

eHealth Ontario Privacy and Data Protection Policy

Document Identifier: 00998

Version: 3

Owner: Chief Privacy and Security Officer

Document Control

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

Document Location: I:\Privacy and Security\PRIVACY\Policies

Review Frequency: Every two years or with greater frequency at the discretion of the Chief Privacy and Security Officer

Document Prime* Angelique Hamilton,
Senior Privacy Analyst

*Enquiries relating to this document should be referred to the responsible Document Prime.

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
3	2009-08-12	Revision as per Chief Privacy and Security Officer	Patrick Lo
2	2008-09-26	Revision as per VP, Privacy and Security. Final Revisions completed	Angelique Hamilton
1	2007-09-28	Final Draft	Sharan Dosanjh

1 eHealth Ontario's Mandate

The eHealth Ontario Agency (“eHealth Ontario” or the “Agency”) provides information management and information technology services to the health care sector in Ontario. eHealth Ontario is an Agency of the Ontario Ministry of Health and Long-Term Care (MOHLTC).

The objects of the Agency are:

- To provide eHealth Services and related support for the effective and efficient planning, management and delivery of health care in Ontario;
- To develop eHealth Services strategy and operational policy; and
- To protect the privacy of individuals whose Personal Information (PI) or Personal Health Information (PHI) is collected, transmitted, stored or exchanged by and through the Agency, in accordance with the *Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act, 2004* and any other applicable law.

eHealth Ontario provides its services to Ontario's health sector, including hospitals, physicians, labs, Public Health Units, Community Care Access Centres, and pharmacies.

eHealth Ontario's information infrastructure provides a suite of products and services that create electronic connections to improve the flow of patient information between health care professionals. eHealth Ontario's products and services can be generally described as follows:

- **ONE™ Network:** This service allows health care providers to share information over a high-speed network built for health care and to access applications hosted by eHealth Ontario. It also provides a custom connection for their specific information sharing needs, such as health card validation by hospitals.
- **ONE™ ID:** This service provides registration and identity management services which allow eHealth Ontario to support health care professionals in accessing and using other eHealth Ontario products and services.
- **ONE™ Mail:** This e-mail service facilitates the secure exchange of patient information between registered health care professionals.
- **ONE™ Pages:** This searchable directory of ONE Mail users, allows all registered users to search for individuals, as well as groups of health care professionals, based on location, role (e.g., Infectious Disease Officers), or organization.
- **ONE™ Hosting:** This is the service in which eHealth Ontario hosts computer equipment for clients allowing them to offer software applications to their users.
- **ONE Portal:** Is the service by which eHealth Ontario provides a controlled gateway through which clients may access eHealth Ontario hosted applications and e-communities.

2 Purpose of this Policy

eHealth Ontario maintains a comprehensive set of privacy policies, guidelines, standards, procedures and tools that set out the Agency's privacy roles and responsibilities. This *eHealth Ontario Privacy and Data Protection Policy* is the Agency's overarching privacy policy, and is supported by subordinate policies, procedures, standards, and guidelines.

The *eHealth Ontario Privacy and Data Protection Policy*:

- Identifies privacy legislative and regulatory requirements for eHealth Ontario;
- Articulates eHealth Ontario's general approach to privacy and data protection; and

- Defines the privacy and data protection principles and policies common to the Agency's operations, regardless of whether eHealth Ontario is acting in its capacity as a corporate entity or in its capacity as a service provider to the health care sector in Ontario.

This policy contributes to eHealth Ontario meeting its regulatory requirements to put in place administrative, technical and physical safeguards, practices and procedures that achieve the following:

- protect the privacy of individuals in relation to their Personal Health Information (PHI) in the course of providing services to Ontario's health sector;
- protect the privacy of individuals in relation to their Personal Information (PI) in the course of conducting its corporate activities and providing services to external clients which involve the handling of PI;
- support compliance with the Personal Health Information Protection Act, (PHIPA) by Health Information Custodians ("HICs") who rely on services supplied by eHealth Ontario to collect, use, modify, disclose, retain, or dispose of personal health information; and
- ensure eHealth Ontario complies with the requirements of sections 6 and 6.1 of the Regulation made under PHIPA; and

This policy must be read in conjunction with eHealth Ontario's other policies especially the Agency's subordinate privacy policies, standards, and procedures. The subordinate policies, standards and procedures define the privacy and data protection principles and policies specific to eHealth Ontario's role as an Institution, subject to the Freedom of Information and Protection of Privacy Act, or FIPPA, and to its various roles as a service provider to the health care sector in Ontario, as described in Section 3.2, below.

