

eHealth Ontario Personal Health Information Privacy Policy

Document Identifier: 1206

Version: 4

Owner: Chief Privacy and Security Officer

Document Control

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

Document Location:	http://records/sites/Privacy/Privacy%20Policies/Forms/AllItems.aspx
Review Frequency:	This policy will be reviewed bi-ennially, or with greater frequency at the direction of the Chief Privacy and Security Officer
Document Prime* *Enquiries relating to this document should be referred to the responsible Document Prime.	Angelique Hamilton 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
4	2009-08-12	Revision as per Chief Privacy and Security Officer	Patrick Lo
3	2008-09-25	Final revisions as per VP, Privacy and Security	Angelique Hamilton
2	2008-08-06	Revised following review with VP, Privacy and Security	Angelique Hamilton
1	2008-07-31	First Draft Provided for Review by Chief Privacy and Security Officer	Angelique Hamilton

1 Purpose / Objective

eHealth Ontario (“eHealth Ontario” or “the Agency”) derives its operational mandate from Ontario Regulation (O.Reg) 43/02 as amended by 339/08 under the *Development Corporations Act*, R.S.O. 1990, c. D.10. eHealth Ontario’s mandate includes supporting hospitals, clinics, and other Ontario health organizations in protecting the Personal Health Information (PHI) they collect by providing secure infrastructure, hosting, secure networks, secure email and related services for transmission, processing and storage of that PHI.

1.1 Personal Health Information and Personal Information

Section 4 of the *Personal Health Information Protection Act*, S.O. 2004, as amended, (“PHIPA”) defines Personal Health Information (PHI) to generally mean identifying information about an individual in oral or recorded form pertaining to that person’s health or health services provided to the individual. Health Information Custodians collect PHI in the course of providing health services to individuals.

Personal Health Information (PHI) is distinguished from Personal Information (PI) by the context in which it was collected and/or disclosed. Personal Health Information is collected by health care providers in the course of providing health related services to individuals. Personal Information, such as a patient’s name and address, is considered Personal Health Information (PHI) when it is collected and retained in connection with the provision of health services. When this personal health information is disclosed directly by a Health Information Custodian to non-Health Information Custodians such as eHealth Ontario, it is considered to be PHI subject to the provisions of PHIPA. If an individual who is not acting as a Health Information Custodian discloses that same information directly to eHealth Ontario, it is considered to be Personal Information (PI) subject to the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, as amended (“FIPPA”).

The purpose of this policy is to clearly articulate the responsibilities of the Agency as it meets its mandate to provide Health Information Custodians (HICs) in Ontario with the secure electronic means by which to collect, use, disclose and otherwise manage the PHI in their custody and control.

2 Scope

This policy applies wherever eHealth Ontario Personnel or Third Parties are engaged in business activities which support facilitating the secure transmission, processing and storage of PHI, or where such individuals may have access to PHI in the course of delivering authorized services and products to Ontario’s health sector. 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 Health Information held by eHealth Ontario must comply with all applicable eHealth Ontario policies and procedures in accordance with the terms of their written agreements with the Agency.

eHealth Ontario’s roles and responsibilities with respect to Personal Health Information (PHI) are defined by the *Personal Health Information Protection Act*, S.O. 2004, as amended (PHIPA) and its Regulation. This policy applies to eHealth Ontario’s handling of PHI when acting in its capacity as an Electronic Service Provider (ESP), Health Information Network Provider (HINP), a Third Party Retained by a Health Information Network Provider (3rd Party to a HINP) or as an Agent of a Health Information Custodian (Agent).

eHealth Ontario's responsibilities with respect to its handling of Personal Information (PI) are governed by the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, as amended (FIPPA) as well as the eHealth Ontario Personal Information Privacy Policy, and are outside the scope of this policy.

3 eHealth Ontario Roles under PHIPA

PHIPA Regulations identify five possible roles an individual or organization may fulfill while handling PHI:

- Health Information Custodian (HIC),
- Agent of a Health Information Custodian (Agent of a HIC),
- Electronic Service Provider (ESP),
- Health Information Network Provider (HINP) and
- Third Party Retained by a Health Information Network Provider (3rd Party to a HINP).

The requirements contained in this policy apply to eHealth Ontario when it is managing or handling PHI in its capacity as an ESP, HINP, a 3rd Party to a HINP or an Agent of a HIC.

eHealth Ontario is not a Health Information Custodian. eHealth Ontario's roles under PHIPA are limited to that of Electronic Service Provider (ESP), Health Information Network Provider (HINP), Third Party Retained by a Health Information Network Provider (3rd Party to a HINP) and Agent of a Health Information Custodian.

