eHealth Ontario
It's working for you

Identity Provider Policy

Identity and Authentication Services (IA Services)

Ontario
eHealth Ontario

Table of Contents

1 Background

1.1 eHealth Ontario Identity Federation

1.1.1 The eHealth Ontario Identity Federation ("**Federation**") managed by eHealth Ontario (the "**Agency**") is a network whose members either provide or access electronic health services ("**Federated Services**") over the Agency's **Federated System –** a technology infrastructure comprising applications, systems, registries, databases, files, portal applications and tools.

1.1.2 The Agency's ONE® ID Program is the Federation Operator of the Federation – a "broker" that relays End Users' access requests for Federated Services, together with their Identity Providers' (**IDPs**) identity validations, to enable Application Providers to make informed Authorization decisions.

1.2 Purpose

1.2.1 This Policy sets out:

a) Accreditation requirements for IDPs;

b) Minimum standards for the Identity and Authentication Services ("**IA Services**") accredited IDPs provide to End Users; and

c) Operational policies relating to the access and use of Federated Services, including:

- End User responsibilities;
- Monitoring and compliance provisions; and
- Privacy and security requirements.

1.3 Objectives

1.3.1 This Policy helps to ensure that:

a) Accountabilities and responsibilities for Registering and Authenticating End Users for accessing Federated Services are identified.

b) IA Services attain defined standards, so that End Users are Registered and Authenticated:

- Using consistent, well-defined, reliable and secure processes; and
- To the required Level of Assurance for the Federated Service(s) being accessed.

c) Privacy and security requirements are established to protect the Personal Information or Personal Health Information accessed through Federated Services.

1.4 Scope and Applicability

1.4.1 This document applies to all accredited IDPs and their Representatives.

1.4.2 This Policy establishes mandatory, minimum requirements for accredited IDPs and the IA Services they provide within the Federation.

1.5 Policy Exemption

1.5.1 The Senior Director, Identity, Access & Privacy, is responsible for ensuring compliance with this Policy.

1.5.2 In exceptional cases, an IDP may request an exemption from one or more requirement(s) in this Policy in writing to the Agency, which must state the reason(s) for the request. All requests shall be reviewed and approved by ONE ID Identity Services and Security Services leads.

1.6 Violations

1.6.1 Any violation of this Policy by an IDP or its Representatives is subject to the penalties contained in the contractual agreement between that IDP and the Agency. In addition, the Agency may also pursue any other remedy available pursuant to any applicable Laws and Regulations.

1.7 Terminology

1.7.1 This Policy follows certain wording conventions with precise requirements and obligations:

Shall/Must: This requirement is mandatory.

Should: The implementer must choose this action, unless business requirement(s) dictate(s) otherwise.

Exceptions must be approved by management, as modifications to the standard practice.

May: The implementer may choose to take one or more of a selection of options, but must make a choice of one or more, as dictated within the context of the item.

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

1.7.3 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”.

1.7.4 Words and terms in this Policy that have meanings differing from the commonly accepted definitions are capitalized and their meanings are set out in the Glossary.

2 Identity Provider Policies

2.1 Accreditation

2.1.1 To be accredited, the IDP must:

a) Be capable of validating End Users' identity to an AL2 or higher;

b) Enter into all applicable agreement(s) with the Agency; and

c) Have an Identity Access and Management System ("IAMS") and provide IA Services that, upon review by the Agency, are considered to meet the requirements of the eHealth Ontario Identity Federation - Standards for Identity Providers ("Standards") and, as applicable, the eHealth Ontario Identity Federation - [Federation Attributes Specifications] and [Federated Services Specifications] (collectively "Specifications").

2.1.2 If the IAMS or the IA Services provided by an IDP does/do not meet any requirement(s), the Agency may recommend changes that would bring it into compliance. If the IDP does not implement the recommended changes or does not implement the recommended changes in a manner that is satisfactory to the Agency, the Agency shall not accredit the IDP.

2.1.3 The Agency shall document a list of accredited IDPs and provide it to Federation members and End Users upon request.

