Briefing Note

ONE® ID CHAIN OF TRUST MODEL

INTRODUCTION

eHealth Ontario's identification, authentication and authorization (IAA) policy and process, known as ONE ID helps to protect the privacy and confidentiality of Personal Information (PI) and Personal Health Information (PHI) by providing a Chain of Trust which establishes the unique identity of End Users of the Agency's information infrastructure to a defined Level of Assurance.

The process involves the following basic requirements:

- Assigned Level of Assurance.
- Sponsorship
- Face to Face
- Information Requirements
- Identity Documents
- Authentication Credentials (username, password)

ONE ID is consistent with the equivalent Government of Ontario's Policy for Public Facing Electronic Identification, Authentication and Authorization.[1]

KEY ASSUMPTIONS

The security and privacy of Personal Information and Personal Health Information are fundamental to the Agency's mandate.

- The collection and use of PI by ONE ID to register healthcare practitioners who want access to eHealth Ontario's Services is governed by FIPPA.
- The collection and use of PHI by a service delivered to healthcare practitioners through the Agency's information Infrastructure is governed by PHIPA.

Regulation 329/04 of PHIPA requires that eHealth Ontario put in place administrative, technical and physical safeguards, practices and procedures to permit compliance with

[1] Government of Ontario, Ministry of Government Services, *Policy for Public Facing Electronic Identification, Authentication and Authorization*, Version 8.1, April 21, 2010.

PHIPA by HICs that use eHealth Ontario's services These practices and procedures must ensure the accuracy, completeness and currency of personal information and/or personal health information and guard against theft, loss, unauthorized use.

Ensuring accuracy and ascertaining that a person is who he/she says he/she is demands appropriate due diligence. It is incumbent on the Agency to do more than take one's word for their identity.

ASSIGNED LEVELS OF ASSURANCE (LOA)

Levels of Assurance are assigned to electronic service delivery systems according to the sensitivity of the information that is being accessed:

As Service Owners, Client Organizations negotiate and select the Level of Assurance that meets their business requirements for the Services that they provide through the Agency's information infrastructure. In making their selection, Client Organizations consider the applicability and appropriateness of the different Levels of Assurance.

ONE ID currently uses two levels:

- Assurance Level 1 used for non-sensitive, generally unclassified, and normally used for public information and internal communications.
- Assurance Level 2 used for sensitive information, including PI & PHI, that is intended for use by specific and identified users.

Asurance Level 2 requires a verified user to provide a verifiable identity which is checked using managed registration process and identification claim is verified with documentary evidence or through authoritative source(s).

SPONSORSHIP

Sponsors are responsible for the following:

- Attesting that Registrants meet the eligibility requirements to be registered or enrolled in an eHealth Service(s) for which the Sponsor has been given authority to act as a Sponsor.
- Confirming, verifying, supplying, and recording the information required for Registration and Enrolment in an eHealth Service to the Agency.
- Obtaining any necessary consents required by applicable Laws and Regulations before collecting, using, or disclosing the Personal Information or Personal Health Information of a Registrant.

- Informing the Agency if any Registrant sponsored by the Client Organization no longer (a) has a legitimate business requirement to be enrolled in any eHealth Service, or (b) meets the eligibility requirements.
- Validating that specific individuals are eligible and have a legitimate business requirement to be registered in the Information Infrastructure and enrolled in eHealth Service(s).

FACE-TO-FACE REGISTRATION

- The Registrant must be involved in the process, and present his/her supporting identity documents to the RA or LRA in a face-to-face interview, or the Sponsor may attest to the authenticity of the supporting identity documentation that is presented to the RA or LRA.
- The face-to-face requirement is basic to eHealth Ontario's commitment that its information infrastructure will maintain the security, privacy and accuracy of PI and PHI.
- The face-to-face encounter also enhances compliance with FIPPA's requirements to: (1) collect personal information from an individual only if it is done directly, and (2) not to use such personal information unless reasonable measures have been taken to make sure the information is accurate and up to date.
- Face to face encounters are standard for equivalent registration processes such as opening bank accounts, obtaining health cards and drivers licenses.

INFORMATION REQUIREMENTS:

- The minimum mandatory identification information required to register an individual is: legal name, gender, date of birth, and identity documentation/evidence.
- The Registrant must be 16 years of age or older.

IDENTITY DOCUMENTS

- The Registrant must provide two pieces of identification, one of which must be a government-issued identity document. The second document may be issued by any type of institution that is approved by eHealth Ontario. (A list of primary and secondary documents is issued by the Agency)
- At least one must include a photo of the individual
- Both documents must be current.
- The applicant must provide the RA or LRA with original versions or notarized photocopies of their identity documents.
- Both documents must show the first and last name of the individual.
- These documents must be reviewed and the numbers recorded by the RA or LRA.

AUTHENTICATION CREDENTIALS

- ONE ID Policy requires an End User to use a User ID and a Password to sign on to and access eHealth Ontario services.
- The User ID (Name) Standard applied by the Agency was developed to ensure that every Registrant has a unique User Name and that User Names are created using a uniform set of rules.
- Paswords and the System shall comply with the requirements of the ONE ID Password Standard.
- The use of authentication methods involving the collection of Challenge Questions from an End User shall comply with the requirements of the ONE ID Challenge Question standards.