An Electronic Service Provider (ESP) under PHIPA is a person who supplies services for the purpose of enabling a Health Information Custodian (HIC) to use electronic means to collect, use, modify, disclose, retain or dispose of Personal Health Information (PHI), and who is not an Agent of the Health Information Custodian. A Health Information Network Provider (HINP) provides the same services but to more than one HIC in order to facilitate electronic disclosure of PHI between HICs.

When acting in its capacity as an ESP, HINP or Agent of a HIC, eHealth Ontario provides services to support Health Information Custodians in meeting their responsibilities under PHIPA as they pertain to the collection, use, disclosure, storage and safeguarding of PHI. When acting in its capacity as a 3rd Party to a HINP, the Agency provides similar support to another Health Information Network Provider in meeting their obligations under PHIPA.

The Agency has no independent decision making role regarding, or interest in PHI, but acts in accordance with the directions of the HICs and HINPs it serves, within the prescribed limits defined by PHIPA.

4 Policy

The majority of eHealth Ontario Personnel and Third Parties providing services to the Agency never have access to the PHI our clients process using eHealth Ontario's ONE Products and services. There is, however, occasional, limited exposure to such information by a small group of eHealth Ontario authorized users required to provide product support, such as troubleshooting and implementation of upgrades, and related network, application and data exchange services.

eHealth Ontario Personnel and Third Parties acting on eHealth Ontario's behalf have a duty to collect, use and disclose Personal Health Information in accordance with PHIPA and eHealth Ontario policy. In signing the eHealth Ontario Privacy and Security Standard of Conduct Acknowledgment, all eHealth Ontario Personnel agree to comply with the provisions of this policy.

4.1 Collection, Use and Disclosure of Personal Health Information by eHealth Ontario

Personal Health Information is collected by Health Information Custodians in the course of the provision of health services to individuals. eHealth Ontario does not provide health services to individuals; therefore, eHealth Ontario does not directly collect Personal Health Information from individuals.

When a Health Information Custodian retains the services of eHealth Ontario as an ESP or HINP to support the secure transmission and storage of PHI, eHealth Ontario Personnel may require incidental access to PHI for purposes of providing services including maintenance, support and repairs. This is deemed to be a “use” of that information. Except as necessary in the course of providing services to its clients, eHealth Ontario shall not use any PHI to which it has access in the course of providing services to HICs or HINPs. Further, eHealth Ontario shall not disclose the PHI entrusted to it by HICs unless permitted or required to do so by law. Requests for access by individuals to PHI stored by HICs within eHealth Ontario Data Centres shall be redirected to the responsible HIC for response.

When acting in its capacity as an Agent of a HIC, eHealth Ontario must comply with section 17 of PHIPA. This section states that a HIC may permit its Agents to collect, use, disclose, retain or dispose of PHI on its behalf only within the limitations already imposed on the HIC in this regard, with the express authorization of the HIC. As an Agent of a HIC, eHealth Ontario shall not make any independent decisions with respect to the handling of PHI, but acts only in accordance with the terms of its agreement with the HIC, and in compliance with PHIPA.

4.2 Written Agreements for Provision of Services to HICs and HINPs

eHealth Ontario shall enter into written agreements with each HIC or HINP prior to providing services to them. The Agency shall retain and track these agreements in a central location, along with agreements with Third Parties with whom eHealth Ontario contracts to assist us in providing services. eHealth Ontario shall maintain tools and procedures to ensure that these agreements are updated as required. Any agreement eHealth Ontario enters into with Third Parties to support its provision of services to HICs and HINPs will ensure that the Third Party agrees to comply with all applicable legislation, restrictions, conditions and requirements to which eHealth Ontario is also bound.

4.3 Duty to Conduct Privacy Impact Assessments

eHealth Ontario shall perform Privacy Impact Assessments (PIAs) and provide summary results to HICs and HINPs prior to providing services to them. eHealth Ontario shall also make PIA summaries available to the public on the eHealth Ontario website. eHealth Ontario will maintain a Privacy Impact Assessment Policy, templates and guidelines to support its PIA process, and will update these documents and tools as required.

