eHealth Ontario

Personal Health Information Privacy Policy

Privacy Office

Document ID: 2478

Version: 6.3

Owner: Chief Privacy Officer

Sensitivity Level: Low

Ontario
eHealth Ontario

Contents

Tables

1 Purpose / Objective

The purpose of this privacy policy is to establish mandatory requirements and responsibilities for the protection of personal health information (PHI) that is received or sent by eHealth Ontario.

PHI generally means identifying information about an individual in oral or recorded form that relates to their physical or mental health. Examples include family health history, health card number, and any information that identifies an individual and links them to a healthcare provider.

eHealth Ontario is committed to being a leader in privacy, and fostering trust and confidence with its clients and the public. Therefore the requirements in this Policy go beyond the requirements laid out in legislation and regulation, and reflect best practices for information management for the protection of PHI.

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:

- *Personal Health Information Protection Act, 2004* (PHIPA), S.O. 2004, c. 3, with particular reference to:
  - s. 10
  - s. 17
- *Ontario Regulation (O. Reg.) 329/04* made under PHIPA, with particular reference to:
  - S. 6
  - s. 6.1
  - s .6.2
- O. Reg. 43/02 made under the *Development Corporations Act, R.S.O. 1990*, c. D. 10.

Section 6.2 of PHIPA O. Reg. 329/04, as amended by O. Reg. 331/11 in June 2011, clarifies eHealth Ontario's role in creating or maintaining one or more electronic health records (EHRs) and specifies eHealth Ontario's responsibilities and obligations in this role. Under section 6.2 of the regulation, eHealth Ontario is not considered to be collecting or disclosing PHI when it is creating or maintaining EHRs. This amendment applies to eHealth Ontario until January 1, 2017, when the amended regulation section expires and/or until otherwise determined.

See section 3 below for the roles under PHIPA that eHealth Ontario could potentially fill, and the obligations under PHIPA that pertain to each of these roles.

Where the repository or system is governed by the EHR Privacy Policies, follow the appropriate policies and procedures outlined in the *eHealth Ontario Electronic Health Record Privacy Policies*.

Application

This Policy applies to all eHealth Ontario personnel and third party service providers whom it has retained. It applies to all services and corporate activities that may impact the privacy of PHI in eHealth Ontario's care. Applicable provisions of this Policy shall be addressed in eHealth Ontario's agreements with third party service providers and end-users of eHealth Ontario's services.

Other Policies

This privacy 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 PHI. 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*

3 Overview of PHIPA

3.1 General

PHIPA is a provincial health privacy statute. It establishes rules for the management of PHI and protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services.

In developing, delivering and maintaining solutions and services, eHealth Ontario must comply with the requirements particular to roles described in PHIPA and its regulation. 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 services that eHealth Ontario provides to them.

eHealth Ontario may act in a number of capacities, as described in PHIPA and its regulation: under section 6.2 of O. Reg. 329/04, health information network provider (HINP), agent to a HIC, electronic service provider (ESP), or service provider to a HINP. Each role is focused around eHealth Ontario's relationship to one or more health information custodians (HICs).

3.2 Health Information Custodian

A HIC is a person or organization that delivers healthcare services. Physicians, hospitals, pharmacies, laboratories, community care access centres and the Ministry of Health and Long-Term Care (MOHLTC) are examples of HICs. eHealth Ontario is not a HIC.

A HIC has custody or control of PHI as a result of the work it does. The HIC has the right to deal with the PHI and create records the responsibility to maintain the confidentiality and security of the PHI. Though the HIC is the owner of the materials and systems in which information is recorded (e.g., paper charts, computers or information technology systems), patients are the owners of their PHI.

3.3 PHIPA O.Reg. 329/04

Section 6.2 of PHIPA O. Reg. 329/04 was amended in June of 2011 to clarify eHealth Ontario's role in creating or maintaining one or more EHRs as a service for HICs. Under the amended s. 6.2 of the Regulation to PHIPA, eHealth Ontario has the authority to create records of PHI in electronic form to enable health information custodians to use electronic means to disclose PHI to one another for the purpose of providing or assisting in the provision of health care to the individual whose PHI is contained in the record.

eHealth Ontario may have PHI within its systems during service provision; however the HIC remains fully accountable to the patient forthe privacy practices associated with the PHI.

3.4 Health Information Network Provider

As a HINP, eHealth Ontario provides services to two or more HICs primarily to enable them to use electronic means to disclose PHI to one another. eHealth Ontario acts in this capacity in a number of its business relationships.

For example, eHealth Ontario is a HINP when it provides ONE® Network services to thousands of HICs to enable them to disclose PHI to one another over this secure network.

As a HINP, eHealth Ontario may have PHI within its systems during service provision; however the HIC remains fully accountable to the patient for the privacy practices associated with the PHI.

3.5 Electronic Service Provider

As an electronic service provider (ESP), eHealth Ontario supplies services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain, or dispose of PHI. For example, eHealth Ontario may host a clinical management service that is used by physicians.

