3.6. Documentary Requirements

To Register at AL2:

- All identity documents must contain a photograph of the End-User
- Professional Designation(s) & License Number(s) (where applicable)

To Register at AL3:

- All identity documents must contain a photograph of the End-User
- A copy of the identity document must be taken and retained on record
- Professional Designation(s) & License Number(s) (where applicable)
- End-Users must sign their Registration application with a handwritten signature

3.7. Account Creation and Management

3.7.1. Account Listing

The IDP must maintain a list of assigned accounts used for consuming Federated Services for each End User, including the name of the authorizing personnel. Such information must be made available to Ontario Health upon request or during an audit.

3.7.2. Resolving Duplication

An apparent duplication means a full match on all Core Identity Information (see section 3.2.1). The IDP must have processes in place to identify and resolve apparent duplications, such as:

- Referring the issue to the Health Information Custodian under whose delegation or authority the End User accesses or uses Federated Services; or
- Confirming or requesting additional information or evidence from the End User.

3.8. Managing Entitlements

3.8.1. Assigning a Sponsor

The Legally Responsible Person (LRP) must identify a named person(s), group(s), or the role(s) that has the authority to act as a Sponsor.

3.8.2. Entitlement Criteria

Access to applications and services vary based on the entitlement criteria of the data and application owner(s).

Some applications and data permit access for research while others prohibit access for research. Some applications are specifically for use by technical administrators. Please refer to the Ontario Health Entitlement Management Procedures Manual for requirements to enrol End Users into applications and services.

- If an agent or Electronic Service Provider has multiple roles, e.g., is both a clinician and a risk manager, the Sponsor may assign that person with access to [the EHR Solution] for the purposes of collecting PHI for providing or assisting in the provision of health care and must ensure that the end-user understands their permissions and obligations
- Once access to [the EHR Solution] has been revoked, agents or Electronic Service Providers must re-enroll in order to have their access to [the EHR Solution] reinstated

Documentary Requirements

- Name of the authorizing person Sponsoring the Entitlement

3.8.3. Review of Accounts

- A review of all active accounts and enrollments to the Federation Services must be completed at least an annually

- The review should be coordinated with the authorized Sponsor to ensure that all account access is appropriate and up-to-date
- Where discrepancies are found timely actions to rectify access privileges must be implemented
- Accounts that have not been used in more than 180 days must be suspended
- For Patient Portals/Applications only, the patient must be notified that his/her account has been inactive for 365 days or more and take appropriate action; if no response from the Patient, his/her account will be suspended

3.9. Retention and Subsequent Changes of End User Information

The IDP must keep a record of End User Information, as well as any subsequent changes made to this information. The IDP must retain its records of End User Information permanently and must transfer this information to Ontario Health in accordance with the agreement between it and Ontario Health. Permanent retention is required because it cannot be determined in advance when an access request may be made or a breach investigation may occur. End-User Information would be required in either case to tie accounts to End Users' real-world identities.

What Is Recorded	Record Details (Minimum)	Retention Period
End-User Information	• User ID (Provided the User ID is an anchor (unchangeable and unique) attribute that does not change over time. If it is not an anchor attribute, a record of another anchor attribute must also be retained. In other words, the record must either show the association between the End User's real-world identity and an unchangeable, unique electronic identity at any given point in time or it must indicate all changes (if any) that the End User's electronic identity undergoes) • Legal First Name • Legal Last Name • Professional Designation(s) & Licence Number(s) • Level of Assurance the IDP has assigned (section 3.4); • Telephone number when the Provincial 2-factor authentication service is used. • Modifications to any of the above fields (including the From and To values, who made the change and when)	Permanent

See also section 9.2 for audit logs retention requirements.

4. Authentication

4.1. Authenticating Factors

Single-factor Authentication may be used when accessing the Federated System from a secure environment (e.g., using the Health Service Providers Managed Private Network). Single-factor Authentication would not be appropriate in all situations, such as when AL3 is required (see section 3.4).

Within the Federation, Authentication must involve two or more factors when Federated Services are accessed from:

- The Internet or unsecured environments/locations;
- A point-of-service application, such as a hospital Information System (HIS), if the user is remote (not on site); or

- Where any Privileged function is being accessed, e.g., system administrator.