2.2 Role and Responsibilities

2.2.1 The responsibilities of an accredited IDP include:

a) Identity validation (e.g., validating End Users' real-world identity and assigning to each a unique User ID);

b) Credentials management (e.g., issuing Credentials appropriate for a Federated Service's required Level of Assurance);

c) IAMS management (e.g. maintaining or upgrading its IAMS);

d) Policies and standards (e.g. establish and enforce IA Services-related policies and Identity Provider Standards that are consistent with the Agency's);

e) Compliance (e.g. observing all applicable Federation policies, standards, privacy and security guidelines, legal agreement(s) and applicable Laws and Regulations); and

f) Client Support (e.g. providing helpdesk support for End Users).

2.3 Registration

2.3.1 During Registration, the IDP must assign to each End User the following information, in accordance with the requirements set out in the Identity Provider Standards:

a) A unique User ID;
b) a Level of Assurance; and
c) The information required to set and maintain a password.

2.3.2 Generally, End Users must attain an AL2 or above in order to be authorized to access Federated Services, particularly where any Sensitive Information, including Personal Information or Personal Health Information, may be accessed therefrom.

The Standards should be consulted for further requirements relating to Levels of Assurance.

2.3.3 The IDP must ensure that all End Users agree to observe the Agency's Acceptable Use Policy when accessing Federated Services, as a condition for Registration.

2.4 Authentication

2.4.1 No interaction between the Federated System and an End User shall be permitted until an acceptable Authentication has been received by the Agency.

2.4.2 The IDP must establish Authentication processes to validate the association between an End User's Credential and real-world identity, in accordance with the requirements in the Standards.

2.4.3 The minimum mandatory information required for Authenticating End Users are set out in the Identity Provider Standards.

2.4.4 An Authentication method that involves the use of Challenge Questions must comply with the requirements in the Identity Provider Standards.

2.4.5 The Agency may, in its sole discretion, revise its accepted Authentication requirements upon giving the IDP written notice in accordance with the terms of the applicable agreement(s).

2.4.6 To facilitate portable access to Federated Services, the IDP should have the capability to Authenticate on different types of portable electronic devices (e.g., smartphones, tablets), as detailed in the Identity Provider Standards.

2.4.7 The IDP must ensure the accuracy of all electronic identities and attributes submitted to the Agency.

2.5 Customer Support

2.5.1 The IDP must have Registered and Enrolled customer service representatives to perform the tasks of Registering, Authenticating and assisting their client End Users, within the scope of authority delegated by the IDP.

2.5.2 The IDP's customer service representatives must be Registered at AL2 or above.

2.5.3 The IDP's customer service representatives shall be provided with access to only the information required to carry out their assigned duties.

2.5.4 Individuals who contact an IDP's customer service representatives must first be Authenticated through a process defined by the IDP, in accordance with the requirements set out in the relevant section(s) of the Identity Provider Standards.

2.6 Privacy

2.6.1 The IDP must only collect, use, retain and disclose information, including PHI or PI, for Registration or Authentication purposes, and only to the extent necessary for the purpose for which the information is collected.

2.6.2 The IDP must separate information collected for the purposes of Registration and Authentication from other information and must ensure this Registration and Authentication information is handled in accordance with the applicable agreement(s) and Laws and Regulations.

2.6.3 The IDP must provide a physical Privacy Impact Assessment to the Agency to facilitate the Agency's completion of any Privacy Impact Assessment(s) required.

2.6.4 The IDP must meet the requirements in the Agency's *Privacy Impact Assessment Policy*.

2.6.5 The IDP must comply with any risk treatment plans required by the Agency relating to the provision of IA Services. If the IDP does not implement the recommended changes or does not implement the recommended changes in a manner that is satisfactory to the Agency, the Agency may pursue such recourse as set out in its agreement(s) with the IDP.

2.7 Privacy Compliance Monitoring

2.7.1 The Agency may conduct privacy and data protection compliance reviews on the IDP on a basis and schedule proposed by the Chief Privacy Officer and Compliance Officer.

