eHealth Ontario

Privacy Incident and Breach Management Policy

Privacy Office

Document ID: 2480

Version: 2.2

Owner: Chief Privacy Officer

Sensitivity Level: Low

Ontario
eHealth Ontario

Contents

Tables

1 Purpose / Objective

This Policy describes the manner in which eHealth Ontario will identify, contain, investigate, notify, report and remediate privacy incidents and breaches as defined in this Policy.

The eHealth Ontario Privacy Incident and Breach Management Policy must be read in conjunction with the *eHealth Ontario Privacy and Data Protection Policy*, *Personal Health Information Privacy Policy*, *Personal Information Privacy Policy* and applicable Privacy Breach Management (PBM) documents.

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. Applicable provisions of this Policy must be addressed in eHealth Ontario's agreements with third party service providers as required. This Policy applies to eHealth Ontario services which may impact the privacy of Personal Information (PI)/Personal Health Information (PHI) in the Agency's care.

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

3 Legislative Requirements

eHealth Ontario may act in a number of capacities, as described in the *Personal Health Information Protection Act*, 2004 (PHIPA) and its supporting regulation: under section 17 of PHIPA, under section 6.2 of Ontario Regulation (O. Reg.) 329/04, section 6 of O. Reg. 329/04 as a health information network provider (HINP), an electronic service provider (ESP), an agent or as a service provider to a HINP. Each role is focused around eHealth Ontario's relationship to one or more health information custodians (HICs).

Section 6 and section 6.2 of O.Reg. 329/04 requires t eHealth Ontario to put administrative, technical and physical safeguards in place to protect PHI against theft, loss, and unauthorized or inappropriate use or disclosure that is not in accordance with relevant privacy law. O.Reg. 329/04further requires eHealth Ontario to notify every applicable HIC at the first reasonable opportunity if the PHI it has provided to eHealth Ontario has been stolen, lost or accessed by unauthorized persons.

eHealth Ontario is an "institution" as defined in Ontario's *Freedom of Information and Protection of Privacy Act*, 1990, S.O. 2004, c. F.31 (FIPPA), as amended and is subject to its provisions. eHealth Ontario is committed to protecting PI subject to FIPPA and extending privacy protection practices to its handling of personal information where that information may not be subject to privacy laws or regulations.

4 Definitions

A privacy incident includes:

- A contravention of the privacy policies, procedures or practices implemented by eHealth Ontario, where this contravention does not result in unauthorized collection, use, disclosure and destruction of PI/PHI or does not result in non-compliance with applicable privacy law.
- A contravention of agreements which eHealth Ontario enters 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 suspected privacy breach.

A privacy breach includes:

- The collection, use or disclosure of PHI that is not in compliance with the PHIPA and its regulation.
- The collection, use or disclosure of PI that is not in compliance with the FIPPA and its regulations.
- Circumstances where PI/PHI is stolen lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.

Privacy incidents and breaches can be intentional or inadvertent.

5 Policy

The Chief Privacy Officer (CPO) at eHealth Ontario is responsible for leading the design and operation of the Agency's privacy program, including putting processes, practices and tools in place to manage, investigate and remediate privacy incidents or breaches. The Privacy Breach Management (PBM) Team is responsible for handling the end-to-end privacy breach management efforts.

All personnel and third party service providers are responsible for immediately reporting privacy incident and breaches to eHealth Ontario's service desk. Personnel and third party service providers are required to provide a description of the incident or breach, the individuals involved and immediate steps taken, if any, to contain the incident or breach.

eHealth Ontario extends whistleblower protection to personnel and third party service providers who report a privacy incident or breach and to those who refuse to perform a transaction that they believe to be in contravention of eHealth Ontario's roles under PHIPA or FIPPA, relevant agreements or in contravention of eHealth Ontario's privacy policies and procedures.

All personnel and third party service providers are responsible for actively supporting the Privacy Office in privacy incident or breach containment, investigation and remediation activities as needed. Some of these activities may occur concurrently.

5.1 Containment

The containment phase of the privacy incident and breach management process focuses on confirming a privacy incident or breach has transpired, preventing additional information assets from being affected, ensuring affected information assets are not further compromised, minimizing adverse impact to the Agency and restoring normal operation as quickly as possible.

Examples of containment activities may include:

- Suspending the unauthorized practice that resulted in the incident or breach;
- Recovering affected records of PI/PHI;
- Shutting down the system that was breached;
- Revoking access permanently or temporarily to a system; and
- Contacting the police (if the breach involves theft or other criminal activity).

All reported privacy incidents and breaches shall be contained immediately, in accordance with the *Privacy Incident and Breach Management Reference Guide for the Privacy Office*. Immediate containment of privacy incidents will prevent them from becoming breaches and immediate containment of breaches will prevent further unauthorized collection, use and/or disclosure of PI/PHI.

