

# eHealth Ontario Personal Information Privacy Policy

Document Identifier: [1194](#)

Version: 6

Owner: Chief Privacy and Security Officer

## Document Control

The electronic version of this document is recognized as the only valid version

---

<b>Document Location:</b>	<a href="http://records/sites/Privacy/Privacy%20Policies/Forms/AllItems.aspx">http://records/sites/Privacy/Privacy%20Policies/Forms/AllItems.aspx</a>
<b>Review Frequency:</b>	This document will be reviewed bi-ennially or with greater frequency at the discretion of the Chief Privacy and Security Officer.

---

<b>Document Prime*</b>	Angelique Hamilton
*Enquiries relating to this document should be referred to the responsible Document Prime.	Senior Privacy Analyst

---

## Approval History

Approver(s)	Title	Approved Date
David Hallett	Chief Operating Officer	2009-08-13
Karen Waite	Chief Privacy and Security Officer	2009-08-13
Michael Power	VP, Privacy and Security	2008-11-12

## Revision History

Version No.	Version Date	Summary of Change	Changed By
6	2009-08-13	Revision as per Chief Privacy and Security Officer	Patrick Lo
5	2008-07-25	Final revisions completed	Angelique Hamilton
4	2008-06-27	Additional revisions following review with Chief Privacy and Security Officer	Angelique Hamilton
3	2008-06-24	Additional revisions following review by Chief Privacy and Security Officer	Angelique Hamilton
2	2008-06-05	Revised version following review by Chief Privacy and Security Officer	Angelique Hamilton
1	2008-05-08	Draft Policy	Angelique Hamilton

---

## 1 Purpose / Objective

---

The Personal Information Privacy Policy has been developed to govern the collection, use and disclosure of Personal Information 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*, 2004, S.O. 2004, c. F.31, as amended (“FIPPA”) and is subject to its provisions. eHealth Ontario is committed to extending its current practices as required by FIPPA to its handling of Personal Information where that information may not be subject to privacy laws or regulations. The intention of this policy is to ensure that Personal Information not currently subject to FIPPA, such as employment related information, is treated according to the same privacy standards afforded Personal Information under the legislation.

## 2 Scope

---

This policy 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 collection, use, disclosure, retention and destruction of Personal Information contained in eHealth Ontario Records. For the purpose of this policy, “Personal Information” has the same meaning as defined in Section 2 of FIPPA, and includes Internet Protocol (IP) addresses and employment related information about identifiable individuals. “Personal Information” 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 Personal Information collected, used and disclosed by eHealth Ontario, whether or not that Personal Information 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 within the scope of this policy.

## 3 Policy

---

eHealth Ontario considers Personal Information under its control or custody as confidential and will only make such information available to authorized users. Subject to specific limitations and exceptions, individuals (or their legal representatives where permitted) may access their own Personal Information contained in records under the custody or control of eHealth Ontario by following the appropriate access processes identified in section 3.5 of this policy. For the purpose of this policy, the specific limitations and exceptions are those identified in FIPPA.

eHealth Ontario Personnel and Third Parties acting on eHealth Ontario’s behalf have a duty to collect, use and disclose only such Personal Information as is essential to carry out eHealth Ontario’s business activities. In signing the eHealth Ontario Privacy and Security Standard of Conduct Acknowledgement, all eHealth Ontario Personnel agree to comply with the provisions of this policy. For the purpose of this policy, “eHealth Ontario Personnel” means eHealth Ontario staff, consultants and contract employees.

“Third parties”, for the purpose of this policy, means individuals or organizations with whom eHealth Ontario contracts for services. Third party vendors and their employees who handle Personal Information held by eHealth Ontario must comply with all applicable eHealth Ontario policies and procedures.

“Authorized Persons” are individuals who require access to Personal Information in order to meet the requirements of their role(s) within eHealth Ontario. Authorized Persons who have been granted access to Personal Information are responsible to protect 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, and to ensure the accuracy and integrity of the Personal Information. Authorized persons shall only be granted access to Personal Information 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 determines that Personal Information 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 Personal Information through various means, including Personal Information that is provided by Personnel and Third Parties 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 collect Personal Information directly 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 Personal Information where the indirect collection is permitted by law.

### **3.2 Notification and Consent Requirements**

eHealth Ontario shall notify individuals of the purpose for the collection, use or subsequent disclosure of their Personal Information. eHealth Ontario shall inform individuals as to all intended uses of their Personal Information 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 Personal Information 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**

Personal Information 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 Personal Information to establish, manage and administer employment and contractual relationships, including administration of payroll and benefits and use of Personal Information to establish and maintain end user client accounts and services.

### **3.4 Disclosure of Personal Information by eHealth Ontario**

eHealth Ontario shall not disclose Personal Information 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 Parties shall consult the Chief Privacy and Security Officer prior to disclosing Personal Information without consent.

All disclosures of Personal Information must be documented and that documentation shall be retained with the record(s) and managed in accordance with the records’ established retention period.