2.7.2 The Agency shall provide prior notice of a privacy and data protection compliance review in accordance with the terms of the applicable agreement(s) with the IDP.

2.8 Security Safeguards

2.8.1 The IDP must ensure that its IAMS and the IA Services it provides meet the requirements and Identity Provider Standards

2.9 Federation Standards

2.9.1 The IDP must comply with the Identity Provider Standards.

2.10 End Users

2.10.1 To be eligible for accessing any Federated Services, all End Users must:

a) be Registered and Authenticated by an accredited IDP;
b) receive from the IDP notification of the legal authority and purpose(s) for the collection, recording, use and disclosure of any End User information, including PI and PHI;
c) consent to the collection, recording, use and disclosure of Registration information; and
d) Agree to abide by the Agency's Acceptable Use Policy.

2.11 IDP Selection

2.11.1 End Users may choose the Agency's ONE®ID as their IDP for the purpose of accessing Federated Services.

2.11.2 Service Consumers may provide IA Services to their Representatives internally, provided they have been accredited as an IDP of the Federation. For instance, a hospital that had been accredited as an IDP within the Federation may provide IA Services to its staff to access Federated Services.

2.11.3 End Users may also choose their IDP from the list of IDPs accredited by the Agency. For instance, a physician seeking to access Federated Services may retain an accredited IDP to provide identity assertions on his/her behalf to the Agency, to confirm that the physician had been Authenticated.

2.12 Authorization

2.12.1 Application Providers are responsible for Authorization – they are entitled to determine whether to grant any End User access to Federated Services they offer, as well as the scope of their entitlements.

2.12.2 In accordance with the Identity Provider Standards, Application Providers may also determine the rule(s) by which End Users may be given access to any Federated Services they offer, including role-based access, e.g. granting End Users a level of access corresponding to the level of privacy and separation of privileges the Application Provider considers appropriate for each role.

2.12.3 The Agency shall enforce any Authorization rule(s) that are established by Application Providers.

2.13 Legal Agreement

2.13.1 The IDP must sign all applicable agreement(s) with the Agency prior to providing any IA Services. Applicable provisions of this Policy shall be addressed in any such agreement(s).

2.14 Suspension, Termination and Revocation

2.14.1 The Agency may suspend, terminate or revoke the rights of the IDP (including its accreditation status) or its Representatives found in violation of this Policy, in accordance with the applicable agreement(s).

2.14.2 The Agency shall provide notice of any suspension, termination or revocation in accordance with the terms in the applicable agreement(s) between it and the IDP.

2.15 Compliance

2.15.1 The IDP must provide IA Services in compliance with this Policy and with all applicable Laws and Regulations.

2.15.2 The IDP must establish, document and enforce its own policies, standards, processes or procedures that may be required to ensure compliance with applicable Identity Provider Standards.

2.16 Monitoring

2.16.1 The Agency may implement processes to monitor compliance with this Policy.

2.17 Audit

2.17.1 The Agency may audit compliance by an IDP on an on-going basis.

2.17.2 The Agency may exercise its rights under this section for purposes that include verifying compliance by the IDP with any applicable Federation policy, standard or agreement.

2.17.3 The IDP must provide such information, access and assistance as is reasonably required by the Agency for the purpose of conducting any audit. Specifically, the IDP shall allow the Agency and its Representatives to enter or inspect its premises, as well as any information, record or document in its possession or control, in accordance with the terms of the applicable agreement(s) between the IDP and the Agency.

3 Approval and Administration

3.1 Approval

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

3.1.2 This Policy shall be effective on the date of its final approval.

3.1.3 Enforcement of this Policy shall begin on the date of its final approval.

3.2 Administration

3.2.1 The Senior Director, Identity, Access & Privacy shall be accountable for and be responsible for administering this Policy.