When eHealth Ontario is acting as an ESP, its privacy obligations are defined by an agreement between eHealth Ontario and the HIC. Under this authority, eHealth Ontario has no independent decision-making role regarding, or interest in, PHI, but acts in accordance with the directions of the HICs it serves, within the prescribed limits defined by PHIPA.

3.6 Agent

As an agent to a HIC, eHealth Ontario acts for or on behalf of the HIC in respect of collecting, using or disclosing PHI, for the purposes of the HIC, and not the agent's own purposes. For example, MOHLTC may designate eHealth Ontario as its agent to manage an electronic index of patients in Ontario.

A HIC may permit eHealth Ontario to access, 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 does 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 Policy

This Policy is structured around the *10 Fair Information Principles of the Canadian Standards Association's Model Code for the Protection of Personal Information* (CSA Model Code)[1]. The CSA Model Code, was recognized as a national standard for privacy protection in 1996, and is used across Canada as the basis for health information privacy legislation, including PHIPA.

4.1 Principle 1: Accountability

The principle of accountability means that an organization is responsible for PHI under its control and has designated an individual or individuals who are accountable for the organization's compliance with privacy principles.

[1] Canadian Standards Association, "CAN/CSA – Q830-96, Model Code for the Protection of Personal Information," March 1996.

4.1.1 Accountability of eHealth Ontario

The Board of Directors of eHealth Ontario is accountable to HICs and patients for the protection and privacy of the PHI with which it has been entrusted. eHealth Ontario is committed to ensuring the highest standard of privacy care and data protection is applied in the services and technologies it manages.

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

The CPO is responsible for overseeing eHealth Ontario's Privacy Office. The CPO is responsible for implementing eHealth Ontario's privacy policies and program throughout the organization.

Key components of eHealth Ontario's privacy program include:

- A suite of privacy policies and procedures which support the effective management and operationalization of privacy by eHealth Ontario;
- A comprehensive and role-based privacy training and awareness program for personnel and third party service providers;
- Up-to-date and accurate privacy assessments of eHealth Ontario's systems and services which involve PHI;
- Privacy risk management activities throughout the full lifecycle of eHealth Ontario's systems and services which involve PHI; and
- A network of individuals across the organization with specific privacy responsibilities.

The responsibilities of the CPO include:

- ensuring the Privacy Office is informed of new services or corporate activities that involve PHI;
- ensuring that responsible parties allocate sufficient time and funds in their project plans to conduct Privacy Threshold Assessments (PTAs) and/or Privacy Impact Assessments (PIAs) in accordance with *eHealth Ontario's Privacy Impact Assessment Policy*;
- ensuring the availability and cooperation of sufficient personnel to facilitate information collection and documentation pertaining to the service under privacy analysis; and
- implementing PTA and/or PIA recommendations.

The Vice President, Strategic Sourcing and Vendor Management is accountable for ensuring the privacy requirements established by the CPO are applied in agreements with third party service providers that require access to eHealth Ontario information, physical sites, information assets or information systems (including remote access) or handle PHI on eHealth Ontario's behalf.

eHealth Ontario personnel and third party service providers shall comply with all eHealth Ontario privacy policies, to the extent that those policies are applicable to their activities.

eHealth Ontario's Privacy Office has responsibility for defining and oversight of the day-to-day operations within the Agency that are meant to protect PHI and privacy. The Privacy Office, in collaboration with relevant eHealth business units, will maintain the privacy protocols that eHealth has established in its privacy policies, procedures and other governing artefacts.

eHealth Ontario may apply sanctions to personnel and third party service providers acting on eHealth Ontario's behalf found in violation of this Policy consistent with the Agency's disciplinary and procurement policies and procedures, may include invoking measures up to and including dismissal or termination of contract.

4.1.2 Agreements

The purpose of agreements is to formally establish roles and responsibilities related to the management and protection of PHI. eHealth Ontario enters into agreements with all individuals and entities:

- to which eHealth Ontario provides services, before providing those services, including end-users, HICs and HINPs; and

- that provide services to eHealth Ontario, before they provide those services, including eHealth Ontario personnel and third party service providers.

Agreements shall address, where applicable, the following areas:

- applicable legislative responsibilities and obligations
- mutual roles and responsibilities, processes and safeguards for the protection of PHI;
- the handling of PHI;
- the conditions under which parties may access PHI, and the scope of PHI each party can access;
- roles and responsibilities for managing privacy incidents and breaches;
- roles and responsibilities regarding the service provided;
- processes and mutual obligations regarding monitoring and compliance;
- penalties for breaches of the agreement; and
- privacy schedule (for third party service providers, where applicable).

Under PHIPA, when eHealth Ontario is acting under s. 6.2 of PHIPA O. Reg. 329/04 for the purposes of creating or maintaining one or more EHRs, the Agency is not required to enter into agreements with those HICs. However, eHealth Ontario is committed to implementing best practices that are over and above its obligations under PHIPA and to building trust within and outside the health sector. eHealth Ontario therefore commits to enter into agreements with all entities and individuals that handle PHI (including HICs, agents, HINPs, end-users, MOHLTC and third parties that assist in providing services), to the extent reasonable, in order to ensure that PHI is protected and privacy is respected.

eHealth Ontario retains and manages agreements through a central corporate function.

eHealth Ontario maintains tools and procedures to ensure that agreements are monitored and updated as required.