Strong Authentication typically involves the use of a strong password (see section4.3.2) combined with a second factor. Examples of second-factor technologies include hard security tokens, callbacks, SMS messages, Risk-Based Authentication, one-time passwords, machine certificates, biometrics and personal certificates.

However, certain Federated Services may require the use of specific type(s) of second factors, e.g., hard security tokens. In such cases, the required type(s) of second factors must be implemented in order to access the Federated Services in question.

The above principles regarding two-factor Authentication apply whenever Federated Services are accessed from browsers on portable electronic devices (e.g., smartphones, tablets).

Special requirements for Patient Portals/Applications

The requirements for multi-factor authentication continue to apply to Patient Portals/Applications by default. To accommodate users, patient can be given the option to disable/opt-out of multi-factor authentication during or after registration.

4.2. Challenge Questions

Where the IDP chooses to use Challenge Questions for Authenticating End Users, they must have processes and policies in place, such as:

- Requirements on the nature or number of questions permitted or required
- Storage and transmission of answers to Challenge Questions
- End Users' rights or obligations to set or change their Challenge Questions

In addition, the IDP' IAMS must ensure that:

- End Users are prohibited from setting their own Challenge Questions (e.g., End Users must select from a pre-defined list instead)
- Challenge Questions are connected to or affiliated with the Registration record of the respective End Users
- Unauthorized persons are prevented from seeing or changing End Users' Challenge Questions

For the purpose of Authentication during login, the use of Challenge Questions is permitted only where they are used in conjunction with:

- Risk-Based Authentication mechanisms (e.g., device recognition)
- Heuristic tests (e.g., verifications of IP address or browser identity)

Follow the link for more information regarding the ONE ID Challenge Question Standard.

4.3. Credential Management

Credentials include passwords, challenge questions and where the provincial 2-factor authentication services are used, the telephone number of the user is considered a credential and must be securely managed.

4.3.1. General Requirements

The IDP is responsible for implementing appropriate measures to distribute, maintain and protect credentials. The IDP must have a comprehensive credential management policy to ensure passwords of sufficient strength and complexity are used.

4.3.2. Creating Passwords

The following requirements apply to passwords that may be used to 'Authenticate' users accessing Federated Services.

- The IDP must enforce strong passwords, which must:
    - Be at least 8 characters, with a maximum not less than 64 characters long; and
    - Include characters/digits from at least three of the following conditions of complexity:
        - At least 1 uppercase character (A through Z)
        - At least 1 lowercase character (a through z)
        - At least 1 numerical digit (0 through 9)
        - At least 1 non-alphanumeric character (~!@#$%^&*_-+=' |\(){}[]:;"'<>,.?/)

To permit no complexity, live screening of new passwords must be completed and displayed to users during password creation. Live screening must be done against a list of commonly used passwords: blacklist, dictionary, usernames, service names, sequential strings, and passwords from previous breaches.

- Password history should prevent reuse of the last 5 passwords
- Where technology permits, passphrases must be used (e.g., 24SussexDrive) instead of a (typically shorter) password
- Where technology permits, software that prohibits the use of recognizable patterns must be used
- Passwords must not include all or part of the End User's first/last names or any easily obtained personal information (e.g., names of family members, pets, birthdays, anniversaries, all or part of a Login ID or a commonly known nickname)
- Initial or temporary passwords must be unique, not guessable and must follow this Standard regarding password strength

4.3.3. Passwords Distribution

- An initial password should be generated by an automated service and issued directly and securely to the End User (e.g., in person, by mail, telephone or encrypted email)
- The IDP must ensure that the passwords are communicated to the intended End Users (e.g., they must be mailed to a confirmed postal or email address or a wire-line phone number of record)
- The password distribution process must be auditable
- Systems passwords must not be given to staff or contractors who have not signed a non-disclosure agreement or who are otherwise not authorized to receive such information