### **3.5 Incident Management**

eHealth Ontario has established an Enterprise Security and Privacy Incident Management program (ESPIM) in order to effectively respond to privacy and security incidents. Any eHealth Ontario Personnel who become aware of a possible or actual incident which may threaten the privacy or security of PI entrusted to eHealth Ontario shall immediately contact the Enterprise Service Desk (ESD) to trigger the ESPIM process.

### **3.6 Duty to Conduct Privacy Impact Assessments**

Prior to implementing any significant change to the way in which Personal Information is collected, used, disclosed, processed, stored or disposed, eHealth Ontario shall perform Privacy Threshold Analyses (PTAs) and/or Privacy Impact Assessments (PIAs). eHealth Ontario shall also make PIA summaries available to the public via the eHealth Ontario website. eHealth Ontario will maintain a Privacy Impact Assessment Policy, templates and guideline to support the PTA and PIA processes, and will update these documents and tools as required.

### **3.7 Individual Access to Personal Information**

FIPPA provides individuals with a right of access to their Personal Information 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 personal information without having to resort to making a formal request under the Act. eHealth Ontario Divisions should establish processes by which access to commonly requested Personal Information 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 FIPPA Officer, 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 Personal Information in its custody or control. Where an individual believes their Personal Information 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 Personal Information wherever possible. All formal requests for correction of Personal Information shall be forwarded to the Chief Privacy and Security Officer in his or her capacity as Freedom of Information Coordinator for eHealth Ontario.

### **3.9 Retention and Destruction of Personal Information**

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

eHealth Ontario is required to safeguard all Personal Information for the duration of its retention. Responsibility for eHealth Ontario Records Management rests with the Director of Finance, eHealth Ontario. eHealth Ontario Personnel and Third Parties acting on behalf of eHealth Ontario shall ensure that destruction of records containing Personal Information is in accordance with the processes established by eHealth Ontario's Information Disposal Guideline.

### 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 Personal Information. This information is provided to the Minister, who in turn has a statutory responsibility to make it available to the public through annual publications. It is the responsibility of all eHealth Ontario Program Managers to provide listings of record holdings for PIBs to the Chief Privacy and Security Officer, in his or her capacity as Freedom of Information Coordinator for eHealth Ontario .

## 4 Responsibilities

The CEO, with the advice of the Freedom of Information (“FOI”) Coordinator, is responsible for interpreting the policy as it pertains to Personal Information 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 459. Responsibilities for FIPPA and Privacy at eHealth Ontario are contained in the eHealth Ontario Freedom of Information and Protection of Privacy Act Access Policy and eHealth Ontario Privacy Roles and Responsibilities.

All eHealth Ontario Personnel and Third Parties are responsible for handling Personal Information in a manner consistent with this policy and applicable legislation. Reviews and updates of this policy will be completed by the Director, Privacy and at the discretion of the Chief Privacy and Security Officer. The Chief Privacy and Security Officer is considered the ultimate authority for interpretation of this policy as it pertains to Personal Information that does not fall under FIPPA.

## 5 Glossary

Term	Definition or Explanation
Personal Information	<p>“Personal Information” means recorded information about an identifiable individual, including,</p> <ol style="list-style-type: none"> <li>information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,</li> <li>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,</li> <li>any identifying number, symbol or other particular assigned to the individual,</li> <li>the address, telephone number, fingerprints or blood type of the individual,</li> <li>the personal opinions or views of the individual except where they relate to another individual,</li> <li>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,</li> <li>the views or opinions of another individual about the individual, and</li> <li>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; (“renseignements personnels”)</li> </ol> <p>For the purposes of eHealth Ontario policies, “Personal Information” also includes IP addresses of identifiable individuals.</p>
eHealth Ontario Personnel	“eHealth Ontario Personnel” means eHealth Ontario staff, consultants and contract employees.
Third Parties	“Third Parties” means individuals or organizations with whom eHealth Ontario contracts for services.
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.
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.

Term	Definition or Explanation
Access	"Access" refers to the ability of an individual to retrieve, view or process personally identifiable information.
Collection	"Collection" refers to the gathering of Personal Information of identifiable individuals which may occur directly, indirectly, actively or passively.
Use	"Use" refers to the handling of Personal Information within the Agency.
Disclosure	"Disclosure" refers to the release of information to parties external to eHealth Ontario.
"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.
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.
eHealth Ontario Records	All records created in the course of eHealth Ontario business activities.

## 6 References and Associated Documents

- [eHealth Ontario Privacy and Data Protection Policy](#)
- [eHealth Ontario Privacy and Security Employee Standard of Conduct](#)
- [eHealth Ontario Personal Health Information Privacy Policy](#)
- [eHealth Ontario Privacy Impact Assessment Policy](#)
- [eHealth Ontario Freedom of Information and Protection of Privacy Access Request Policy](#)
- [eHealth Ontario Information Disposal Guideline](#)
- [eHealth Ontario Privacy Roles and Responsibilities](#)