Any agreement eHealth Ontario enters into with third parties to support its provision of services to HICs and HINPs shall ensure that the third party agrees to comply with all applicable legislation, restrictions, conditions and requirements to which eHealth Ontario is also bound.

4.1.3 Information Management

eHealth Ontario's policies and procedures for the protection of PHI and patient privacy are key components of the Agency's information management approach. This approach places all eHealth Ontario repositories of PHI within a matrix of roles and responsibilities, high-level business and operational processes, and safeguards and controls.

eHealth Ontario protects the PHI with which it has been entrusted, throughout its full lifecycle, from the time the PHI enters the Agency's care until the time it is destroyed according to its records retention schedule.

Information management includes procedures and processes for PHI retention and destruction. Detailed policy on PHI lifecycle management is found in section 4.5.

eHealth Ontario's information management approach defines roles for all eHealth Ontario business units that play a role in the protection of PHI – most notably Security Services, but also Procurement, Legal, Risk Management and Operations. These roles are defined as part of a high-level information management RACI (responsible, accountable, consulted, informed) matrix. eHealth Ontario's Privacy Office facilitates the definition of all relevant roles.

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 PHI 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.

4.1.4 Compliance Monitoring

eHealth Ontario proactively monitors compliance with its policies and procedures that include the safeguards and controls it has put in place to protect PHI in its systems.

The compliance of eHealth Ontario's personnel and third party service providers with which eHealth Ontario has agreements (specifically HICs and third party suppliers with access to PHI) is monitored on an ongoing basis, in a manner which allows the Agency to measure, assess and report on compliance with its privacy policies and standards. The CPO regularly reports compliance monitoring results to the eHealth Ontario Executive Committee and, as required, to the eHealth Ontario Board of Directors.

eHealth Ontario supports the HICs that use its services in meeting their own compliance monitoring obligations with regard to these services.

As a key component of safeguarding PHI, compliance monitoring is addressed in greater detail in section 4.6.

4.1.5 Privacy Incident and Breach Management

eHealth Ontario takes all necessary measures to address any access, collection, use, disclosure, copying, modification, retention or disposal of PHI in its systems that is not in accordance with relevant legislation – specifically PHIPA – or with eHealth Ontario policies and procedures.

eHealth Ontario's Privacy and Breach Management Policy describes the Agency's approach to privacy 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) and Security Incident Response (SIR) programs.

In accordance with the *Privacy Incident and Breach Management Policy*, 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 – the primary notification being to the HIC or HICs that have actual custody of the PHI that was subject to the incident or breach.

4.1.6 Training and Awareness

eHealth Ontario is dedicated to fostering a robust culture of privacy awareness amongst eHealth Ontario personnel and third party service providers which it retains. eHealth Ontario therefore has in place a comprehensive enterprise-wide privacy and security training and awareness program, which provides eHealth Ontario's personnel and third party service providers with:

- an overview of PHIPA and eHealth Ontario's obligations under privacy legislation;
- a description of their privacy responsibilities;
- role-based privacy responsibilities for those who may require access to PHI where it is appropriate based on the person's job/contractual responsibilities;
- information on the physical, technical and administrative safeguards that eHealth Ontario has in place to protect PHI; and
- the process for identifying and reporting potential or actual privacy incidents or breaches and security incidents.

Training content shall be reviewed annually, or more frequently at the discretion of the CPO. The content shall be updated to address any substantive changes to eHealth Ontario's statutory, regulatory and policy requirements, and any other issues that the CPO deems to be appropriate.

All eHealth Ontario personnel shall complete the enterprise-wide Privacy and Security Fundamentals Training within 30 days of beginning work at the Agency, and annually thereafter.

eHealth Ontario shall deliver role-based privacy and security training for its personnel who may require access to PHI in order to carry out their assigned duties.

eHealth Ontario personnel who may have access to PHI as part of their duties must complete privacy and security role-based training prior to being granted access to any PHI.

HICs and third party service providers are responsible for providing privacy and security training to their staff and representatives. eHealth Ontario supports HICs and third party service providers in providing privacy and security training with respect to eHealth Ontario's services (e.g., policies regarding privacy incident and breach management). eHealth Ontario third party service providers must complete privacy and security training as directed by eHealth Ontario.

eHealth Ontario maintains procedures and any other supporting mechanisms necessary to allow it to track training completion and ensure compliance with training requirements.

4.1.7 Standard of Conduct

All eHealth Ontario personnel and third party service providers must formally acknowledge and agree with the *eHealth Ontario Privacy and Security Standard of Conduct* prior to commencing work at the Agency and annually thereafter.

eHealth Ontario provides a *Standard of Conduct* to its personnel and third party service providers which details their privacy and security responsibilities and obligations.