4.3.4. Administering credentials

- The IDP must first validate End Users' identity before issuing any credentials for accessing Federated Services
- The IDP may choose its Authentication method(s), provided they are properly documented, i.e., by contacting the IDP' service desks, which after validating an End User's identity using information that only the End User should know (e.g., Challenge Questions), will issue a temporary password to the End-User
- Helpdesk functions that assist in access control, especially credential resets, must not allow the personnel to see, hear or know End User temporary passwords
- System administrators with global rights must not perform the function of creating and maintaining End User credentials
- Old credentials must not be released to End Users
- The briefest possible explanation must accompany a denial of access when a password does not conform to rules for the creation and/or change of passwords. The message should provide contact information for End User assistance (e.g., "access denied – contact your system administrator")
- Access must be denied after five consecutive incorrect password attempts, for a duration of at least 30 minutes. The IDP shall record access denials due to the entry of five consecutive incorrect password attempts in an audit or system log, which must be reviewed and where warranted, investigated in accordance with monitoring and escalation procedures that the IDP has established approved and/or in accordance with the terms of the agreement(s) between the IDP and Ontario Health

4.3.5. Password Display

- An IAMS must not display or echo the characters of a password on output devices or while being entered but may be represented on the screen by special characters such as asterisks. Temporary visibility of passwords is permitted depending on technology limitations.

4.3.6. Password Expiration

- Permanent passwords for accessing Federated Services must expire after 90 days of their issuance or modification. Up to one year is permitted where the IDP is in compliance with the other supporting password controls outlined in the EHR Security Policies and IDP Standard
- Once a password has expired, access to Federated Services must be suspended until a new password is created

4.3.7. Changing Credentials

- An IDP must provide a secure mechanism for End Users to change, recover or reset their credentials (e.g., where an End User has been locked out or has forgotten his or her password)
- The IDP shall require End Users to change their initial passwords on first use (if not set by the End User)
- The credential reset process must include strong positive Authentication of the requester so that it can be performed for any End User who is not visually identifiable, (e.g., requests via the telephone)

4.3.8. Password Storage

- When password lockers/storage software is implemented, these products must require strong passwords and secure authentication and transmission
- When applicable automated login by password locker must be authenticated by a strong password (or biometrics when possible)
- Unsecure login methods such as macros scripts, screen scraping, function keys are not permitted
- Browsers must not be used to store, autofill, cache passwords or any other forms fills

4.3.9. Phone Challenge

- A Provincial Two Factor Authentication is offered as part of the risk-based authentication interdiction method and as such, the phone challenge may be bypassed (if a recognized device) or the user may be denied access (if a risky IP or device) based on rules of the service
- Identity providers are responsible for determining when a user requires a challenge before allowing access to EHR. E.g., for remote users rather than for users physically within the four walls of the organization. Identity Providers must use the authentication service only when necessary to access EHR assets

4.3.9.1. Phone Number Management

- Identity Providers must capture and maintain securely the telephone numbers passed to the Federation Broker for the purpose of authenticating their users
- Identity Providers must provide telephone numbers that are not shared or go through a switchboard. Note that initially at least, extensions, IVRs and TTYs will not be supported
- Identity Providers must ensure they are permitted to provide users' telephone numbers for authentication purposes
- Identity Providers must have mechanisms in place to manage the accuracy of the telephone numbers that are passed to the Federation Broker and updating them

4.3.9.2. Do Not Call List

- Ontario Health maintains a 'do not call' list set of telephone numbers and may reject a telephone number sent by the Identity Provider should it appear on this list
    - As an example if may contain, phone numbers such as 1-900 numbers

5. Identity Assertions and Attributes

The IDP must ensure the accuracy of all assertions and comply with requirements in the Specifications. The IDP is liable for any inaccuracy in the identity assertions it submits to Ontario Health or other Federation members.

User IDs issued to End Users by the IDP must be sent as assertions in the acceptable format (see the Specifications) to Ontario Health or other Federation members to be captured in a central repository that will be hosted at and managed by Ontario Health.

In the event that the IDP becomes aware of an assertion of inaccurate attributes, the IDP must:

- Notify Ontario Health immediately by contacting the Ontario Health Service Desk at 1-866-250–1554 as this may have implications of a Privacy Breach or Security Breach

- Take whatever action is necessary to correct the inaccuracy
- Follow recommendations and direction from Ontario Health if provided
- Give notifications as required pursuant to the terms of the applicable agreement(s)

Where the IDP makes repeated assertions of inaccurate attributes, Ontario Health may suspend the use of the IDP's IAMS and/or revoke the IDP's accreditation, if the IDP fails to remedy such deficiencies within the cure period specified by Ontario Health. Ontario Health shall provide reasonable assistance to the IDP in order to remedy such deficiencies.

