



PROGRAM POLICY

NUMBER: ADM 140

TITLE: Handling a Privacy Breach

CATEGORY: Administrative

APPROVED: September 2013

VERSION: 2.2

AUTHORITY: Program Director

LAST REVIEWED: July 2025

LAST REVISED: July 7, 2025

1. Policy Statement

The RPPEO is committed to protecting the privacy and confidentiality of personal health information (PHI) under its custody or control. In the event of a suspected or confirmed privacy breach, the RPPEO will take immediate and coordinated action in accordance with The Ottawa Hospital's (TOH) Patient Privacy Policy, relevant legislation, and guidance from oversight bodies.

2. Purpose

This policy outlines the steps RPPEO staff must take in the event of a privacy breach, whether suspected or confirmed. It ensures alignment with the *Personal Health Information Protection Act* (PHIPA) and TOH policy, and supports appropriate reporting, mitigation, and documentation.

3. Scope

This policy applies to all RPPEO staff and paramedics certified by RPPEO who collect, use, disclose, or access personal health information as part of their role.

4. Definition

A **privacy breach** is defined as any unauthorized collection, use, or disclosure of personal health information (PHI), whether intentional or unintentional. This includes failure to safeguard PHI or the loss of records containing PHI. The term "privacy breach" in this policy includes both suspected and confirmed breaches.

5. Policy Framework

5.1 Privacy Breach Reporting



- RPPEO will report all suspected or confirmed privacy breaches to The Ottawa Hospital's Information and Privacy Office (IPO) without delay.
- RPPEO will fully cooperate with investigations conducted by:
 - The Ottawa Hospital (TOH)
 - The Information and Privacy Commissioner of Ontario (IPC)
 - The Ministry of Health (MOH)

5.2 Implementation of Recommendations

- RPPEO will make every reasonable effort to implement any recommendations received from TOH, the IPC, or MOH regarding privacy safeguards or breach response.

6. Procedure

1. Immediate Reporting

Any staff member who suspects or confirms a privacy breach must report it immediately to their direct supervisor. If unavailable, the report should be made to any RPPEO management team member.

2. Escalation and Preliminary Assessment

Managerial staff who receive a report must collect initial details about the breach and contact TOH's Information and Privacy Office (IPO) without delay, as per TOH Patient Privacy Policy 00175.

3. Mitigation Guidance

Management will consult the IPO on immediate steps to mitigate any impact of the breach.

4. Implementation of Mitigation

RPPEO will implement any recommended mitigation actions promptly.

5. Notification to MOH

The Program Director will notify the MOH Emergency Health Services Branch about the privacy breach and its status.

6. Investigation and External Reporting

In the case of a confirmed breach, the IPO will lead the investigation and coordinate any required notifications to the IPC or regulatory colleges.

7. Follow-Up with MOH

The Program Director will provide a written update to EHS, including the outcome of the investigation, any recommendations, and their implementation status.

7. Related Policies and Legislation

- *Patient Privacy*, Ottawa Hospital Policy 00175
- *Personal Health Information Protection Act*, S.O. 2004, c. 3, Sched. A



Summary of Updates

REVISION RECORD:

Version number	Revision Date	Summary of Changes
1.0	June 2016	The contact information has changed since last policy revision. In order to avoid giving the wrong information in the future, the phone number was removed and the onus placed on the reporting manager to find current extension in the Corporate directory.
2.0	February 2016	Added numbered process steps.
2.1	July 2025	<ul style="list-style-type: none">• Reformatted policy to align with RPPEO standard layout• Applied consistent language and headings• No substantive changes to policy content• Removed internal classification no longer supported by TOH