4.1.8 Public Accountability and Transparency

eHealth is dedicated to making its privacy program, and the measures it takes to protect PHI, as clear and accessible as possible. eHealth Ontario provides plain language descriptions of its privacy services and safeguards and, in this Policy, clear discussions of relevant legislation and regulations – in particular, PHIPA and PHIPA O. Reg. 329/04.

Additionally, eHealth Ontario provides reporting on audit logs where required, makes available plain language summaries of its Privacy Impact Assessments, and provides a clear process for managing privacy-related complaints and inquiries. Details on these measures can be found in this Policy, in sections 4.6, 4.7, 4.8 and 4.9.

4.2 Principle 2: Identifying Purposes

The principle of identifying purposes means that the purposes for which PHI is collected shall be identified by the organization at or before the time the information is collected.

It is the responsibility of the HIC who collects PHI to inform the patient of the purposes for which the PHI will be collected, used and disclosed.

The purposes for which eHealth Ontario is permitted to use PHI are listed in this Policy in section 4.5. *eHealth Ontario Directory of Records*, found on eHealth Ontario's website, includes a Statement of Purpose for each data repository. eHealth Ontario shall act in accordance with the Statement of Purpose in respect of sharing, collecting, using or disclosing data, as appropriate, contained within each repository that it manages.

4.3 Principle 3: Knowledge and Consent

The principle of consent means that the knowledge and consent of the individual are required for the collection, use or disclosure of PHI, except when inappropriate.

Consent is the permission that a patient gives to a HIC to collect, use, or disclose his or her PHI. Consent must be knowledgeable, transparent and meaningful; must relate to the information collected, used or disclosed by the HIC for a particular purpose; and must be obtained without deception or coercion.

An individual has the right to establish a consent directive on their PHI. A consent directive is an express instruction of an individual to their HIC regarding the use or disclosure of their PHI. Consent directives include:

- the withdrawal of consent to share or use PHI for healthcare purposes (which results in the patient's record being blocked); and
- the reinstatement of consent to share PHI for the purpose of providing or assisting in the provision of healthcare and treatment (which results in the patient's record being unblocked).

HICs can generally rely on implied consent (assuming the patient is knowledgeable) to collect, use and disclose PHI for the purpose of providing healthcare or assisting in providing healthcare.

A HIC must obtain express consent (consent that is explicitly and directly given by the patient in oral or written form) when using or disclosing PHI for a reason other than that for which it was collected.

4.3.1 eHealth Ontario's Role in Managing Consent

eHealth Ontario shall assist HICs in meeting their obligations under PHIPA for consent by providing in its services, the mechanisms for HICs to record patient consent and manage consent directives – specifically, creating and revoking consent directives, overriding directives, and logging and alerting of overrides.

eHealth Ontario shall maintain up-to-date requirements for the design and implementation of consent management processes into its services and systems. Consent directives shall be consistently documented to the extent reasonable and practical and retained in a secure environment.

eHealth Ontario will not access PHI that has been blocked as a result of a consent directive unless it is absolutely necessary to do so in accordance with PHIPA. If the PHI must be accessed, the access will be logged, and constrained in accordance with the relevant eHealth Ontario information security requirements on system access control, and in accordance with the access control requirements in this Policy.

4.4 Principle 4: Limiting Collection

The principle of limiting collection means that the collection of PHI shall be limited to that which is necessary for the purposes identified by the organization. PHI shall be collected by fair and lawful means.

eHealth Ontario does not 'collect' PHI, as that term is defined in PHIPA, for its own purposes. eHealth Ontario collects PHI only as directed by the HICs to which it is providing services when it is acting as an Agent under PHIPA.

When eHealth Ontario is creating or maintaining one or more EHRs, eHealth Ontario is not *collecting* PHI as the term is defined in PHIPA.

HICs determine what PHI, from the information they collect from patients, is provided to eHealth Ontario, and for what purposes. eHealth Ontario is permitted to receive only the information that the HICs share.

4.5 Principle 5: Limiting Use, Disclosure and Retention

The principle of limiting use, disclosure and retention means that PHI shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. eHealth Ontario does not 'use' or 'disclose' PHI, as those terms are defined in PHIPA, for its own purposes. .

eHealth Ontario shall not provide PHI if other information, namely de-identified and or/aggregate information, will serve the purpose, and shall not provide more PHI than is reasonably necessary to meet the purpose. Where de-identifying PHI, de-identification will occur in accordance with the IPC *De-identification Protocols: Essential for Protecting Privacy, 2014,* or other comparable best practice standard.

4.5.1 eHealth Ontario's Use of PHI

eHealth Ontario only uses PHI as directed by the HICs to which it is providing services when it is acting as an Agent under PHIPA.

The following activities are considered to be permitted and necessary uses of PHI by eHealth Ontario:

- handling PHI in order to create and maintain EHRs;

- handling PHI for pre-production testing; or
- incidental access to PHI for the purposes of providing services including maintenance, support, investigating incidents and breaches and monitoring (refer to section 4.5.4).

Permitted and necessary uses of PHI shall be established through agreements between eHealth Ontario and HICs, and guided at all times by relevant requirements in PHIPA.