3 Scope

This policy applies to all eHealth Ontario Personnel, including contract employees in the provision of services to external clients as well as conduct of the Agency's corporate operations. Applicable provisions of this policy must be addressed in eHealth Ontario's agreements with third party service providers as required.

It applies to all information in the custody or control of eHealth Ontario, particularly Personal Information subject to the Freedom of Information and Protection of Privacy Act (FIPPA) and Personal Health Information subject to the Personal Health Information Protection Act (PHIPA). It will also apply to any other information the Chief Privacy and Security Officer deems that eHealth Ontario will treat as Personal Information, regardless of whether or not it is subject to established privacy and data protection legislation or regulations.

3.1 Applicable Legislation: eHealth Ontario

eHealth Ontario is subject to and must comply with the following Statutes and Regulations:

- Ontario Regulation 43/02 (O. Reg.) as last amended by O. Reg 339/08 made under the Development Corporations Act. This regulation establishes eHealth Ontario as a corporation and includes obligations and prohibitions relating to privacy, security, and confidentiality. It applies to eHealth Ontario when eHealth Ontario provides services to health care providers in Ontario as well as in connection with its corporate operations. This Regulation establishes eHealth Ontario's power to collect, use and disclose personal information and personal health information, while providing eHealth Services if necessary for the provision of the service,
- Personal Health Information Protection Act (PHIPA), R.S.O. 2004, c. 3, including O. Reg. 329/04, as amended by O. Reg. 537/06 made under PHIPA, 2004. This Act and

its Regulations apply to eHealth Ontario when eHealth Ontario provides services to Ontario's health sector to support Health Information Custodians' management of the Personal Health Information in their custody and control.

- Freedom of Information and Protection of Privacy Act (FIPPA), R.S.O. 1990, c. F. 31, R.R.O. 1990, Reg. 459, R.R.O. 1990, Reg. 460. This Act applies to eHealth Ontario in its capacity as a designated Institution. eHealth Ontario must comply with FIPPA in its handling of Personal Information. FIPPA does not apply to Personal Health Information as defined by PHIPA.

3.2 The Roles of eHealth Ontario

In developing, delivering and maintaining products and services, eHealth Ontario must comply with the requirements particular to roles described in the regulations made under PHIPA which could apply to the Agency. The set of requirements that apply to eHealth Ontario depends on the nature of the business relationship between eHealth Ontario and its clients, and the nature of the products or services that eHealth Ontario is providing to them. In addition, eHealth Ontario is subject to FIPPA where the Agency handles Personal Information.

Specifically, eHealth Ontario may play one of the following roles:

- An Electronic Service Provider:

In this role, eHealth Ontario provides products or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain, or dispose of personal health information.

- A Health Information Network Provider (HINP):

In this role, eHealth Ontario provides services to two or more HICs primarily to enable them to use electronic means to disclose personal health information to one another, whether or not eHealth Ontario is an agent of any of the HICs. eHealth Ontario acts in this capacity in the vast majority of its business relationships with its clients. For example, eHealth Ontario provides ONE Network services to thousands of HICs to enable them to disclose personal health information to one another.

- A Third Party retained by a HINP:

In this role, eHealth Ontario is retained by a HINP to assist in providing services to a HIC. For example, eHealth Ontario may host a clinical management solution for a HINP which is used by physicians. In this case, eHealth Ontario is providing services to the HINP rather than directly to the physicians, who are the HICs. eHealth Ontario's privacy obligations are defined by the agreement between the HINP and eHealth Ontario.

- An Agent to a Health Information Custodian:

eHealth Ontario is an Agent when it provides services to Health Information Custodians in managing the PHI in their custody. For example, eHealth Ontario is an Agent to the MOHLTC in connection with the Electronic Master Patient Index (EMPI).

As an Agent, eHealth Ontario must comply with the direction of the HIC accountable for the PHI involved in provision of the service, and must comply with all applicable sections of PHIPA.

- An Institution under the Freedom of Information and Protection of Privacy Act (FIPPA):

When eHealth Ontario provides registration management services, such as those required for ONE ID users, it collects Personal Information that is subject to the Freedom of Information and Protection of Privacy Act (FIPPA).

FIPPA governs the way in which eHealth Ontario collects, uses, discloses, stores, disposes and otherwise handles Personal Information and, to some extent, its corporate records. FIPPA also applies to the Agency's handling of the Personal Information it collects through the eHealth Ontario website and in the course of its corporate operations.

