Winnipeg Regional Health Authority
Caring for Health
Office régional de la santé de Winnipeg
À l'écoute de notre santé

Breach Investigation Process for Privacy Officers

Effective Nov. 2022

Known or suspected breaches must be reported to the Privacy Officer (PO) or Manager. Whomever receives the initial report, shall advise the other.

Immediate steps are determined to investigate, report, and determine risk and related mitigation measures. Breach Mitigation Process

If reasonable likelihood of breach is suspected or breach confirmed, PO shall work and collaborate with the Manager

- Gathers (who, what, when where, how, why) data to determine nature and extent of breach
- Identifies staff and individuals involved
- Determines nature and extend of breach (amount and sensitivity of personal health information (PHI))
- Works with Manager and Human Resources (HR) to ensure privacy requirements are met.
- Determine where additional audits might be required.

Willful Breach	Non-Willful Breach
Audit Report received 1st review: PO to complete review – Flag inappropriate or questionable access based on employee's position and department/ program	Gathers data and collaborates with Manager to determine extent of breach, persons affected, risk and relevant mitigation measures.
2nd review: Manager shall review report in its entirety and collaborate with the PO to determine whether use of PHI was required and appropriate to role according to departmental/ program workflows. If initial audit confirms questionable or inappropriate access; manager to notify PO PO may request additional information from Shared Health Privacy Team responsible for conducting audits via Shared Health Audit Request Form **Shared Health Audit Request Form**	

Willful Breach	Non-Willful Breach
PO shall flag questionable activity based on employee's position and department/program and send for manager to review report in its entirety.	
If snooping is identified or reasonably suspected, PO shall notify Human Resources (HR) to ensure the breach investigation process is followed - Employee User Interview Questions for Breach Investigation	- Determines whether notification is required
PO determines whether notification to affected individuals is required ➢ PO determines who needs to be notified with manager's assistance and notifies CPO with a breach notification letter template template ➢ a contact list of persons to be notified, and ➢ a Record of User Activity Audit Report	- Works with Chief Privacy Officer (CPO) / Regional Privacy Officer (RPO)to ensure that notification is conducted in a timely manner as required – either verbally or by letter.
Chief Privacy Officer (CPO) / Regional Privacy Officer (RPO)or PO/designate (as appropriate) alerts site officials (HR, Manager, Program Director) and issues the notification letters	- Collaborate with HR to ensure timely notifications to individuals affected
CPO/RPO advises the Manitoba Ombudsman and other stakeholders as determined/appropriate	- PO/Manager fill out form for notification to the Manitoba Ombudsman and send to CPO/RPO
PO Enters breach into RL6	- PO enters into RL6 or other SDO designated Breach reporting system

Links:
Current PO list
Employee User Interview Questions
Breach mitigation
Guideline for notification of Privacy Breaches
Breach Notification Letter template
Script for telephone notification – can be customized by PO from Breach Notification letter template
Audit toolkit - **User Audit Instruction Guide**