1-A-1 STANDARDS	Approved by: Board of Directors Date: June 27, 2019
1-A-18-1 Privacy Breach Protocol Policy	Applies to: All employees, Volunteers and Board Members
Effective Date: August 23, 2016	Revised: August 2019
Next Review Date: August 2022	

Policy
It is the Policy of Gateway Community Health Centre to review the policies and procedures in place in the event of a privacy incident or breach.

.

Procedure
The Centre will take the necessary steps to ensure personal information in their custody is protected against theft, loss and unauthorized use or disclosure. However, despite our best efforts, a privacy breach may occur. A privacy breach occurs whenever a person has contravened or is about to contravene a provision of the *Personal Health Information Protection Act (PHIPA), 2004,* or its regulations, including section 12(1) of *PHIPA*.

> *A health information custodian shall take steps that are reasonable in the circumstances to ensure personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.*

Section 12(1) of the *PHIPA* requires health information custodians (HICs) to take steps that are reasonable in the circumstances to ensure personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

If a breach is suspected, the Privacy Officer, will activate the Privacy Breach Protocol, to mitigate the effects of the breach.

Benefits of the protocol include:
- GCHC can respond quickly and in a coordinated manner;
- Roles and responsibilities of staff are clarified;
- A process for effective investigations will be documented;
- Effective containment of the breach will be aided;
- Remediation efforts will be easier.

The Privacy Breach Protocol consists of four steps:

Step 1: Respond immediately by implementing the privacy breach protocol
- Fill out and submit an Occurrence and Incident Report (A400) and inform the Privacy Officer of the breach.
- Ensure appropriate staff within your organization is immediately notified of the breach

Step 2: Containment - Identify the scope of the potential breach and take steps to contain it

- The Privacy Officer will use the Privacy Breach Decision Tree (R400) to determine appropriate action.
- Identify the scope of the breach (Who Else Do I Notify (Form R402) and Critical Action Timeline (Form R401) and take immediate steps to prevent any further unauthorized use or disclosure of personal health information.
- Ensure that no copies of the personal health information have been made or retained by the individual who was not authorized to receive the information
- Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system) to mitigate further risk.

Step 3: Notification - Identify those individuals whose privacy was breached and notify them of the breach

- *PHIPA* requires GHCHC to notify individuals, at the first reasonable opportunity. For example, notification can be by telephone or in writing, or depending on the circumstances, a notation made in the individual's file to be discussed at his/her next appointment.
- There are numerous factors that may need to be taken into consideration when deciding on the best form of notification (e.g. the sensitivity of the personal health information).
- When notifying individuals affected by the breach, provide details of the extent of the breach and the specifics of the personal health information at issue.
- Advise affected individuals of the steps that have been or will be taken.

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter.
- The objectives of the investigation are to:
  1) Ensure the immediate requirements of containment and notification have been addressed;
  2) Review the circumstances surrounding the breach;
  3) Review the adequacy of existing policies and procedures in protecting personal health information;
  4) Ensure staff are appropriately educated and trained in relation to the breach.

The course of action will be based upon all information received, the surrounding factors, and the client's (or employee's as applicable) best interests. Every effort will be made to determine if the breach of confidentiality qualifies as intentional or unintentional. Any breach of confidentiality may result in disciplinary actions. The Executive Director represents the responsible authority. The Privacy Officer will keep a record of the breach, the follow up actions and any corrective measures that were implemented.

Internal References:

Policy 1-A-9: *Occurrence Reporting and Recording*
Policy 1-A-15: *Lost or Stolen Health Records*
Policy 1-A-18: *Personal Health Information*
Form R400: *Privacy Breach Decision Tree*
Form R401*Critical Action Timeline*
Form R402: *Who Else do I notify?*