Halton Healthcare GEORGETOWN · MILTON · OAKVILLE	**Privacy Breach Management Policy**			
	Program/Dept:	Privacy Office	Document Category:	Privacy
	Developed by:	Privacy Office	Original Approval Date:	October 2014
	Approved by:	Senior Leadership Team	Reviewed Date:	August 2022
	Review Frequency:	Annually	Revised Date:	August 2022

Purpose

Halton Healthcare is responsible for the protection of the *privacy* of all personal health information (*PHI*) in its custody. This Policy identifies the steps to follow in the case of an actual or suspected *privacy breach*.

Any term that appears in italicized font in this Policy is a defined term and its definition is provided under "Definitions" at the end of this Policy.

Scope – who does this policy apply to?

This Policy applies to all employees, *credentialed staff*, volunteers, students (collectively "*workforce members*"), and any other *agents* acting on behalf of Halton Healthcare who may become aware of an actual or suspected *privacy breach.*

Policy

If you become aware of an actual or suspected *privacy breach*, you must report it through the Incident Reporting System (IRS). Appendix A provides information on how to report a *privacy breach* through the IRS.

Once the Privacy Office receives a report from the IRS, the Privacy Office will work with the individual reporting *the privacy breach* and, as appropriate, program leadership to investigate the *privacy breach* in accordance with the procedures as outlined below.

The Privacy Office will maintain the confidentiality of any *workforce member* that raises a privacy concern related to Halton Healthcare's privacy practices.

Procedure

IDENTIFICATION OF INCIDENTS RELATING TO A PRIVACY BREACH

All *workforce members* and *agents* are responsible for the immediate reporting of suspected or actual *privacy breaches* to the Privacy Office through the IRS. This includes complaints or incidents involving the unauthorized disclosure of *PHI*, including possible compromise of security systems containing *PHI*.

Once a report of an actual or suspected *privacy breach* is received, the Privacy Office will:

1. Begin its investigation into the reported *privacy breach.* This will include:
   (a). working with the individual who reported the *privacy breach*,
   (b). working with program leadership as appropriate,
   (c). determining if there is a need to obtain legal advice (in consultation with the General Counsel), inform the police, inform Healthcare Insurance Reciprocal of Canada (HIROC), and/or external experts. If there is a potential legal risk, the Privacy Office together with the General Counsel will decide if the investigation should take place within the context of solicitor - client privilege.
2. Notify other staff and/or health information custodians (*HIC*) if the *PHI* at risk relates to them.
3. Address the priorities around the scope of the *privacy breach*, containment, documentation, notification and reporting using the guidelines set out below.
4. Provide any recommendations for process improvement and additional training to program leadership.
5. Escalate to appropriate member of Senior Leadership Team (SLT), CEO or Board of Directors as necessary.
6. Determine if there are obligations to report to the Information and Privacy Commissioner of Ontario (IPC) and any applicable regulatory colleges.

A. <u>IDENTIFY SCOPE OF PRIVACY BREACH AND CONTAINMENT</u>

The following steps will be taken to investigate an actual or suspected *privacy breach*:

1. The Privacy Office, in collaboration with the *workforce member*(s) or *agent*(s) that reported the *privacy breach*, will determine the scope of the *privacy breach,* including by identifying the:
   a. Individuals or organizations who may have been involved with or are responsible for the *privacy breach*;
   b. Number of patients whose *PHI* may have been disclosed without authority; and
   c. Nature of *PHI* (i.e. data elements involved, sensitivity of information and possible *uses*).
2. Halton Healthcare will take steps to contain or support the containment of any reported *privacy breach* to prevent further unauthorized access, collection, use or disclosure of *PHI*. Containment steps may include:
   - Retrieving copies of *PHI* that have been disclosed and/or securing electronic copies
   - Requesting that no copies of *PHI* be made or further distributed by anyone who received the information in error

- Determining whether the *privacy breach* would allow unauthorized access to any other *PHI*
- Taking reasonable steps to remove access (i.e. changing passwords and/or identification numbers and/or temporarily shutting down a system)
- Determining if it is necessary to suspend the activity that caused the *privacy breach*

3. If a *privacy breach* is discovered involving another *HIC*'s information, the Privacy Office will work with such other *HIC* to assist that *HIC* to meet its obligations under *PHIPA*.

B. REMEDIATION

1. The Privacy Office will examine the related information handling practices, procedures and security processes to determine whether there are systemic issues that require remediation.
2. The Privacy Office will provide any recommendations for process improvements for consideration and implementation by the appropriate program leadership and/or SLT.
3. The Privacy Office will engage Human Resources, Medical Staff Office, the Director of Professional Practice or Manager of Volunteer Services with respect to *privacy breaches* involving actions of employees, *credentialed staff* or medical learners, other clinical students or volunteers, respectively, to determine the appropriate course of action, including discipline and reflective learning.
4. The Privacy Office will document its findings and recommendations within the IRS. It is the responsibility of program leadership to close the IRS file.

