

## **Welland McMaster Family Health Team**

### **Privacy Breach Protocol<sup>1</sup>**

This policy is part of the Privacy Policy. It applies to all physicians, Welland McMaster Family Health Team and Welland McMaster Family Health Organization staff, students, volunteers and vendors (“**Team Members**”).

#### **Report**

All privacy breaches must be reported immediately to the Privacy Officers (the Executive Director of the Welland McMaster Family Health Team and the Lead Physician from the Family Health Organization). If you have any questions, contact one of the Privacy Officers.

#### **Privacy Breach**

A privacy breach happens whenever a person contravenes or is about to contravene a rule under the *Personal Health Information Protection Act, 2004* (PHIPA) or the Harmonized Privacy Policy or its related privacy policies. The most obvious privacy breaches happen when patient information is lost, stolen or accessed by someone without authorization.

For example:

- A fax with patient information is misdirected
- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package of patient records is not delivered to the correct address
- An unencrypted USB key with patient information is lost
- A patient reads another patient’s health record on a computer while waiting in a clinic room
- A Team Member talks about a patient with a friend
- Health records to be disposed of are recycled and not shredded
- Out of curiosity, a Team Member reviews a neighbour’s health record
- A student or any other Team Member looks at health records of patients of the Family Health Team on a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise
- Health information is given to the media
- A Team Member makes a copy of an ex-spouse’s health record without the permission of the patient

#### **Privacy Breach Protocol**

The following steps will be taken by the Privacy Officers (or delegate) if they believe there has been a privacy breach:

---

<sup>1</sup> Based on the Information and Privacy Commissioner/Ontario “What to Do When Faced with a Privacy Breach? Guidelines for the Health Sector”. Available online: <http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf>

**Step 1: Respond immediately by implementing the privacy breach protocol**

- Ensure appropriate staff members within the Welland McMaster Family Health Team and the Family Health Organization are immediately notified of the breach, including the Privacy Officers and the physicians whose patients are potentially affected by the privacy breach.
- Address the priorities of containment and notification as set out in the following steps.

**Step 2: 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 personal health information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required.
- 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).
- Consider notifying the Information and Privacy Commissioner/Ontario (IPC/O) and/or legal counsel if appropriate.

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

- At the first reasonable opportunity, any affected patients (or others whose personal health information has been affected) will be notified.
- The type of notification will be determined based on the circumstances (such as the sensitivity of the personal health information, the number of people affected, and the potential effect the notification will have on the patient(s)).
  - For example, notification may be by telephone or in writing, or depending on the circumstances, a notation made in the patient's file to be discussed at his/her next appointment.
- Provide details of the extent of the breach and the specifics of the personal health information at issue.
- Advise affected patients of the steps that have been or will be taken to address the breach, both immediate and long-term.
- Consider notifying the IPC/O and/or legal counsel if appropriate.

#### **Step 4: Investigation and Remediation**

- Conduct an internal investigation into the matter. The objectives of the investigation will be to:
  - Ensure the immediate requirements of containment and notification have been addressed.
  - Review the circumstances surrounding the breach.
  - Review the adequacy of existing policies and procedures in protecting personal health information.
  - Address the situation on a systemic basis.
  - Identify opportunities to prevent a similar breach from happening in the future.
- Change practices as necessary.
- Ensure Team Members are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future.
- Continue notification obligations to affected individuals as appropriate.
- Consider notifying the IPC/O and/or legal counsel as appropriate.
- Consider any disciplinary consequences with staff or contract issues with independent contractors or vendors that follow from the privacy breach.