Reporting Privacy Breaches: Guideline for University Units

Queen’s University provides a broad range of services to a diverse community. From teaching and learning, to health counseling and disability services, rental housing, and employment, the University routinely collects, maintains, and uses personal information about the people it serves. By law, the University is required to ensure the safety and security of that information, and to take appropriate action when a privacy breach occurs. Demonstrating responsible information stewardship is also an important part of maintaining the community’s trust in Queen’s.

What is a privacy breach?
A privacy breach is an unauthorized collection, use or disclosure of someone’s personal information (PI) or personal health information (PHI), in contravention of either the Freedom of Information and Protection of Privacy Act (FIPPA) or Personal Health Information Protection Act (PHIPA) which:

- May affect an individual or a group
- May be discovered in the course of conducting University business
- May be reported by someone within the University community, or by someone external to the University, including Ontario’s Information and Privacy Commissioner who may have received a complaint

What is personal information?
FIPPA defines personal information (PI) as recorded information about an identifiable individual, including:

- Ethnic origin, race, religion, age, sex, sexual orientation, marital status, etc.
- Information regarding educational, financial, employment, medical, psychiatric, psychological or criminal history
- Identifying numbers: e.g., S.I.N., student number
- Home address, telephone number
- Other people’s personal opinions of, or about, the individual
- Correspondence sent to Queen’s by the individual that is of a private or confidential nature
- The individual’s name where it appears with or reveals other personal information

What makes Personal Health Information different?
While information about an individual’s medical, psychiatric, or psychological history may fall under FIPPA, when that information is collected, used, or disclosed by a Health Information Custodian it is classified as Personal Health Information (PHI) and subject to a special set of legal obligations under PHIPA.

- PHI carries increased legal obligations under PHIPA
- When PHI is collected or used in an unauthorized way, or disclosed to an unauthorized person, it must be reported as a privacy breach to the individual whose information was affected
- Unlike FIPPA, privacy breach reporting under PHIPA is mandatory
Who is a Health Information Custodian?

- A healthcare practitioner or a person who operates a group practice of health care practitioners
- A person who operates a hospital, psychiatric facility, an independent healthcare facility, or a pharmacy
- A person who operates a centre, program or service for community health or mental health whose primary purpose is the provision of health care

Examples of unauthorized collection, use or disclosure:

- Information collected in error
- Information used for a purpose not consistent with the original collection
- Lost or misplaced information
- Stolen information (laptops, data drives or discs)
- Accidental disclosure of PI or PHI to an unauthorized person or group
- Deliberate disclosure of PI or PHI to an unauthorized person or group (for fraudulent or other purposes)

If a privacy breach is suspected or confirmed, report it to:

- Your immediate supervisor (or, if unavailable, the next available level of management) and the unit or department head
- The Queen’s Privacy Officer at access.privacy@queensu.ca or (613) 533-6000 ext. 75226. With the assistance of the University unit concerned, the Privacy Office will take the lead in investigating the incident. Use the companion Privacy Breach Report Form to record details
- Follow the four steps outlined on the following pages
Reporting Suspected or Confirmed Privacy Breaches

Important notes

- Contact the Queen’s Privacy Officer at access.privacy@queensu.ca or (613) 533-6000 ext. 75226
- Use the companion Privacy Breach Report Form to record details

Decisions on how to respond to a suspected or confirmed privacy breach should be made on a case by case basis. Take each situation seriously and undertake steps 1, 2, and 3 on the following pages in quick succession.

Preliminary questions

✓ What was the date of the incident?
✓ What was the location of the incident?
✓ When was the incident discovered?
✓ How was the incident discovered?
✓ What happened?

Step 1: Contain

Contain the incident and assess the situation immediately. Contact the Privacy Officer.

Key questions

✓ Have you contained the incident?
  This step includes such actions as: recovering the information, changing access codes, shutting down systems, stopping the unauthorized collection, use, or disclosure.
✓ Have you designated an appropriate individual to lead an initial assessment?
  This should be someone who has appropriate decision-making authority and responsibility within the unit(s) concerned.
✓ At this preliminary stage, have the appropriate internal staff members been made aware of the incident?
✓ Does criminal activity (e.g., theft) appear to be involved?
  If yes, Queen’s Campus Security should be notified: (613) 533-6733.
✓ Have the details of the incident that are known at this stage been recorded?
  This step will aid in later investigation and corrective actions.

Step 2: Assess the Risks

Assess the types of information involved and the sensitivity of the information to determine the appropriate response and notification to affected individuals. Examine the situation fully and work with the Queen’s Privacy Officer to ensure that any necessary details of the breach and any corrective actions are documented for later investigation and review.
Reporting Privacy Breaches

Key questions

Information Involved

✓ Was health information involved?
Information related to an individual's health can be governed by either FIPPA or PHIPA. If the information was in the custody or control of a Health Information Custodian, it is governed by PHIPA and the breach must be reported.

