OntarioMD

Privacy Breach Management Policy

Version: 0.3

Table of Contents

Document Control

Review Frequency:	Biennially or at greater frequency at the discretion of the Chief Privacy Officer

Approval History

Approver(s)	Approved Date
Sarah Hutchison, Privacy Officer, OntarioMD	August 29, 2013

Revision History

Version No.	Version Date	Summary of Change
0.1	July 20, 2012	First Draft
0.2	June 3, 2013	Gosia Kacprzak consistency review
0.3	June 17, 2013	Kathy Tudor – general edits and corporate communications

1. Purpose

This policy describes the manner in which OntarioMD will identify, contain, investigate, notify, report and remediate privacy breaches as defined in this policy.

2. Scope

This policy applies to all OntarioMD permanent employees and temporary staff (collectively, "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 OntarioMD's agreements with third party service providers, as required. This policy applies to OntarioMD's services which may impact the privacy of Personal Information (PI) and Personal Health Information (PHI) in OntarioMD's care.

3. Definitions

A privacy breach or incident includes the collection, use or disclosure of PI or PHI that is not in compliance with applicable privacy law, or circumstances where PI or PHI is stolen, lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.

Under Ontario Reg. 329/04, s. 6 (2), a HINP is defined as, "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians."

4. Legislative Requirements

In some capacities, OntarioMD may be acting as a Health Information Network Provider (HINP) as regulated by section 6 of Ontario Reg. 329/04 made under the *Personal Health Information Protection Act* (PHIPA). Section 6 of Ontario Reg. 329/04 made under PHIPA requires OntarioMD to notify every applicable Health Information Custodian (HIC) at the first reasonable opportunity if, in the course of providing services to enable a HIC to use electronic means to collect, use, disclose, retain or dispose of personal health information (PHI), the PHI has been stolen, lost or accessed by unauthorized persons.

5. Policy

The Privacy Officer at OntarioMD is responsible for putting processes, practices and tools in place to manage, investigate and remediate privacy breaches, complaints and inquiries.

6. Identifying Incidents

All OntarioMD personnel and third party service providers are responsible for immediately reporting suspected or real privacy breaches to the Privacy Officer by completing and submitting the OntarioMD Privacy Breach/Incident Report, found in section 8 of this policy. Personnel and third party service providers are required to provide a description of the breach, the individuals involved and immediate steps taken, if any, to contain the breach.

Personal health information should not be submitted with the OntarioMD Privacy Breach/Incident Report.

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

6.1 Containment

OntarioMD will work to immediately contain or support containment all reported privacy breaches to prevent further unauthorized collection, use and/or disclosure of PI or PHI.

6.2 Investigation & Remediation

Once a privacy breach has been effectively contained, it will be investigated and the details of the incident and investigation will be documented. The documentation will include the recommendations emanating from the investigation with timeframes for the recommendations to be implemented.

When acting under the capacity of a HINP, OntarioMD will notify HICs when a breach has occurred. When required, as determined by the Privacy Officer, OntarioMD will notify the Information and Privacy Commissioner of Ontario of the incident, investigation and remediation plan.

6.3 Logging and Document Retention

The Privacy Officer will maintain a log of privacy breaches and the recommendations emanating from investigations of these breaches. The log will be used to provide regular reports to the OntarioMD CEO on the number and nature of privacy breaches.

All documentation related to the identification, containment, investigation of a privacy incident or breach will be securely retained by OntarioMD for 7 years.

7. Responsibilities and Compliance

The Privacy Officer is responsible for implementing and enforcing this policy. Where a privacy breach is intentional or the result of negligent work practices, disciplinary action will be taken, up to and including termination of employment.

This policy will be updated or revised biennially or more frequently, as needed, under the approval of the Privacy Officer. In reviewing and updating this policy, OntarioMD will consult the guidelines produced by the Information and Privacy Commissioner of Ontario.

All OntarioMD personnel and third party service providers must comply with this procedure.

8. Glossary

Term	Definition
Health Information Custodian (HIC)	As defined in section 3 of *Personal Health Information Protection Act, 2004* (PHIPA), "a person or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or work". 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)	As defined in section 6 of the Ontario Reg. 329/04, s. 6(2), "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians."
Information and Privacy Commissioner (IPC)	The IPC is an independent oversight body responsible for educating the public concerning their rights under privacy legislation and reviewing the decisions, policies and practices of government organizations and HICs to ensure that organizations fulfill their obligations under the legislation.
Personal Health Information (PHI)	As defined in section 4 of the *Personal Health Information Protection Act, 2004* (PHIPA), PHI generally means information about an individual in oral or recorded form pertaining to that person's health or health services provided to the individual that could identify the individual.
Personal Information (PI)	As defined in section 2 of the *Freedom of Information and Protection of Privacy Act* (FIPPA), "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."

Term	Definition
Personnel	OntarioMD employees and temporary staff (contractors, temporary agency staff, co-op students and individuals seconded from other health care organizations).
Privacy Breach/Incident	A privacy breach or incident includes the collection, use or disclosure of PI or PHI that is not in compliance with applicable privacy law, or circumstances where PI or PHI is stolen, lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.
Third Party Service Providers	Entities that OntarioMD engages to support the delivery of its operations and services. They may provide either goods or services.

9. OntarioMD Privacy Breach/Incident Report

OntarioMD Privacy Breach/Incident Report	
Reporting Privacy Breaches to the Privacy Officer All personnel and third party service providers are required to inform OntarioMD's Privacy Officer of real or suspected privacy breaches or incidents to initiate appropriate action. The Privacy Officer will notify the appropriate HIC(s) of a suspected privacy breach, as appropriate, at the first reasonable opportunity. **A Privacy Breach/Incident can be reported by filling out the form below and contacting OntarioMD's Privacy Officer:** By email: privacy.officer@ontarioMD.com By phone: 416-340-2889	
Severity Level*:	<Privacy Breach/Incident>
To:	
From:	< Privacy Officer>
Report Date:	
Incident Date & Duration:	
Incident Description:	
Type or description of Personal Information or Personal Health Information involved (do not submit PI or PHI):	
Impacted Services / Clients:	
Incident Cause (if known):	
Incident Resolution:	
Other Notes & Comments:	

*Severity Level:

- High – Privacy breach involving multiple patients
- Medium – Privacy breach involving a single patient
- Low – Potential privacy breach