Privacy Breach Procedure

Purpose/Rationale:

Under the *Freedom of Information and Protection of Privacy Act* (FIPPA) or *Personal Health Information Protection Act* (PHIPA), The Humber College Institute of Technology & Advanced Learning (hereafter referred to as "Humber" or "the College"), has a responsibility to ensure that the personal information in its custody or control is properly safeguarded from those not entitled to have access.

This document is available in alternate format on request.

Scope:

This Procedure applies to all full-time, part-time, contract and casual employees of Humber, and the University of Guelph-Humber, all of whom are collectively referred to herein as "employees".

Definitions:

Personal information: is defined in FIPPA and refers to recorded information about an identifiable individual, including but not limited to:

- information relating to the race, nationality or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status of the individual
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
- any identifying number (e.g. student number), symbol or other particular number assigned to the individual
- the home address, or e-mail address, telephone number, fingerprints or blood type of the individual,
- personal opinions of, or about, an individual except where they relate to another individual,
- correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence
- the views or opinions of another individual about the individual, and
- the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual

Personal Health Information (PHI): is confidential recorded information about an identifiable individual related to the individual's health or the provision of treatment services to the individual, subject to PHIPA s. 4(1).

Procedure:

1. What is a Privacy Breach?

A privacy breach is an incident involving unauthorized collection, use or disclosure of an individual's personal information (PI) or personal health information (PHI) in the custody or under the control of the College in contravention of Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA). The information can be either recorded or verbal.

2. Examples of unauthorized collection, use or disclosure:

- 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 information (through hacking or physical theft of lost laptops, data drives or disks containing unencrypted PI/PHI);
- accidental disclosure of PI/PHI to an unauthorized 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 unauthorized person or group (for fraudulent or other purposes);
- deliberate access of PI/PHI by an unauthorized person or group (for fraudulent or other purposes);
- PI/PHI is copied, modified or disposed of in an unauthorized manner;

3. What Should I do if a Privacy Breach Occurs?

When you discover or suspect a breach of personal information or personal health information has occurred, immediately inform your supervisor or the department head and the College's Chief Privacy Officer (currently, the Chief Legal, Risk and Privacy Officer) to determine how to proceed at access.privacy@humber.ca or 416-675-6622 x 5509. With the assistance of the department involved, the Chief Privacy Officer will take the lead in investigating the incident.

4. 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?
- What was the location of the incident?
- What happened?
    - what is the cause of the incident?
    - is it likely a one-time or on-going occurrence?;
    - who is affected?;
    - what is the scope of the breach (internal/external)?;
    - how many individuals are affected?;
    - what type of information is involved (identify all specific data types)?;
    - what is the sensitivity of the information?;
    - what format was the information in (such as email, laptop, hard copy is involved; and any suspicion of criminal activity)?;
    - can the information be used for fraudulent purposes?.

5. Next Steps

5.2 Step 1 – Contain

a) Stop the breach or minimize it as far as possible.

5.3 Step 2 – Inform

b) Contact all relevant units to ensure they are appropriately informed (eg. Public Safety, ITS).

5.4 Step 3 – Notify

c) Upon approval of the Chief Privacy Officer, proceed with alerting the persons whose information has been affected if possible and appropriate.

5.5 Step 4 – Prevent

d) Review current privacy practices to determine whether changes should be made to reduce the risk of a future occurrence.

References:

Freedom of Information and Protection of Privacy Act (Ontario)

Personal Health Information Protection Act (Ontario)