4.5.2 eHealth Ontario's Disclosure of PHI

eHealth Ontario shall disclose PHI only as directed by the HICs to which it is providing services when it is acting as an Agent under PHIPA, or when permitted or required to do so by law.

According to PHIPA and its regulations, when PHI is provided to eHealth Ontario by a HIC for the purposes of creating or maintaining one or more EHRs, the HIC is not considered to be *disclosing* the PHI to eHealth Ontario, nor is eHealth Ontario considered to be *collecting* the PHI, as these terms are defined in PHIPA.

eHealth Ontario does not *disclose* PHI to HICs when it is creating or maintaining one or more EHRs. eHealth Ontario receives PHI from and sends PHI to authorized HICs for the purpose of providing or assisting in the provision of healthcare services.

4.5.3 eHealth Ontario's Retention of PHI

eHealth Ontario retains PHI only as directed by the HICs to which it is providing services when it is acting as an Agent and HINP under PHIPA.

eHealth Ontario, when acting as an Agent or Electronic Service Provider, retains PHI for the duration of time required by HICs according to the HICs' statutory and policy requirements to the extent reasonable and practical. The PHI retention requirements are stipulated in eHealth Ontario's agreements with HICs.

- 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 Data Retention Schedule* (September 30, 2013).

eHealth Ontario, when creating or maintaining one or more EHRs, retains PHI in accordance with the *EHR Retention Policy*.

4.5.4 Access Control

Access controls are used to prevent unauthorized or inappropriate access to PHI, ensure the protection of eHealth Ontario's services, prevent unauthorized computer access, detect unauthorized or inappropriate activities and ensure information security.

eHealth Ontario only grants access to PHI to authorized persons based on the principle of least privilege, meaning that only those personnel and third party service providers who require access to PHI receive access and that personnel and third party service providers are given access only to the PHI required by them to fulfill the requirements of their job.

eHealth Ontario shall ensure access control is based on roles and responsibilities. It shall maintain an access control matrix that maps roles to types of access to PHI. Access privileges for each role shall include details on what information or service can be accessed and the type of the access (e.g., read-only, read and update) that is permitted.

eHealth Ontario shall identify the reasons for and methods of access to PHI in agreements with HICs and third party service providers.

4.5.4.1 Access by eHealth Ontario Personnel

Most eHealth Ontario personnel never have access to the PHI that HICs provide when using eHealth Ontario's services. However in any information technology environment, a limited number of specialized personnel may be required to access, or will have incidental access to, sensitive information such as PHI in order to provide technical or

support services to clients. As an example, eHealth Ontario personnel may have incidental access to PHI when they troubleshoot a problem with a client's system.

eHealth Ontario allows access to PHI by its authorized personnel only for the permitted and necessary uses of PHI as described in section 4.5 of this Policy. Authorization is granted by the Privacy Office via the *eHealth Ontario Logical Access Request Process*. eHealth Ontario personnel are prohibited from accessing PHI for any other purpose.

eHealth Ontario ensures that separation of information technology duties is implemented to manage conflict of interest, the appearance of conflict of interest, and fraud.

eHealth Ontario's Security Services team maintains a list of roles to be assigned to personnel for the purposes of controlling access to the information repositories.

eHealth Ontario maintains procedures to ensure that:

- upon being interviewed, hired or contracted, personnel are aware of the need to maintain confidentiality and information security through explicit reference in job descriptions and contracts;
- upon hiring or contracting, personnel are assigned just those access privileges required to fulfill their job functions;
- during the course of employment or contract, the access privileges assigned to personnel are periodically reviewed to ensure they are still required;
- immediately following change of employment or contract, access privileges assigned are reviewed for appropriateness; and
- immediately following termination of employment or contract, access to any information repositories is promptly terminated.

eHealth Ontario personnel who require access to information assets from a remote location must obtain approval from eHealth Ontario's Privacy Office and Security Services prior to being granted remote access.

4.5.4.2 Access Logging

eHealth Ontario keeps an electronic record of accesses to all or part of the PHI contained in an EHR and ensures the record identifies the person who accessed the information, and the date, time and location of the access.

eHealth Ontario makes available to a HIC, on request, logging reports regarding eHealth Ontario's access to PHI that is in the HIC's custody and/or control.

An authorized person is one who requires access to the PHI as part of their duties and has an appropriate level of authority, training and security screening to warrant access.

Authorized persons who have been granted access to PHI 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, policies and contractual agreements to ensure the security and integrity of the PHI.

eHealth Ontario personnel who may have access to PHI as part of their duties must complete role-based privacy and security training prior to being granted access to any systems containing PHI.

