eHealth Ontario

Personal Information Privacy Policy

Privacy Office

Document ID: 1194

Version: 9.4

Owner: Chief Privacy Officer

Sensitivity Level: Low

Ontario
eHealth Ontario

Contents

Tables

1 Purpose / Objective

The *eHealth Ontario Personal Information Privacy Policy* has been developed to govern the collection, use and disclosure of personal information (PI) in a manner that will facilitate eHealth Ontario business operations and service delivery while protecting the rights and privacy of eHealth Ontario personnel, clients and members of the public.

eHealth Ontario is an "institution" as defined in Ontario's *Freedom of Information and Protection of Privacy Act*, 1990, S.O. 1990, c. F.31, as amended (FIPPA) and is subject to its provisions. eHealth Ontario is committed to protecting PI subject to FIPPA and extending privacy protection practices to its handling of PI where that information may not be subject to privacy laws or regulations.

2 Scope

This Policy applies to all eHealth Ontario personnel and third party service providers whom it has retained to support the delivery of its operations and services. It applies to information about identifiable individuals in the custody or control of eHealth Ontario, regardless of medium, including information collected via the eHealth Ontario website. It governs the access, collection, use, disclosure, retention and destruction of PI contained in eHealth Ontario Records.

For the purpose of this Policy, "PI" has the same meaning as defined in Section 2 of FIPPA. "PI" does not include eHealth Ontario personnel business contact information, such as name, title and business addresses of eHealth Ontario personnel. This Policy applies to all PI collected, used and disclosed by eHealth Ontario, whether or not that PI is subject to FIPPA.

This Policy does not address the processing of Personal Health Information by eHealth Ontario as that term is defined by the *Personal Health Information Protection Act*, S.O. 2004, c.3, Schedule A, as amended ("PHIPA") of Ontario. Personal Health Information that is collected directly from an individual by eHealth Ontario, and not from a health information custodian, is not subject to PHIPA, and is therefore not within the scope of this Policy.

This Policy should be read in conjunction with the *eHealth Ontario Privacy and Data Protection Policy*. This Policy is supported by eHealth Ontario's subordinate policies, standards, procedures and guidelines that are part of a comprehensive program for the protection of PI. These policies include but are not limited to:

- *eHealth Ontario Privacy Impact Assessment Policy*
- *eHealth Ontario Privacy Incident and Breach Management Policy*
- *eHealth Ontario Privacy Complaints and Inquiries Policy and Procedure*
- *eHealth Ontario Privacy Risk Management Policy and Procedure*
- *eHealth Ontario Privacy Policy on the Responsibilities of Third Party Service Providers*
- *eHealth Ontario Freedom of Information and Protection of Privacy Access Request Policy*
- Where the repository or system is governed by the Electronic Health Record (EHR) Privacy Policies, follow the appropriate policies and procedures outlined in the *eHealth Ontario Electronic Health Record Privacy Policies*.

3 Policy

eHealth Ontario considers PI under its control or custody as confidential and will only make such information available to authorized users and in accordance with FIPPA. Subject to specific limitations and exceptions, individuals (or their legal representatives where permitted) may access their own PI contained in records under the custody or control of eHealth Ontario by following the appropriate access processes identified in section 3.7 of this Policy. For the purpose of this Policy, the specific limitations and exceptions are those identified in FIPPA.

eHealth Ontario personnel and third party service providers retained by eHealth Ontario have a duty to collect, use and disclose only such PI as is essential to fulfill their job duties. In signing the *eHealth Ontario Privacy and Security Standard of Conduct Acknowledgement and Agreement*, all eHealth Ontario personnel and third party service providers agree to comply with the provisions of this Policy.

Third party service providers are individuals or organizations retained by eHealth Ontario to support the delivery of its operations and services. Third party vendors and their employees who handle PI held by eHealth Ontario must comply with all applicable eHealth Ontario policies and procedures.

Authorized persons are individuals who require access to PI in order to meet the requirements of their role(s) within eHealth Ontario. Authorized persons who have been granted access to PI are responsible for protecting the confidentiality of that information and the privacy of the individuals who are the subject of the information. They are also required to use the information responsibly in accordance with all applicable legislation, regulations and policies. Authorized persons shall only be granted access to PI on a need to know basis.