3.3 Publication and notification

3.3.1 A copy of this Policy and related documentation shall be available in electronic format on the Agency website.

3.3.2 Notification of substantive changes or modification to this Policy shall be communicated to the IDP.

3.4 Interpretation

3.4.1 The Senior Director, Identity, Access & Privacy shall be responsible for the interpretation of this Policy, including the resolution of any dispute related to it.

3.4.2 The CISO / VP, Security Services shall be responsible for interpreting the security aspects of this Policy.

3.4.3 The Chief Privacy Officer shall be responsible for interpreting the privacy aspects of this Policy.

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

3.4.5 Each provision of this Policy and any relevant agreement pursuant to it shall be interpreted in such manner as to be effective and valid under applicable Laws and Regulations, including:

a) Ontario Regulation 43/02 amended to O. Reg. 339/08 made under the Development Corporations Act;

b) Personal Health Information and Protection Act, 2004 and Ontario Regulation 329/04 as amended; and

c) Freedom of Information and Protection of Privacy Act.

3.5 Organizational references

3.5.1 Where this Policy refers to any organizational body (division, committee, etc.) or position, the reference shall be interpreted to reference the successor body or position in the event of any organizational change.

3.6 Modification

3.6.1 This Policy may be reviewed annually and revised as needed. The IDP should periodically check the Agency's website for notice of modification to this Policy.

3.7 Contact Details

3.7.1 Information concerning this Policy may be obtained from:

ONE® ID Business Solutions
eHealth Ontario,
415 Yonge Street, Toronto, Ontario
M5B 2E7

Glossary

Term	Definition
Acceptable Use Policy	The Agency's requirements regarding acceptable use of the Federated System or the Federated Services, as modified from time to time and available at www.ehealthontario.on.ca.
Application Provider	An organization that provides one or more electronic health application(s) available for consumption through the Agency's Federated System as Federated Service(s).Federated Services
Authenticate or Authentication	Any process that validates the electronic identity of an End User against his/her real world identity.
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.
Challenge Questions	Questions that an End User is required to select from a drop-down list and answer during Registration, which are used subsequently to Authenticate that End User.
End User	An individual who is Authorized to access one or more Federated Service(s), usually as a Representative of a Service Consumer.
Enroll or Enrolment	The process of giving an End User access to specific Federated Service(s).
Federated Service	The electronic health services, resources and information that are accessible over the Federated System.
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' 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. the Agency

Term	Definition
Identity Provider (IDP)	An individual or organization who/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, 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 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.
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 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.
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.
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 Consumer	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	A process designed to identify and analyze threats and risks to I&IT

Term	Definition
(TRA)	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.

Reference and Associated Documents

Reference Document	Location
eHealth Ontario Acceptable Use Policy	http://www.ehealthontario.on.ca/pdfs/ProgramsFSs/AUP.pdf
eHealth Ontario Information Security Policy	http://www.ehealthontario.on.ca/pdfs/Privacy/Information_Security_Policy.pdf
eHealth Ontario Personal Health Information Privacy Policy	http://www.ehealthontario.on.ca/images/uploads/pages/documents/PHI_PrivacyPolicy.pdf
eHealth Ontario Personal Information Privacy Policy	http://www.ehealthontario.on.ca/images/uploads/pages/documents/PI_PrivacyPolicy.pdf
eHealth Ontario Privacy and Data Protection Policy	http://www.ehealthontario.on.ca/pdfs/Privacy/Privacy_Data_Protection_Policy.pdf
eHealth Ontario Privacy Impact Assessment Policy	Available on request
eHealth Ontario Privacy Policy on the Responsibilities of Third Party Application Providers	Available on request
Government of Ontario Corporate Policy on Electronic Identification, Authentication and Authorization (IAA): Ministry of Government Services (July, 2012)	Available on request

The following documents are associated with the policy and may be consulted for additional detail or policy interpretation.

Associated Document	Location
Ontario Regulation 43/02 amended to O. Reg. 339/08 made under the *Development Corporations Act*	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90d10_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
Personal Health Information Protection Act, 2004	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

Copyright Notice

All rights reserved

Trademarks