3.3 Privacy and Data Protection Principles at eHealth Ontario

eHealth Ontario supports Ontario's health sector in meeting their obligation to protect the Personal Information and Personal Health Information collected in the course of providing health care services. eHealth Ontario acknowledges its responsibility to protect the privacy of the data entrusted to us in accordance with applicable privacy and data protection laws and regulations.

eHealth Ontario operates, builds products and provides services in accordance with the following basic principles:

- Recognizing that PHI is among the most sensitive types of Personal Information, eHealth Ontario is committed to treating it with the utmost care.
- Health care providers are responsible for protecting the privacy and the confidentiality of their patients' PHI in accordance applicable legal and ethical requirements including those found in the Personal Health Information Protection Act (PHIPA).
- eHealth Ontario shall support its clients as they fulfill their legal and ethical obligations with respect to PI and PHI.
- eHealth Ontario must seek opportunities to design privacy enhancing features into its products, services and operations.
- As a provider and consumer of advanced technologies, eHealth Ontario will continue to identify, assess, and pursue opportunities to apply privacy-enhancing technology wherever possible at the earliest possible stage.
- eHealth Ontario extends privacy and data protective measures to personal information in its control which may not be subject to current privacy and data protection laws or regulations.
- eHealth Ontario will act in a manner which fosters trust and confidence with its clients and the public in managing privacy and data protection issues in all its activities.
- eHealth Ontario shall be open and transparent about its privacy and data protection policies, practices, and safeguards to the greatest extent possible.
- eHealth Ontario shall be consistent in its application of privacy and data protection policies and standards to the Agency's activities.

3.4 eHealth Ontario Protects Ontarians' Personal Information and Personal Health Information

Most eHealth Ontario Personnel never have access to the Personal Information or Personal Health Information that its clients share when using the Agency's ONE products.

However in any information technology (IT) environment, a limited number of specialized personnel may be required to, or will have incidental access to, sensitive information such as Personal Health Information in order to provide technical or support services to clients. As an example, eHealth Ontario Personnel may have incidental access to Personal Health Information when they troubleshoot a problem with a client's system on that client's behalf.

In instances such as these, eHealth Ontario is permitted to access Personal Information, including Personal Health Information, if necessary in the course of providing services (including the performance of maintenance or repairs). It is prohibited from accessing Personal Information or Personal Health Information for any other purpose when providing those services.

4 Policy

eHealth Ontario is actively committed to fostering a culture of privacy and data protection among its personnel. eHealth Ontario shall be open about its privacy, data protection, and information handling policies and practices except where doing so could reasonably be expected to compromise the security of its products or services or the confidentiality of PI and/or PHI. eHealth Ontario shall provide and make freely available information about its privacy, data protection, and information handling practices in multiple ways, such as, posting information on its website.

eHealth Ontario shall consider the spirit and intent of applicable privacy laws, regulations, agreements, and standards when it considers the privacy implications of its business decisions. In so doing, it may consult with its clients, the MOHLTC, stakeholders, the Office of the Information and Privacy Commissioner Ontario, Ontario's Chief Information and Privacy Officer, and others, as appropriate.

eHealth Ontario shall work collaboratively with its clients and the MOHLTC to support them in meeting their privacy obligations and commitments in the context of their initiatives.

Privacy and Data Protection Management at eHealth Ontario

eHealth Ontario shall manage privacy at the Agency in a comprehensive manner through a set of coordinated activities that safeguard the privacy of personal information, including personal health information that is collected, transmitted, stored, and exchanged by and through the eHealth Ontario infrastructure and in the Agency's business activities. Privacy activities include but are not limited to privacy compliance, privacy education and awareness, privacy policy and standards development, privacy assurance services such as Privacy Impact Assessments (PIAs), incident management and access and complaint procedures.

Policies and Procedures

eHealth Ontario shall develop and implement security, privacy and data protection policies, standards, and procedures in a co-ordinated manner. eHealth Ontario shall maintain tools and mechanisms that support the Agency in assessing the privacy and data protection implications of any of eHealth Ontario's activities.

eHealth Ontario shall define accountabilities and responsibilities for privacy and data protection in its agreements with clients, vendors, and Personnel.

Training, Awareness and Standard of Conduct

All eHealth Ontario Personnel must sign the Acknowledgement and Agreement of the Privacy and Security Standard of Conduct prior to commencing their work with the Agency. This acknowledgement advises personnel that they are required to complete privacy and data protection training within thirty (30) days of beginning work at eHealth Ontario, and annually thereafter. The Agency shall maintain procedures and any other supporting mechanisms necessary to allow it to monitor and ensure compliance with training requirements.