✓ What data elements were involved?
Determine the specific data elements (e.g., name, date of birth, S.I.N.) that were involved.

✓ What format were the records in?
Indicate the format(s) of the records involved: paper, electronic, on network server, workstation, portable media (e.g., data drive, disc, audio or video cassette tape, microfiche), mobile device (e.g., cell phone, tablet, or laptop), etc. Determine whether the information was encrypted, anonymized or otherwise not easily accessible, and what physical or technical security measures were in place at the time of the breach.

✓ How sensitive is the information involved?
In most cases, the more sensitive the information, the greater the harm to individuals from a privacy breach. Sensitive information includes (but is not limited to): health, financial, student or employment information, especially in combination.

Cause and Extent of the Breach

✓ What is the cause and extent of the breach?
Determine what caused the breach and assess the extent of the unauthorized access to—or collection, use, or disclosure of—the information, include the number and types of possible recipients.

✓ Is there a risk of ongoing breaches or further exposure of the information?
Ongoing or further exposure may include exposure through mass media (online or otherwise).

✓ Can the information be used for fraudulent or other purposes?
Establish whether the information has been lost or stolen, and if so, whether it has been recovered. If criminal activity is involved, notify Queen's Campus Security: (613) 533-6733.

✓ How many individuals were affected by the breach and who are they (e.g., employees, students)?

Foreseeable Harm

✓ Is there foreseeable harm to individuals?
Assess what harm could foreseeably result to individuals from the breach. Examples include: risk to physical security, identity theft, financial loss, and damage to reputation or relationship(s).

✓ Is there foreseeable harm to Queen's?
Evaluate the foreseeable harm that could result to Queen's University from the breach. Examples include: loss of trust in the University, damage to its reputation, financial losses, and legal proceedings.

✓ Is there foreseeable harm to the public?
Consider what public harm could foreseeably result from the breach, such as risk to public health or safety.
Reporting Privacy Breaches

Step 3: Notify the Affected Individuals

Based on the results of the assessment, decide: (i) whether to notify individuals affected by the breach; (ii) when and how they will be notified; and (iii) what information should be included in the notification. Consult the Privacy Officer on the notification before sending.

Key questions

✓ Should affected individuals be notified?
   Consider the risk of harm to the individual (see Foreseeable Harm, above, for relevant factors). If there is any foreseeable harm, notification is required, except in exceptional circumstances (e.g., where notice would interfere with a law enforcement investigation or where there is a foreseeable risk to public health or safety).

✓ Have you decided when and how affected individuals should be notified, and by whom?

✓ Have you established what should be included in the notification?
   Depending on the circumstances, notification could include some or all of the following:
   - Description of the breach
   - Specifics of the information inappropriately accessed, collected, used, or disclosed
   - Steps taken so far to address the breach and any future steps planned to prevent further privacy breaches
   - Additional information, if required, about how individuals can protect themselves (tracking credit cards, monitoring bank accounts, changing ID numbers, etc.)
   - Contact information for an individual (include her/his position title) within the University who can answer questions or provide further information

Tips

- If notifying a number of individuals by telephone, use a script that provides the same information to all recipients. Clearly identify the University and provide contact information for an individual (including her/his title) who can answer questions or provide further information.
- If notifying in writing (letter or e-mail), make the contents clear and concise. The Privacy Officer can assist in drafting the notification, if requested. Use a delivery method that provides a receipt of the letter, such as registered mail or courier. When sending notification by e-mail, ensure that the current e-mail address is known. Request delivery notification and read receipts where possible.

Hand-deliver the completed Privacy Breach Report Form to the Privacy Officer in Mackintosh-Corry Hall, F300, or send by encrypted e-mail to access.privacy@queensu.ca.

NOTE: Limit distribution of the Privacy Breach Report Form to only those individuals who need to be informed about the incident as part of their duties and responsibilities.
Step 4: Investigate and Correct

The Privacy Officer will: (i) further investigate the cause of the privacy breach; (ii) work with the unit(s) concerned to prepare documentation; and (iii) consider whether to develop a prevention plan. The Privacy Officer will also determine whether Ontario’s Information and Privacy Commissioner should be informed of the breach.

A prevention plan may address such issues as:

✓ Staff training
✓ Policy review or development
✓ Audit of physical and/or technical security
✓ Review of relationships with third-party service delivery partners
✓ Audit to ensure that prevention plan has been fully implemented