



Village Family Health Team Privacy Breach Protocol

Note: We refer throughout to the Village Family Health Team (VFHT) and staff and agents– but this policy applies to all Queen West Family Health Organization (FHO) members and staff equally. The FHO is the health information custodian for purposes of the Personal Health Information Protection Act (PHIPA), and VFHT acts as the FHO’s agent for purposes of PHIPA.

Definition of a privacy breach:

An unauthorized collection, use or disclosure of personal health information. For example, personal health information may be lost (a file is misplaced within the health information custodian and not found despite reasonable efforts, or a USB key is dropped), stolen (laptop computers are a prime example) or inadvertently disclosed through human error (a letter addressed to person A is actually mailed to person B, or a patient list is inadvertently attached and circulated electronically to those who should not receive it).

In the event of a privacy breach the following steps will be initiated by the FHT:

STEP 1: Containment

- Identify the scope of the potential breach and take steps to contain it: retrieve the hard copies of any personal health information that has been disclosed; 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 and obtain the individual’s contact information in the event that follow-up is required; and
- 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 an electronic system).

STEP 2: Notification

Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly:

- Notify the individuals whose privacy was breached, by telephone or in writing (or more rarely and according to the circumstance, upon a next scheduled visit);
- provide details of the extent of the breach and the specifics of the personal health information at issue;
- advise of the steps that have been taken to address the breach, both immediate and long-term;

- provide contact information for someone within your organization who can provide additional information, assistance and answer questions; and
- Advise that the IPC (where that has occurred, this is a decision made on a case by case basis and while not required under PHIPA, is part of the analysis of every privacy breach) has been contacted to ensure that all obligations under the Act are fulfilled and, where appropriate, provide information about how to complain to the IPC.

Additional steps:

- ensure appropriate staff within the FHT are immediately notified of the breach [**Note to draft: these are not the correct people, that is a Freedom of Information Protection of Privacy Act reference**]
- Ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of the Act; and
- Cooperate in any further investigation into the incident undertaken by the IPC, if the IPC is involved.