eHealth Ontario

Ontario
eHealth Ontario

Privacy Frequently Asked Questions
For Local Registration Authorities

This list of frequently asked questions (FAQs) has been prepared to assist you in your role as an LRA. You may be asked to answer any of these FAQs by individuals who are registering or enrolling.

Information Collection

Q.	What privacy legislation is eHealth Ontario subject to?
A.	For the Personal Information that eHealth Ontario collects, it is subject to the Freedom of Information and Protection of Privacy Act (FIPPA), R.S.O. 1990, c. F.31.

Q.	Does eHealth Ontario have a privacy and security policy?
A.	Yes, eHealth Ontario has put in place suite of privacy policies for the protection of personal and personal health information. The policies include Privacy and Data protection policy as well as Personal Information privacy policy. The full set of policies can be viewed on our website at http://www.ehealthontario.on.ca/en/privacy Our security program is built on a foundation of best practices, and includes a range of features, procedures and processes that are designed to protect sensitive health information . Our policy, guides and FAQ's can be viewed on our website at http://www.ehealthontario.on.ca/en/security

Q.	Why does eHealth Ontario collect personal information about registrants?
A.	eHealth Ontario collects information about individuals in order to verify their identity when registering them for eHealth services, such as OLIS, DPV, and eHealth Ontario Portal. eHealth Ontario is permitted by law to collect this information.

Q.	How does eHealth Ontario use this information?
A.	eHealth Ontario uses the information for the following purposes: ▪ Registering individuals as users of eHealth services. ▪ Enrolling registrants for eHealth services. ▪ Maintaining Registration and Enrolment information. ▪ Managing, administering and operating the registration system and the eHealth services that eHealth Ontario provides through it. ▪ Establishing and controlling directories for the purposes of enabling eHealth services. ▪ Monitoring and auditing compliance with Terms and Conditions and Acceptable Use Policies for Services. ▪

Q.	Who has access to this information?
A.	eHealth Ontario Registration Authorities and Local Registration Authorities, who collect and enter information; as required in the Registration and Enrolment process have access to the information. The RAs and LRAs are trained to protect personal information collected during the registration process. **eHealth Ontario is only allowed to collect the information to register and verify the identity of people using the information services that it provides. It is not allowed to use it for any other purpose.**
Q.	What mandatory information is required for a registration?
A.	eHealth Ontario requires the following information about your identity: • Full legal name • Gender • Date of birth This information is used to establish a **unique identity** for the registrant, which helps us prevent duplicate registrations, and facilitates finding the correct registrant for subsequent registration activities (e.g., updating information).
Q.	Why does eHealth Ontario require identity documents?
A.	eHealth Ontario uses the information on documents (such as a birth certificate, drivers' licence or passport) to validate the real world identity of individuals. This allows it to create a unique electronic identity for every registrant at a level of assurance that is suitable for accessing Personal Health Information. A Registration Agent will compare the information on the identity documents, such as gender, legal names, and date of birth, with the information provided by the registrant. This process also ensures that variations in name usage (Susan, Sue, Suzy, etc) do not result in the creation of multiple electronic identities for a person. eHealth Ontario does not make copies of or retain identity documents.
Q.	Why does eHealth Ontario collect document numbers?

A.	Document numbers are required for audit purposes. Audit processes include checking that we do not have multiple registrants registered using the same identity documents. As the eHealth Ontario client and user base grows with large numbers of users accessing Personal Information or Personal Health Information, eHealth Ontario will be implementing additional audit controls.
	The document numbers are not visible to anyone accessing the ONE® ID system.
Q.	**What are Challenge Questions and why do we need them?**
A.	Challenge questions are questions to which only the registrant knows the answer and are used to verify the registrant's identity when calling the eHealth Ontario Service Desk for support or online when authenticated by the ONE ID system. The registrant's identity is assumed valid if the registrant can provide the answers that correspond to his/her questions. The two service challenge questions collected on the Registration and Service Enrolment form are for support purposes, so that Service Desk personnel can validate a registrant's identity in a support situation such as helping the user if they are having problems completing the registration process.
	A second set of challenge questions are collected online as part of the registration process which only the end user knows and which can be used for online services such as password resets or to recover a forgotten user name.

Collection Practices

Q.	**What participation and consent is required by registrants?**
A.	Individuals who wish to be registered and enrolled for eHealth services are expected to participate in the registration process by:
	▪ Consenting to the collection, storage, use and disclosure of their personal information, either in writing or electronically.
	▪ Consenting to the use of their personal information.
	▪ Providing personal information including supporting identity documents or other evidence.
	▪ Providing eHealth Ontario with any updates or changes to the personal information.
Q.	**What happens when a registration is terminated?**
A.	When a registration is terminated, eHealth Ontario ceases to use the registration information as of the termination date, and keeps only archival Information about the registration or enrolment activity.
Q.	**How does eHealth Ontario protect your personal information?**

A.	Security practices within eHealth Ontario provide physical, procedural, personnel and technical security for information, as follows:

Physical Security:

- The eHealth Ontario computers and software where information is stored are located in a secure space with access control systems to prevent unauthorized access.

- eHealth Ontario RAs/LRAs and Customer Service Representatives are located in areas with physical security to prevent unauthorized access.

- eHealth Ontario RAs/LRAs and Customer Service Representatives are required to observe access controls, such as password-protected screen savers, not writing down passwords and not leaving an unlocked computer unattended.

- Computer devices and paper containing information must be stored in secure containers, and disposed of in a secure manner when no longer required (e.g., by shredding), or returned to the registrant if applicable (e.g., notarized photocopies of identity documents).

Procedural Controls:

- Access to information and system privileges by eHealth Ontario RAs/LRAs and Customer Service Representatives is limited to what is required for them to fulfill their duties and responsibilities.

- eHealth Ontario RAs and LRAs are given read and update access to information.

- Customer Service Representatives are only given read access to the information required to authenticate registrants.

Personnel Controls:

- All employees and contract staff of eHealth Ontario are required to undergo Canadian Police Information Centre (CPIC) checks, to observe the eHealth Ontario Enterprise Privacy and Security Policies, and to receive privacy and security training.

- LRAs are appointed in writing by eHealth Ontario; they must agree to abide by all eHealth Ontario policies respecting information, be registered at the appropriate level of assurance, and receive proper training in relation to their assigned duties, including privacy and security training.

Technical Controls:

- Access to information systems is authenticated by User ID, password, other tokens (including RSA tokens) and PKI certificates (for RAs and LRAs).

- eHealth Ontario's infrastructure provides transport layer encryption for all Information transmitted across the eHealth Ontario network.

For more information about eHealth Ontario's privacy and security policies and programs, please see www.ehealthontario.on.ca or e-mail us at privacyandsecurity@ehealthontario.on.ca. You can also mail inquiries to the Vice President, Privacy and Security at:

eHealth Ontario

P.O. Box 148,

777 Bay Street, Suite 701,

Toronto, Ontario M5G 2C8