3.1 Collection of Personal Information by eHealth Ontario

eHealth Ontario derives its statutory authority to operate its programs and services from the *Ontario Regulation* 43/02 as amended by O. Reg 339/08 of the *Development Corporations Act*, R.S.O. 1990, c. D. 10. FIPPA states that PI may only be collected by or on behalf of eHealth Ontario in the necessary course of operations where the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity of eHealth Ontario.

eHealth Ontario collects PI through various means, including from personnel and third party service providers for employment purposes, from individuals through the eHealth Ontario website and in the course of registering and assisting end users in the deployment of eHealth Ontario products and services. eHealth Ontario shall only directly collect PI from the individual to whom it relates unless the individual or their legal representative consents to another manner of collection. eHealth Ontario shall only indirectly collect PI where the indirect collection is permitted by law.

3.2 Notification and Consent Requirements

eHealth Ontario shall notify individuals of the purpose for the access, collection, use, retention or subsequent disclosure of their PI. eHealth Ontario shall inform individuals as to all intended uses of their PI when that information is initially collected. Notifications contained in eHealth Ontario forms, communications and posted on the eHealth Ontario website shall be clear, specific and reviewed periodically to ensure currency and accuracy.

Any secondary use or disclosure of PI collected by eHealth Ontario shall require the express written consent of the individual who is the subject of that information, or, where permitted, their legal representative, unless such use or disclosure is otherwise permitted or required by law. An individual's consent must be documented and that documentation shall be retained with the record(s) and managed in accordance with the records' established retention period.

3.3 Use of Personal Information

PI shall be used within eHealth Ontario only by authorized personnel for the purpose for which it was obtained or for a consistent purpose.

Common uses of information by eHealth Ontario include, but are not limited to, the use of PI to establish, manage and administer employment and contractual relationships, including administration of payroll and benefits and use of PI to establish and maintain end user client accounts and services.

3.4 Disclosure of Personal Information by eHealth Ontario

eHealth Ontario shall not disclose PI to external agencies or persons without the consent of the individual to whom the information relates, unless the disclosure is permitted by section 42 of FIPPA. eHealth Ontario personnel and third party service providers shall consult the Chief Privacy Officer (CPO) prior to disclosing PI without consent.

All disclosures of PI must be documented and that documentation shall be securely retained with the record(s) and managed in accordance with eHealth Ontario policies and procedures.

3.5 Incident and Breach Management

eHealth Ontario's Privacy Breach Management Policy describes the Agency's approach to privacy incident and breach management. The process by which a privacy incident or breach and security incident is contained, investigated and remediated is defined by eHealth Ontario's Privacy Breach Management (PBM) Security Incident Response (SIR) programs.

In accordance with PBM and SIR, eHealth Ontario shall contain the effects of the incident or breach by determining the nature and scope of the incident or breach, and issue all required notifications through a clear communications and escalation process.

3.6 Duty to Conduct Privacy Impact Assessments

eHealth Ontario conducts PIAs on every eHealth Ontario service that involves PI in accordance with the *eHealth Ontario Privacy Impact Assessment Policy*.

eHealth Ontario addresses all risks and issues identified in its PIAs in as timely a manner as possible, either through the recommendations provided in the PIAs, or through the privacy risk treatment plans that eHealth Ontario develops in response to PIA findings.

Details regarding eHealth Ontario's approach to performing and responding to PIAs can be found in its *Privacy Impact Assessment Policy*.

3.7 Individual Access to Personal Information

FIPPA provides individuals with a right of access to their PI in the custody or control of eHealth Ontario, subject to specific limitations stipulated in that Act. Wherever possible, eHealth Ontario personnel shall assist individuals in accessing their PI without having to resort to making a formal request under the Act. eHealth Ontario Divisions should establish processes by which access to commonly requested PI may be granted.

Where no process has been established, or where there may be disclosure concerns, individuals shall be advised to make a formal request under FIPPA. Such formal requests shall be directed to the Freedom of Information (FOI) Office within the Privacy Office, in accordance with the *eHealth Ontario Freedom of Information and Protection of Privacy Access Policy* and related procedural documents.