The Chief Privacy and Security Officer is responsible for ensuring that appropriate privacy training and awareness programs are in place at eHealth Ontario. The Agency shall review its privacy and data protection training content every two years, or more frequently at the discretion of the Chief Privacy and Security Officer. The Agency shall update such privacy and data protection training content to address

any substantive changes to eHealth Ontario's policy and requirements and any other issues that the Chief Privacy and Security Officer deems to be appropriate.

Safeguards

eHealth Ontario shall protect PI and PHI with technical, administrative, and physical safeguards appropriate to its sensitivity. eHealth Ontario shall assess the privacy and data protection implications of any proposed security safeguards.

Compliance: Monitoring, Incident Management and Enforcement

eHealth Ontario shall develop and implement a program to proactively measure, assess and report on the Agency's compliance with its privacy policies and standards. eHealth Ontario shall ensure that privacy risks are identified, monitored, managed and subject to mitigation and shall implement tools and methods to achieve that objective.

eHealth Ontario shall conduct privacy and data protection compliance reviews on a basis and schedule proposed by the Chief Privacy and Security Officer and accepted, or directed, by the Audit Committee of the eHealth Ontario Board of Directors.

eHealth Ontario shall define appropriate performance metrics for privacy and data protection. The Chief Privacy and Security Officer shall regularly report on such metrics to the eHealth Ontario Executive Committee and, as required, to the eHealth Ontario Board of Directors.

eHealth Ontario shall investigate and respond effectively to any suspected or actual privacy or security incidents or breaches. The Agency shall maintain the Enterprise Security and Privacy Incident Management (ESPIM) program to achieve this objective. eHealth Ontario shall provide a means for its Personnel to report privacy and data protection concerns in confidence and ensure that measures are taken such that reporting Personnel suffer no reprisals.

eHealth Ontario shall provide a means for any person to submit a complaint, or other feedback, about eHealth Ontario's privacy and data protection practices to eHealth Ontario. eHealth Ontario shall review every complaint, or other feedback, and make changes to its policies and practices where appropriate.

The Chief Privacy and Security Officer shall maintain procedures to receive, manage, and monitor complaints and other feedback, and make information about these procedures available through its website. Copies of these procedures are also available from the Chief Privacy and Security Officer.

5 Responsibilities

The Board of Directors of eHealth Ontario is accountable for the protection of privacy and delegates authority to the Chief Executive Officer (CEO) to implement measures to protect privacy and data protection at the Agency. The CEO may delegate an individual to act on his or her behalf and appoints the Chief Privacy and Security Officer in this capacity.

eHealth Ontario Personnel and Third Parties shall comply with all eHealth Ontario privacy policies, to the extent that those policies are applicable to their activities. eHealth Ontario may apply sanctions to Personnel violating this Policy consistent with the Agency's disciplinary and procurement policies and procedures, up to and including civil liability, criminal sanctions, and dismissal or termination of contract.

Where there is a discrepancy or gap between this Policy and *FIPPA* or *PHIPA*, the regulations made under those Acts, or with eHealth Ontario's enabling regulation, the legislation or regulation shall take precedence. Where there is a discrepancy or gap between this Policy and subordinate eHealth Ontario privacy and data protection policies, this policy shall take precedence.

The Chief Privacy and Security Officer shall maintain the policies, standards, procedures, guidelines, and tools required to support effective management of privacy by the Agency. The Chief Privacy and Security Officer shall be responsible for implementing and enforcing this Policy, and eHealth Ontario Management and other eHealth Ontario Personnel assist the Chief Privacy and Security Officer as required. The Chief Privacy and Security Officer shall serve as the ultimate authority for interpretation of this Policy.

The Chief Privacy and Security Officer shall review and update this Policy every two years, or more frequently at his or her discretion. In doing so, the Chief Privacy and Security Officer shall consult with relevant eHealth Ontario Divisions, as appropriate, during the review process. The CEO shall approve this Policy on the recommendation of the Chief Privacy and Security Officer.

6 Supporting Policies, Standards and Procedures

- *eHealth Ontario Personal Information Privacy Policy*
- *eHealth Ontario Personal Health Information Privacy Policy*
- *eHealth Ontario Freedom of Information and Protection of Privacy Access Policy*
- *eHealth Ontario Privacy Impact Assessment Policy*
- *eHealth Ontario Privacy and Security Employee Standard of Conduct*
- *eHealth Ontario Privacy Feedback and Complaint Procedure*