4.4 Provision of Documentation to Clients and the Public

In addition to providing summary results of Privacy Impact Assessments, eHealth Ontario shall provide a general description of the safeguards it has implemented in relation to the security and confidentiality of PHI to HICs/HINPs and make this information available to the public by publishing it on eHealth Ontario’s website. eHealth Ontario shall comply with its statutory responsibility to provide to clients and the public a “plain language” description of its products and services, including a description of the safeguards it has in place to protect privacy and confidentiality of PHI.

4.5 Access Controls

“Authorized Persons” are individuals who require access to Personal Health Information in order to meet the requirements of their role(s) within eHealth Ontario. Authorized persons who have been granted access to Personal Health 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, policies and contractual agreements to ensure the security and integrity of the Personal Health Information. eHealth Ontario shall only grant access to Personal Health Information to Authorized Persons on a “need to know” basis, and access to Personal Health Information will be limited, documented and strictly monitored.

eHealth Ontario Personnel who are responsible for and authorized to grant access to systems, applications and networks which contain PHI shall establish processes by which to document, monitor, track and otherwise strictly control access to PHI. eHealth Ontario will also develop and deliver enhanced privacy and security training for those individuals who may require limited access to high sensitive data such as PHI.

4.6 Incident Management

eHealth Ontario has established an Enterprise Security and Privacy Incident Management process (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 PHI entrusted to eHealth Ontario shall immediately contact the Enterprise Service Desk (ESD) to trigger the ESPIM process. As an Agent to a HIC, eHealth Ontario has a statutory duty to notify a HIC at the first reasonable opportunity if PHI handled by the Agency on their behalf is stolen, lost or accessed by unauthorized persons.

5 Responsibilities

The CEO shall approve this policy on the recommendation of the Chief Privacy and Security Officer. The Chief Privacy & Security Officer shall be responsible for the implementation and enforcement of this policy, including provision of training, and shall serve as the ultimate authority for interpretation of this policy.

eHealth Ontario Personnel and Third Parties shall comply with this Policy to the extent that eHealth Ontario identifies it as being applicable to them. eHealth Ontario may apply sanctions to Personnel or Third Parties acting on eHealth Ontario’s behalf found in violation of this Policy consistent with the Agency’s disciplinary and procurement policies and procedures, up to and including civil liability, criminal sanctions and termination of employment or contract.

6 Glossary

Term	Definition
Health Information Custodian	Has the same meaning as defined in PHIPA, section 3, which generally means a person or organization set out in section 3(1) of PHIPA that has custody and control of Personal Health Information. Please review the Act for the full definition.
Personal Health Information	Has the same meaning as defined in PHIPA, section 4, and generally means identifying information about an individual in oral or recorded form pertaining to that person’s health or health services provided to the individual, collected in the course of providing those health services. Please review the Act for the full definition.
Electronic Service Provider	Has the same meaning as defined in PHIPA O.Reg 329/04, section 6(1), which generally means a person who supplies services for the purpose of enabling a Health Information Custodian to use electronic means to

	collect, use, modify, disclose, retain or dispose of Personal Health Information, and who is not an Agent of the Health Information Custodian. Please review the Act for the full definition.
Health Information Network Provider	Has the same meaning as defined in PHIPA O.Reg 329/04, section 6(2), which generally means a person who provides services to two or more Health Information Custodians to enable the HICs to use electronic means to disclose PHI to one another, whether or not the person is an Agent of the HICs. Please review the Act for the full definition.
Third Party to a Health Information Network Provider	Means individuals or organizations which provide services that support other Health Information Network Providers in the provision of their services to Health Information Custodians.
Agent to a Health Information Custodian	Has the same meaning as defined in PHIPA, section 2, which generally means, in relation to a Health Information Custodian, a person that, with the authorization of the HIC, acts for or on behalf of the HIC in respect of PHI for the purposes of the HIC, and not the Agent's own purposes, whether or not the Agent has the authority to bind the HIC, whether or not the Agent is employed by the HIC and whether or not the Agent is being remunerated. Please review the Act for the full definition.
Authorized Persons	"Authorized Persons" are employees or agents of eHealth Ontario who have been granted access to specific data bases or other stores of Personal Health Information and/or 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.

7 References and Associated Documents

- *eHealth Ontario Privacy and Data Protection Policy*
- *eHealth Ontario Privacy Impact Assessment Policy*
- *eHealth Ontario Personal Information Privacy Policy*
- *eHealth Ontario Privacy & Security Employee Standard of Conduct*
- *Personal Health Information Protection Act (PHIPA)*
- *Freedom of Information and Protection of Privacy Act (FIPPA)*