6. Notice of Acceptance to End Users

The IDP must implement access control systems or procedures that:

- Provide End Users with a written statement of their access rights and responsibilities (e.g., delineate rules relating to the kinds of data, files or information that could only be accessed by specified personnel)
- Require End Users to indicate their acceptance of disclosed access rights and responsibilities

7. Suspended, Expired or Revoked Credentials

The IDP must deny authentication from End Users with suspended, expired or revoked Credentials

8. Transmitting Credentials

The IDP must create a session key to Authenticate subsequent data transmission in the same session.

9. Logging Transactions

9.1. Minimum Content of Audit Logs

The IDP must keep audit logs that contain at least the following information:

- Authentication (The audit log must be able to associate the action performed with the individual who had performed the action.)
- The User ID (Provided the User ID is an anchor (unchangeable and unique) attribute that does not change over time. If it is not an anchor attribute, a record of another anchor attribute must also be retained. In other words, the record must either show the association between the End User's real-word identity and an unchangeable, unique electronic identity at any given point in time, or it must indicate all changes (if any) that the End User's electronic identity undergoes)
- Authentication outcome (e.g., failed/successful)
- Authentication data (e.g., type of challenge used and Authentication-related details)
- A date and time stamp

Ontario Health is required by law when acting as Health Information Network Provider (HINP) to take steps that are reasonable in the circumstances to keep an electronic record of all accesses to all or part of the personal health information contained in the electronic health record, and to ensure that record identifies the person(s) who accessed the information and the date, time and location of the access. Where required, the IDP shall assist Ontario Health in fulfilling this regulatory requirement.

9.2. Retaining Audit Logs

The IDP must retain audit logs of:

- Authentication events 60 days online and 24 months minimum in the archive;
- End Users' Credentials information permanently; and
- Events relating to its IAMS for 60 days online and 24 months total in the archive. See the EHR Security Logging and Monitoring Standard for more details.

The IDP must retain its audit logs for the periods set out in this section and must transfer this information to Ontario Health in accordance with the agreement between it and Ontario Health. Audit logs would be required in either case to tie accounts to End Users' real-world identities. The requirements for audit logs are summarized below:

What Is Recorded	Record Details (Minimum)	Retention Period

Authentication Events	• User ID
	• Authentication outcome (e.g., successful/failed);
	• Authentication data
	  ○ Type of challenge used, e.g., knowledge-based Authentication, Phone Challenge or RSA token
	  ○ Authentication-related details, e.g., End User successfully passed the challenge on the second attempt)
	• Date and time stamp
		60 days online
		24 months total in archive

End-User / Credential Information	• User ID • End Users' Credentials (e.g., serial numbers of tokens assigned to End Users) • Legal First Name • Legal Last Name • Professional Designation(s) & Licence Number(s) • Name of the authorized person (i.e. Sponsor) • Level of Assurance the IDP has assigned (section 3.4); • Modifications to any of the above fields (including the from and to values, who made the change and when) • Modifications to Credentials (e.g., password resets, changes to Challenge Questions or answers, resets to token PINs) ○ Updates to Phone Challenge including Date updated, who updated the phone number, from and to values.	Permanent
IAMS Events	All events that take place in the IDP's IAMS in connection with an Authentication event with the Federated System, such as:	60 days online 24 months total in the

What Is Recorded	Record Details (Minimum)	Retention Period
	• Who accessed and when (e.g., system administrators, operators and similar roles) • What he/she did during the access • What monitoring alarms were triggered and when. The events in this category exclude the items under "Authentication Events" or "Credential Information". See: EHR Security Logging & Monitoring Policy	archive
Identity Assertions (SAML Responses the IDP sends to the Federation Operator)	Not required	Not applicable

9.3. Continuously Logging

The IDP must ensure that audit logging is operational at all times. Registration, modification of Registration information or Authentication must not be performed if audit logging is not functioning.

9.4. Securing Access to Audit Logs

The IDP must secure access to audit records and logs and safeguard access to system audit tools to prevent misuse or compromise.

The IDP must implement appropriate security measures to protect audit records and logs from being tampered with, such as:

- Implementing segregated network segments with appropriate access controls; or
- Directing audit logs to a Security Information and Event Management (SIEM) system.

