Policies, Procedures and Guidelines

Complete Policy Title:
Privacy Breach Protocol

Policy Number (if applicable):

Approved by:
President

Date of Most Recent Approval:

Date of Original Approval(s):
June 16, 2015

Supersedes/Amends Policy dated:

Responsible Executive:
University Privacy Officer

Enquiries:
University Secretariat

DISCLAIMER: *If there is a Discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails*

Purpose

Under the *Freedom of Information and Protection of Privacy Act* (FIPPA) or *Personal Health Information Protection Act* (PHIPA), McMaster University has a responsibility to ensure that the personal information in its custody or control is properly safeguarded from those not entitled to have access.

What is a Privacy Breach?

A privacy breach is an incident involving unauthorised access to personal information (PI) or personal health information (PHI) in the custody or under the control of the University. The information can be either recorded or verbal.

Examples of unauthorised access:

- PI/PHI collected in error;
- PI/PHI used for a purpose not consistent with the original collection (e.g. given to someone else for some purpose other than those originally stated);
- lost or misplaced PI/PHI;
- stolen or lost laptops, data drives or disks containing unencrypted PI/PHI;
- accidental disclosure of PI/PHI to an unauthorised person or group (e.g. e-mailing information to the wrong person, loss of unencrypted devices containing PI/PHI);
- deliberate disclosure of PI/PHI to an unauthorised person or group (for fraudulent or other purposes);
- deliberate access of PI/PHI by an unauthorised person or group (for fraudulent or other purposes);
- PI/PHI is copied, modified or disposed of in an unauthorised manner;
- contravention of the privacy policies, procedures or practices of McMaster University;
- contravention of the privacy policies, procedures or practices or of the privacy provisions of any agreements pertaining to the Provincial Electronic Health Record.

What Should I do if a Privacy Breach Occurs?

Except in the Faculty of Health Sciences, when you discover or suspect a breach of personal information or personal health information has occurred, immediately inform the University Privacy Officer to determine how to proceed.

In the Faculty of Health Sciences, when you discover or suspect that a breach of personal health information has occurred, immediately inform the Chief Operating Officer of the Faculty to determine how to proceed.

Assess and Record

You can help by identifying and recording to the extent possible, the following information:

- How did you discover the incident?
- When did you discover the incident and when did it likely occur?
- Where did you discover the incident?
- What happened?
    - is it likely a one-time or on-going occurrence;
    - who is affected;
    - what is the scope of the breach (internal/external);
    - the number of individuals affected;
    - what type of information is involved (identify all specific data types);
    - what format such as email, laptop, hard copy is involved; and
    - any suspicion of criminal activity.

Next Steps

The Privacy Officer will work together with University officials in the areas affected to:

Contain

- Stop the breach or minimise it as far as possible

Inform

- Contact all relevant units to ensure they are appropriately informed (eg. UTS, Security).

Notify

- Alert the persons whose information has been affected whenever it is possible.

Prevent

- A privacy breach should result in a review of current privacy practices to determine whether changes should be made to reduce the risk of a future occurrence.

Additional information on the handling of a privacy breach is available on the University's Privacy website.