4.5.4.3 Access by End-Users

An end-user is a HIC or a person who is authorized by a HIC to use an eHealth Ontario service.

eHealth Ontario maintains an end-user registration process that is followed for each end-user prior to being provided an account and granted access to PHI. The end-user identity verification requirements include:

- the accurate capture of an end-user's identity (e.g., name, date of birth, current address, health professional identifier);
- verification of identity through trusted mechanism;
- the accurate capture, after verification, of a user's enduring professional credentials (e.g., medical specialty and/or job title); and

- the assignment of an unambiguous user identifier.

eHealth Ontario manages and terminates end-user accounts in accordance with guidelines set out by information security. eHealth Ontario ensures strong authentication is required for end-user access to PHI. Two-factor authentication means that, to access the eHealth system, the end-user requires both a password and some other authenticating mechanism, such as an access token.

4.5.4.4 Access by Service Providers

eHealth Ontario defines authorized accesses to PHI for service providers through its agreements with these providers. Third party service providers with access to PHI will be subject to the same conditions and constraints, where relevant, as eHealth Ontario personnel regarding the handling of PHI. These conditions include the signing of confidentiality agreements, participation in privacy and security awareness training, explicit approval for remote access, etc.

eHealth Ontario assigns unique credentials to each service provider with access to PHI in its systems. Service providers are not permitted to share access credentials.

4.6 Principle 6: Accuracy

The principle of accuracy means that PHI shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used.

The accuracy of PHI is the responsibility of the HIC who collects it. Any corrections or changes to PHI must be completed only by the HIC who has custody and/or control of the PHI.

eHealth Ontario, where possible, provides mechanisms to HICs to support the accurate entry of PHI into eHealth systems (such as input validation controls). eHealth Ontario also maintains, through its information security practices, mechanisms to protect the integrity of PHI (see section 4.7 below).

eHealth Ontario ensures that the integrity of PHI sent to eHealth Ontario by HICs is maintained and protected at rest and in transit. Integrity means that the PHI has not been altered inadvertently or improperly, and can be relied upon for the purposes for which it was collected.

eHealth Ontario provides a mechanism for HICs to enter notice of disagreements into an EHR with regards to the accuracy of the PHI contained within the EHR.

4.7 Principle 7: Safeguards

The principle of safeguards means that PHI shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1 Security Safeguards

Information security procedures and controls are essential to protect the privacy of PHI, while permitting healthcare professionals to access the information they need to make patient care decisions. eHealth Ontario has in place an *overarching eHealth Ontario Information Security Policy*, which provides an extensive policy framework for the protection of all of eHealth information assets – in particular PHI.

eHealth Ontario's information security policies and procedures specify the manner in which eHealth Ontario protects PHI. This protection encompasses administrative, technical and physical safeguards appropriate to the level of sensitivity of the information, including:

- mandatory encryption of PHI in transit or on mobile devices;
- Threat and Risk Assessments (TRAs) ;
- audit logging;
- monitoring;
- access control and login reports;

- security training; and
- secure destruction of records.

eHealth Ontario implements measures to protect PHI from unauthorized access, disclosure, copying, use, modification, loss or destruction, regardless of the format and media in which it is stored.

eHealth Ontario's requirements for administrative, technical and physical security safeguards to protect PHI are detailed in its *eHealth Ontario Information Security Policy* available on eHealth Ontario's website.

eHealth Ontario provides to the HICs and to the public a general description of its services and the safeguards it has in place to protect the integrity, security and confidentiality of PHI. This information is available on eHealth Ontario's website.

4.7.2 Compliance Monitoring

eHealth Ontario ensures that individuals with access to PHI through eHealth services comply with PHIPA, its regulation and eHealth Ontario's policies and procedures.

Specifically, eHealth Ontario monitors the compliance of:

- personnel with internal eHealth Ontario policies and procedures; and
- service providers with contractual obligations as established in agreements.

eHealth Ontario provides mechanisms and services to HICs to assist them in meeting their compliance monitoring obligations (e.g., reports on audit logs related to any PHI in the custody of a HIC).

eHealth Ontario conducts privacy and data protection compliance reviews on a basis and schedule proposed by the CPO and accepted, or directed, by the Audit Committee of the eHealth Ontario Board of Directors.

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.

eHealth Ontario provides 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 (see the *eHealth Ontario Complaints and Inquiries Policy and Procedure* for more detail).

eHealth Ontario employs both automated and manual monitoring processes that, wherever possible, are meant to *prevent* rather than *expose* incidents of non-compliance.

eHealth Ontario shall execute a systematic and transparent set of monitoring processes including but not limited to the following:

- audit logging program to track key dimensions of PHI handling, including:
    - access to PHI by all roles;
    - transfers of PHI from HIC to HIC;
    - changes to, and overrides of, consent directives;
- business process monitoring, including self-assessments, random walkabouts, process audits (e.g., of incident and breach management processes and complaint handling processes);
- contract enforcement, including timely exercise of audit and monitoring clauses;
- execution of privacy training and awareness;
- renewal of confidentiality agreements and statements of acceptable use; and
- regular review of audit log reporting thresholds.

eHealth Ontario will not limit reporting on compliance monitoring only to technical data, but also to business processes, through such metrics as time within which incidents and breaches are contained, or compliance with completion of privacy training.

4.7.3 Privacy Impact Assessments

eHealth Ontario conducts PIAs on every eHealth Ontario service that involves PHI in accordance with its *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*.