If a privacy incident or breach is suspected to be intentional, it must be immediately escalated to the CPO.

5.2 Investigation & Remediation

Once a privacy incident or breach has been appropriately contained, it shall be investigated by the PBM Team. Investigation will identify the root cause of the privacy incident or breach as well as the information assets, individual(s)/organization(s), and IT systems and hardware involved in the incident or breach.

Based on the findings of the investigation, the PBM Team determines short-term and long-term remediation strategies which are documented in a Privacy Breach Management Report. The report, including the recommendations emanating from the investigation, shall be approved by the CPO and implemented within the stated timeframe.

5.3 Communication and Notification

The eHealth Ontario Stakeholder Relations and Communications Department identifies mandatory and/or discretionary communications that will be issued to internal eHealth Ontario stakeholders (i.e., Senior Management Committee and the Board of Directors) following a privacy incident or breach. Internal communications may be mandatory or at the discretion of the CPO (or designate) in consultation with the PBM lead. Internal communications are conducted as per the requirements noted in the *Privacy Incident and Breach Communication with Internal Stakeholders* as found in the *Privacy Incident/Breach Management Reference Guide for the Privacy Office*.

eHealth Ontario's obligations for notification of privacy incident or breach to custodians of PI/PHI, individuals to whom the PI/PHI pertains or other external stakeholders are mandated through applicable legislation and/ or eHealth Ontario's agreement with third parties. The requirements for external communication/notifications are noted in the *Privacy Incident and Breach Communication with External Stakeholder*s.

5.4 Logging and Document Retention

The Privacy Office shall maintain a log of privacy incidents and breaches, and the recommendations emanating from investigations of these incidents and breaches. The log will be used to provide regular reports to eHealth Ontario senior management on the number and nature of privacy incidents or breaches.

All documentation related to identification, containment, investigation & remediation, communication and notification of privacy incident or breach shall be securely retained by the Privacy Office in accordance with the applicable PBM documentation.

6 Responsibilities

The CPO is is considered the ultimate authority for interpreting, implementing, enforcing and maintaining this Policy. Where a privacy incident or breach is intentional or the result of negligent work practices, disciplinary action will be taken up to and including termination of employment.

The CPO is responsible for monitoring compliance with this Policy.

eHealth Ontario personnel and third party service providers must comply with this procedure.

7 Glossary

The following terminology and acronyms are associated with this Policy:

TERM	DEFINITION
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)
***Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F. 31 (FIPPA)**	A provincial privacy statute that provides a right to access information under the control of institutions in accordance with the principles that information should be available to the public; necessary exemptions from the right of access should be limited and specific; and decisions on the disclosure of government information should be reviewed independently of government. FIPPA also protects the privacy of personal information of individuals held by institutions. It provides individuals with a right of access to, and correction of, that information.
Health Information Custodian (HIC)	Has the same meaning as defined in section 3 of *Personal Health Information Protection Act, 2004* (PHIPA). Examples include: physicians, hospitals, pharmacies, laboratories, community care access centres and the Ministry of Health and Long-Term Care but not eHealth Ontario.
Information and Privacy Commissioner	The 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.
Personal Health Information (PHI)	Has the meaning set out 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.
Personal Health	A provincial health privacy statute that establishes rules for the management of PHI and

***Information Protection Act, 2004*, S.O. 2004, c. 3. (PHIPA)**	protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services.
Personal Information (PI)	Has the meaning set out in section 2 of the *Freedom of Information and Protection of Privacy Act* (FIPPA) as: recorded information about an identifiable individual, including, (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, telephone number, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they relate to another individual, (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, and (h) the individual's name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual.
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 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 result in unauthorized collection, use, disclosure and destruction of PI/PHI or constitute non-compliance with applicable privacy law. A privacy incident may also be a suspected privacy breach.

Table 1: Privacy Breach Management Policy: Glossary

8 References and Associated Documents

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

REFERENCE	LOCATION
Freedom of Information and Protection of Privacy Act (FIPPA) and regulations	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
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	www.ehealthontario.on.ca/privacy
eHealth Ontario Personal Information Privacy Policy	www.ehealthontario.on.ca/privacy
eHealth Ontario Personal Health Information Privacy Policy	www.ehealthontario.on.ca/privacy
eHealth Ontario's Privacy Incident/Breach Management Reference Guide for the Privacy Office	Internal Privacy Office SharePoint
eHealth Ontario Electronic Health Record Privacy Policies	http://www.ehealthontario.on.ca/en/initiatives/resources
Privacy and Security Breach Management Protocols for MOHLTC datasets used in Electronic Health Records – eHealth Ontario & The MOHLTC	Internal Privacy Office SharePoint

Table 2: Privacy Breach Management Policy: References and Associated Documents

9 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.