10. Customer Support

10.1. Hours of Operations

The IDP Services must be available 24 hours a day, 7 days a week.

For IDPs using the Provincial Two Factor Authentication service, service desks must be equipped to handle calls from impacted users and have the ability to correct issues 24 hours a day, 7 days a week, e.g., modify the telephone number quickly and securely. This may include implementing an appropriate error handling process for errors that occur during the challenge, for example, a user cannot complete the challenge because their phone cannot get a signal.

Where IDPs are using the Direct call method of the Provincial Two Factor Authentication, they must have the ability to monitor failed OOBA challenges and take appropriate action if required.

10.2. Customer Service Representatives

The IDP must Register and Enrol personnel responsible for performing End Users' Registration and Authentication and to assist End Users with issues related to its IA Services, within the scope of authority delegated by the IDP.

When required, the IDP is also expected to transfer calls to and receive calls from the Ontario Health Service Desk or those of other Federation members.

10.3. Level of Assurance

Representatives for the IDP must be Registered at AL2 or above. The IDP' Registration agents cannot Register End Users at a Level of Assurance that is higher than their own Level of Assurance, regardless of the number of identity documents presented by the End User or the type of identity validation performed.

10.4. Access to Information

The IDP must provide their Representatives with access to only the information required to carry out their assigned duties.

10.5. End-User Authentication

The IDP must authenticate individuals who contact their Representatives through well-defined processes. At a minimum, the IDP must require individuals to present evidence of identity that is equivalent to that required at initial Registration or information that only the End User should know, e.g., Challenge Questions.

References

- Development Corporations Act, R.S.O. 1990, Chapter D10 Ontario Regulation 43/02 as Amended to Ontario Regulation 54/05
- Freedom of Information and Protection of Privacy Act
- GO-ITS Number 25.13 Security Requirements for Internet Web Applications (Version 1.2), 2009-03-26
- GO-ITS Number 25.00 – General Security Requirements
- Government of Ontario Corporate Policy on Electronic Identification, Authentication and Authorization (IAA): Ministry of Government Services (July 2012)
- ONE® ID Challenge Questions Standard
- ONE®ID Identification Information and User Name Standard
- ONE® ID Identity Assurance Standard
- ONE® ID Password Standard
- ONE®ID Policy
- Personal Health Information Protection Act, 2004 (PHIPA)
- Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (PIPEDA)

Ontario Health EHR Policy Documents

- Information Security Policy
- Acceptable Use of Information and Information Technology Standard
- Access Control and Identity Management Standard for System Level Access
- Local Registration Authority Procedures
- Identity Federation Standard
- Business Continuity Standard
- Cryptography Standard
- Electronic Service Providers Standard
- Information Security Incident Management Standard
- Information and Asset Management Standard
- Network and Operations Standard
- Security Logging and Monitoring Standard
- Systems Development Lifecycle Standard
- Physical Security Standard
- Threat Risk Management Standard

Appendix A: Acceptable Identity Documents

Primary and Secondary Identity Documents for ONE®ID

This section provides a list of documents that ONE®ID currently accepts as primary or secondary documents. Primary documents provide more stringent proof of identity; secondary documents are issued by an institution that has been approved by Ontario Health.

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 a Canadian Province (Certified Copy)
17	Immigration Canada – Refugee Claimant ID Document
18	Ontario Photo Card
19	Ontario Health Card with photo (Only for patient registration to a Patient portals/applications)

Secondary Documents

Acceptable Secondary Identity Documents	
1	Any document listed as an Acceptable Primary Identity Document except for the Primary Identity Document being recorded.
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 from a Sponsoring Organization
15	Union Card
16	Other Federal ID Card, including Military
17	Ontario Ministry of Natural Resources Outdoors Card
18	Student Identification Card
19	BYID Card (Formerly Age of Majority Card)
20	CNIB Photo Registration Card
21	Identification Card issued under the Blind Persons Rights Act
22	Any document listed as an Acceptable Primary Identity Document except for the Primary Identity Document being recorded.
23	Old Age Security Card

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 (Ontario Health Card with photo is allowed for patient registration to Patient portals/applications)
2	Social Insurance Cards