4.8 Principle 8: Openness

The principle of openness means that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of PHI.

PHI that is being managed by eHealth Ontario belongs to the individual the information is about. eHealth Ontario has a responsibility to be open and transparent about how it manages and protects PHI, and to inform individuals of their privacy rights.

eHealth Ontario makes available to HICs and the public:

- a plain language description of PHIPA and its regulations which apply to eHealth Ontario;
- eHealth Ontario's roles and obligations under PHIPA and its regulations;
- the rights of individuals under PHIPA within the context of eHealth Ontario policies and procedures (e.g., individual access, correction, complaints, consent directives);
- eHealth Ontario's PHI-related policies and procedures (without providing or making available any information that could reasonably be expected to compromise the security of eHealth Ontario's services or the confidentiality of PHI);
- the accountabilities related to the protection of PHI;
- a plain language description of the EHR and a general description of the administrative, technical and physical safeguards in place to protect the EHR and the PHI contained in it; and
- summaries of results of PIAs where required

eHealth Ontario reviews the information about its privacy practices which it makes available to the public on an annual basis and updates it as appropriate or when directed by the CPO.

4.9 Principle 9: Individual Access

The principle of individual access means that upon request, an individual shall be informed of the existence, use and disclosure of their PHI and shall be given access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Under PHIPA, an individual has the right to access a record of their PHI that is in the custody or under the control of a HIC (such as a doctor or a hospital). In response to a written request for access, the HIC is required to either grant the request and provide access, or deny access based on a set of exemptions set out in PHIPA. Individuals also have a right to ask the HIC to correct any inaccurate or incomplete information.

Under the provisions of PHIPA, eHealth Ontario is not responsible for individual requests to access or correct PHI. If eHealth Ontario receives an access or correction request, it shall direct the individual to the appropriate HIC(s) to respond to the request.

4.10 Principle10: Challenging Compliance

The principle of challenging compliance means that an individual shall be able to address a challenge concerning compliance with the privacy principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1 Complaints About eHealth Ontario

Any person may submit a complaint and/or other feedback (including inquiries, compliments and suggestions) related to:

- eHealth Ontario's privacy and data protection practices;
- eHealth Ontario's information management practices; or
- non-compliance with eHealth Ontario's policies, or statutory or regulatory requirements.

Complaints and/or other feedback may be submitted by hand delivery, post, facsimile, e-mail, and telephone using the following eHealth Ontario contact information:

Privacy Office
eHealth Ontario
P.O. Box 148
Toronto, ON M5G 2C8
Fax: (416) 586-4397 or 1 (866) 831-0107
Email: privacy@ehealthontario.on.ca
Telephone: (416) 946-4767or 1 (888) 411 – 7742 ext 64767

eHealth Ontario accepts anonymous complaints and/or other feedback; however, it requires the sender's name and address, telephone number or e-mail address in order to provide the requester with a response in return.

eHealth Ontario provides a form on its corporate website that any person may use to submit a confidential complaint; this form indicates the scope of detail required for eHealth Ontario to initiate an investigation.

PHI should not be submitted with the description of the complaint or other feedback. eHealth Ontario may, however, request this level of detail during the course of its investigation. In doing so, eHealth Ontario obtains the appropriate consent as required.

The CPO reviews all complaints and/or other feedback. eHealth Ontario will make changes to its policies and practices based on the comments received.

eHealth Ontario acknowledges receipt of a complaint and/or other feedback within four (4) days of the receipt.

eHealth Ontario sends a response regarding the outcome of the investigation to the sender within 30 days of the receipt of the complaint and/or other feedback. If there is a delay in sending the response, the individual shall be notified via post of the expected, approximate time frame.

The CPO maintains procedures to receive, forward, manage, close 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 CPO.

4.10.2 Complaints About HICs

If eHealth Ontario is contacted with a complaint regarding a HIC's information management practices, eHealth Ontario shall forward the inquiry to the appropriate HIC, and advise the person making the complaint that the person will receive a response directrly from the HIC.

If, in eHealth Ontario's opinion, a complaint about a HIC could have an influence on contract enforcement and compliance monitoring activities, the Agency may choose to follow up on the investigation and mitigation of a complaint regarding a HIC.

4.10.3 Complaints to the IPC

The Information and Privacy Commissioner of Ontario (IPC) is an oversight body responsible for educating the public concerning their rights under privacy legislation and ensuring that organizations fulfill their obligations under the legislation. The IPC is appointed by the Ontario Legislature and is independent of the government of the day.

Individuals may file a complaint with the IPC if:

- they feel they have incorrectly been denied access to their PHI;
- a HIC refused to make a requested correction to their PHI;
- more than 30 days has passed since the access or correction request was made, and the individual has not received a decision; or
- they feel the HIC's estimate of fees is excessive.

All complaints to the IPC must be in writing. Potential complainants should either write a letter to the IPC, or fill in the form that is available from the IPC's website: https://www.ipc.on.ca/images/Resources/phipa-cudcmp-e_1.pdf. The form cannot be submitted electronically. It should be printed and mailed to the registrar of the IPC. Any relevant documentation should be attached to the complaint form.