C. NOTIFICATION OF AFFECTED INDIVIDUALS

The Privacy Office will notify individuals affected by the *privacy breach* at the first reasonable opportunity, following investigation and containment of the *privacy breach.*

Generally, the Privacy Office will contact the individual directly, however there may be circumstances where indirect notification is appropriate (i.e. affected individual is a minor).

Notification to affected individuals will include the following information:

- Where appropriate, the name of the *agent* responsible
- The date of the *privacy breach*
- A description of the nature and scope of the *privacy breach*
- A description of the *PHI* that was subject to the *privacy breach*
- The measures implemented to contain the *privacy breach*
- The Privacy Office contact information
- Statement informing the individual of their right to submit a complaint to the IPC
- If applicable, that the IPC has been notified of the *privacy breach*
- If financial information or information from government-issued documents are involved, information regarding who to call for support

MANDATORY REPORTING

Halton Healthcare has an obligation under certain circumstances to report to the IPC or a regulatory college. The Privacy Office will determine if a report is necessary following the completion of its investigation.

Roles/Responsibilities

Workforce Members:

- To report *privacy breaches* and cooperate with the Privacy Office throughout the breach management process
- If approached by a third party regarding a *privacy breach* at Halton Healthcare, the workforce member can report the *privacy breach* on the third party's behalf or direct the third party to contact the Privacy Office at privacy@haltonhealthcare.com
- Participate in reflective learning following a *privacy breach*, if recommended by the Privacy Office and/or Human Resources

Privacy Office:

- Investigate reported *privacy breaches*
- Document its findings, recommendations and other steps taken (e.g. reporting to regulatory colleges, IPC, notification of affected individuals).
- Keep records related to investigation, notification and reporting, if any
- Report to SLT, CEO or Board of Directors as appropriate

Human Resources:

- Collaborate with the Privacy Office in its investigation and address issues requiring any disciplinary action

Program Leadership:

- Cooperate with the Privacy Office to investigate and address concerns arising from *privacy breach* investigations
- Complete and close IRS file.

Medical Staff Office:

- Cooperate with Privacy Office to investigate and address *privacy breach* concerns related to *credentialed staff* and medical learners

Manager Volunteers Services:

- Cooperate with Privacy Office and address *privacy breach* concerns related to volunteers

Director Professional Practice

- Cooperate with Privacy Office and address concerns related to clinical students other than medical learners

Definitions

Agent: any individual or organization that is authorized by a health information custodian to provide services on behalf of the health information custodian.

Credentialed Staff: Physicians, dentists, midwives or extended class nursing staff who are appointed by the Halton Healthcare Board of Directors and who are granted specific privileges to practice medicine,

dentistry, midwifery or extended class nursing, respectively, in one or more Halton Healthcare hospital sites.

Health Information Custodian (HIC): a listed person or organization under *PHIPA* (e.g. hospitals) who has custody or control of *PHI* as a result of the work they do.

Personal Health Information (PHI): Identifying information about an individual relating to their medical history, provision of healthcare at Halton Healthcare, plan of service, payment eligibility, health care number or the individual's *SDM*.

Personal Health Information Protection Act, 2004 (PHIPA): the provincial privacy legislation that governs the *collection, use* and *disclosure* of *PHI* in healthcare systems. *PHIPA* also governs the individuals and organizations that receive *PHI* from healthcare systems.

Privacy: an individual's right to control the *collection, use* and *disclosure* of their *PHI* and/or personal information.

Privacy Breach: when *PHI* is *collected, used* or *disclosed* without authorization. This can include theft, loss or unauthorized copying, modification or disposal.

Workforce Member: All Halton Healthcare employees, credentialed staff, students and volunteers

Related Documents
Use of Technology Policy
Privacy Policy

Key Words
PHIPA, IPC, Mandatory Reporting, Investigation, Breach, Privacy

Reviewed by/Consultation with

Director Clinical Information Services
Director, Human Resources
Director, Information and Communications Technology
Director Medical Staff Office
Director Processional Practice
Director Quality and Risk

References

Information and Privacy Commissioner of Ontario. (2021). *Responding to a Health Privacy Breach: Guidelines for the Health Sector*. https://www.ipc.on.ca/wp-content/uploads/2018/10/health-privacy-breach-guidelines.pdf

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A

Signed by

_____

Title

_____

Appendix A: Privacy Breach Reporting Process

1. Access the Incident Reporting System (IRS)
    a. Can be found on your desktop or through Connections
2. Sign in using your Halton Healthcare login credentials
3. Select the "Information Integrity" icon from the home page
4. Select "Breach of Privacy" as the "Specific Incident Type" from the drop down menu
    a. Fill in all of the required fields
5. Once complete, submit the form and respond to any emails/communication from the Privacy Office

Source:
https://connections.haltonhealthcare.on.ca/departments/privacy-freedom-information/SiteAssets/SitePages/Home/Submitting%20an%20IRS%20for%20Privacy%20Breaches.pdf