3.8 Accuracy, Integrity and Requests for Correction of Personal Information

eHealth Ontario shall endeavour to ensure the accuracy, currency and integrity of the PI in its custody or control. Where an individual believes their PI to be in error, they may request correction of that information, and eHealth Ontario shall consider and respond to those requests. Where such requests can be handled informally, eHealth Ontario personnel shall endeavour to assist individuals in ensuring the accuracy of their PI wherever possible. All formal requests for correction of PI shall be forwarded to the CPO.

3.9 Retention and Destruction of Personal Information

Reg. 460, section 5(1) made under FIPPA requires that institutions retain records containing the PI of individuals for a minimum of one year following last use of the record, unless the individual consents to its earlier destruction.

Data retained by eHealth Ontario on the MOHLTC's behalf will be retained for an indefinite period in accordance with the *MOHLTC Interim Electronic Health Record (EHR) Data Retention Schedule* (September 30, 2013).

eHealth Ontario is required to safeguard all PI for the duration of its retention period. Responsibility for eHealth Ontario Records Management rests with the Senior Vice President, Corporate Services, eHealth Ontario. eHealth Ontario personnel and third party service provider retained by eHealth Ontario shall ensure that destruction of records containing PI is done so in accordance with eHealth Ontario policies and procedures.

3.10 Personal Information Banks

eHealth Ontario is required by law to create and maintain a Personal Information Bank (PIB) which identifies by type and location the records under its control which contain PI. This information is provided to the Minister of Government Services, who in turn has a statutory responsibility to make it available to the public through annual publications. This information is also made available to the public in the *eHealth Ontario Directory of Records* as described in section 3.11.

eHealth Ontario personnel shall ensure that information on records and file classes is provided to Records Management in accordance with the *eHealth Ontario Record Management Standard*. It is the responsibility of all eHealth Ontario program managers to provide any requested information regarding listings of record holdings for PIBs to the CPO as requested.

3.11 Information Management

eHealth Ontario's Privacy Office maintains the *eHealth Ontario Directory of Records* found on eHealth Ontario's website. eHealth Ontario periodically reviews the *eHealth Ontario Directory of Records* to ensure that the information in the *eHealth Ontario Directory of Records* is accurate and complete.

eHealth Ontario shall ensure that:

- the confidentiality of the data described in the *eHealth Ontario Directory of Records* is adequately protected;
- access is restricted to those personnel or third party service providers whose roles require such access;
- access is logged, including the name of person who accessed the information, the purpose for the access, and the date and time of the access;
- access logs are reviewed periodically to ensure all access to PI are still relevant for the purposes identified; and
- data repositories are retained only as long as are needed to fulfill the purposes for which they were collected.

4 Responsibilities

The CEO, with the advice of the CPO or delegate, is responsible for interpreting the policy as it pertains to PI included within the scope of FIPPA. Ultimate responsibility for all FIPPA related issues at eHealth Ontario rests with the CEO as Head of the Institution as defined by Ontario Regulation 460 (FIPPA, R.R.O. 1990, Regulation 460 - "General"). Responsibilities for FIPPA Access Requests at eHealth Ontario are contained in the *eHealth Ontario Freedom of Information and Protection of Privacy Act Access Policy*.

The CPO is considered the ultimate authority for interpretation of this Policy.

The CPO is responsible for implementing, enforcing and maintaining this Policy.

The CPO is responsible for monitoring compliance with this Policy.

All eHealth Ontario personnel and third party service providers retained by eHealth Ontario are responsible for handling PI in a manner consistent with this Policy and applicable legislation.

5 Glossary

The following terminology and acronyms are associated with this Policy:

TERM	DEFINITION
Access	"Access" refers to the ability of an individual to retrieve, view or process personally identifiable information.
Authorized User or Authorized Persons	"Authorized Users" or "Authorized Persons" are employees or agents of eHealth Ontario who have been granted access to specific data bases or other stores of Personal Information required for the necessary execution of their duties. It is understood that authorized users will have signed eHealth Ontario's Privacy and Security Standard of Conduct Acknowledgement and, where required, will have completed all required Privacy and Security and/or Role Based Training specific to their role(s) within the Agency.
Collection	"Collection" refers to the gathering of Personal Information of identifiable individuals which may occur directly, indirectly, actively or passively.
Data Repository	A logical partitioning of data where multiple databases that apply to specific applications or sets of applications reside. For example, several databases that support healthcare applications could reside in a single healthcare data repository.
Disclosure	"Disclosure" refers to the release of information to parties external to eHealth Ontario.
eHealth Ontario Managers	A manager is a person whose principal employment responsibilities consist of supervising or directing, or both supervising and directing, human or other resources. At eHealth Ontario, a manager may be the Chief Executive Officer, Senior Vice Presidents, Vice Presidents, Senior Directors, Directors, Managers, Supervisors, program leads, project managers or personnel who carry out managerial duties..
eHealth Ontario Personnel	eHealth Ontario employees and temporary staff (contractors, temp agency staff, co-op students and seconded individuals.) Contractors are individuals procured through a company for a specified period of greater than 3 months to fill a permanent full time position temporarily and on a day- to- day basis are managed directly by eHealth Ontario management.
eHealth Ontario Records	All records created in the course of eHealth Ontario business activities.
Freedom of Information and Protection of	A provincial privacy statute that provides a right to access information under the control of institutions in accordance with the principles that information should be available to the public; necessary exemptions from the right of access should be limited and specific; and

***Privacy Act*, R.S.O. 1990, c. F. 31 (FIPPA)**	decisions on the disclosure of government information should be reviewed independently of government. FIPPA also protects the privacy of personal information of individuals held by institutions. It provides individuals with a right of access to, and correction of, that information.
Minimum and Relevant Information	"Minimum and relevant information" means the most limited data set required for the carrying out of a specific role, task or function.
Need to Know	"Need to know" is the principle which supports an authorized user's access and use of "minimum and relevant" Personal Information necessary to meet required business purposes of eHealth Ontario.
Personal Information (PI)	"Personal Information" means recorded information about an identifiable individual, including, a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, c) any identifying number, symbol or other particular assigned to the individual, d) the address, telephone number, fingerprints or blood type of the individual,e) the personal opinions or views of the individual except where they relate to another individual, f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, g) the views or opinions of another individual about the individual, and h) the individual's name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual.
Retain	"Retain" refers to the keeping possession of Personal Information or Personal Health Information within the Agency.
Right of Access	"Right of Access" refers to an individual's right to view or receive copies of their own Personal Information in the custody or control of eHealth Ontario, subject to the limited and specific provisions of FIPPA, or where FIPPA does not apply, the reasonable discretion of the custodian of the Personal Information.
Right to Request Correction	"Right to Request Correction" refers to an individual's right to request that eHealth Ontario update or otherwise modify their own Personal Information where that information may be in error.
Use	"Use" refers to the handling of Personal Information within the Agency.

Table 1: Personal Information Policy: Glossary

6 References and Associated Documents

The following are legislative references and eHealth Ontario policies associated with this Policy:

REFERENCE	LOCATION
Freedom of Information and Protection of Privacy Act (FIPPA) and regulations	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
eHealth Ontario Privacy and Data Protection Policy	http://www.ehealthontario.on.ca/en/privacy
eHealth Ontario Privacy Impact Assessment Policy	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Privacy Incident and Breach Management Policy	http://www.ehealthontario.on.ca/en/privacy
eHealth Ontario Privacy Complaints and Inquiries Policy and Procedure	http://www.ehealthontario.on.ca/en/privacy
eHealth Ontario Privacy Policy on the Responsibilities of Third Party Service Providers	http://www.ehealthontario.on.ca/en/privacy
eHealth Ontario Directory of Records	http://www.ehealthontario.on.ca/en/privacy
eHealth Ontario Privacy Risk Management Policy and Procedure	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Freedom of Information and Protection of Privacy Access Request Policy	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Records Management Standard	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Privacy and Security Standard of Conduct for Employees	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Privacy and Security Standard of Conduct for Service Providers	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx

eHealth Ontario Electronic Health Record Privacy Policies	http://www.ehealthontario.on.ca/en/initiatives/resources

Table 2: Personal Information Policy: References and Associated Documents

7 Interpretation

Policy requirements preceded by:

- 'shall' are compulsory actions;
- 'may' are options; and
- 'should' are recommended actions

If there is a discrepancy between this Policy and *FIPPA* or *PHIPA*, the regulations made under those Acts, or with the Agency's Regulation, the legislation or regulation takes precedence.

If there is a discrepancy between this Policy and any other eHealth Ontario privacy policy, the *eHealth Ontario Privacy and Data Protection* Policy takes precedence.