Complainants have one year from the time they become aware of the problem to file the complaint. For access and correction complaints, complainants have a six-month time limit from the time they receive a HIC's decision to file these complaints.

Complaints should be sent to:

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Fax: 416-325-9195
TTY: 416-325-7539
Website: www.ipc.on.ca

5 Responsibilities

The CPO is considered the ultimate authority for interpreting, implementing and 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 PHI in a manner consistent with this Policy and applicable legislation.

6 Glossary

The following terminology and acronyms are associated with this Policy:

TERM	DEFINITION

Agent	Has the same meaning as defined in PHIPA, and generally means a person or organization that acts for or on behalf of the HIC in respect of collecting, using or disclosing the PHI in the HIC's custody, with the HIC's authorization and not for its own purposes.
Authorized Person	A person who requires access to PHI as part of their duties and has an appropriate level of authority, training and security screening to warrant access.
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.
De-identification	Has the same meaning as defined in the *Personal Health Information Protection Act, 2004*, and generally means the removal of any information that identifies the individual.
eHealth Ontario Records	All records created in the course of eHealth Ontario business activities.
eHealth Services	One or more services to promote the delivery of health care services in Ontario that use electronic systems and processes, information technology and communication technology to facilitate electronic availability and exchange of information related to health matters, including personal information and personal health information, by and among patients, health care providers and other permitted users. (Enabling Regulation, s.1)
Electronic Health Record (EHR)	Has the same meaning as defined in PHIPA, and generally means a record of PHI in electronic form created or maintained by eHealth Ontario.
Electronic Service Provider (ESP)	Has the same meaning as defined in PHIPA, and generally means a third party that is retained by a HIC to assist in providing services to a HIC. The services are for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain, or dispose of PHI.
End-user	A person who is authorized by a HIC to use an eHealth Ontario service.
Health Information Custodian (HIC)	Has the same meaning as defined in section 3 of *Personal Health Information Protection Act, 2004* (PHIPA), and generally means a person or organization that delivers healthcare services. Examples include: physicians, hospitals, pharmacies, laboratories, community care access centres and the Ministry of Health and Long-Term Care, but not eHealth Ontario.
Health Information Network Provider (HINP)	Has the same meaning as defined in PHIPA, and generally means an organization that provides services to two or more HICs primarily to enable them to use electronic means to disclose PHI to one another.

Personal Health Information (PHI)	Has the same meaning as defined in section 4 of the *Personal Health Information Protection Act, 2004* (PHIPA), 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. Examples include family health history, health card number, and any information that identifies an individual and links them to a healthcare provider.
***Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3. (PHIPA)**	A provincial health privacy statute that establishes rules for the management of PHI and protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services.
Personnel	Collectively, the following: current and former Employees; current Suppliers; and current and former Appointees. Where: • Employee: A person whom through the execution of a contract of service, has entered into an employment relationship with eHealth Ontario and is classified in one of the following categories, as defined by the eHealth Ontario Human Resources Department: Full-Time Regular Employee, Full-Time Temporary Employee, Part-Time Regular Employee or student. • Supplier: Also referred to as a third party service provider. An individual who or entity that supplies goods or services to eHealth Ontario, and is paid through the eHealth Ontario accounts payable system. • Appointee: An individual appointed by the Lieutenant Governor in Council as a member of the board of directors of eHealth Ontario under Ontario Regulation 43/02, "eHealth Ontario", made under the *Development Corporations Act*, *1990*, as amended from time to time.
Privacy Impact Assessment (PIA)	A detailed assessment undertaken to evaluate the effects of a new or significantly modified service to determine its actual and potential impact on the protection of PI/PHI included in the service. PIAs measure compliance with applicable privacy law and broader privacy implications. A PIA addresses all technological components, business processes, flows of personal information, information management controls and human resource processes associated with a service and identifies ways in which privacy risks associated with these may be mitigated.
Privacy Breach	A privacy breach includes the collection, use or disclosure of PI/PHI that is not in compliance with applicable privacy law, or circumstances where PI/PHI is stolen lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.
Privacy Incident	A privacy incident includes circumstances where there is a contravention of the privacy policies, procedures or practices implemented by eHealth Ontario or agreements which eHealth Ontario has entered into with external stakeholders and third party service providers, including but not limited to PHIPA agent agreements, data sharing agreements, confidentiality and non-disclosure agreements and agreements with third party service providers retained by eHealth Ontario, where this contravention does not constitute non-compliance with applicable privacy law. A privacy incident may also be a suspected privacy

	breach.
Privacy Threshold Assessment (PTA)	A preliminary, standardized privacy analysis utilized to determine whether or not a service will require the completion of further privacy assessment.

Table 1: Personal Health Information Policy: Glossary

7 References and Associated Documents

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

REFERENCE	LOCATION
Personal Health Information Protection Act, 2004 (PHIPA) and regulations	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_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 Inquiries and Complaints 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 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 Information Security policies and procedures	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 Health Information Policy: References and Associated Documents

8 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.