Privacy Workshop for the SRA

Trudi Wright
Privacy & Records Management Specialist

November 27, 2022

Agenda

1. Compliance Overview
2. Consent in Key;
3. Privacy Best Practices – Collecting, Using and Sharing information;
4. Steps to Protect & Ensure Confidentiality;
5. Role of the University Privacy Office

Why Do We Care About Privacy?

The University and its employees must comply with privacy legislation, which protects staff and students, and ensures that the information about their identity is secure.

Core Privacy Legislation for McMaster:

- Freedom of Information and Protection of Privacy Act (FIPPA) - Ontario;
- Personal Health Information Protection Act (PHIPA) – Ontario;
- Personal Information Protection and Electronic Documents Act (PIPEDA) – Canada.

Personal Information (PI)

Personal information (or PI) is defined as “recorded information about an identifiable individual.”

How do we determine if the information is about an identifiable individual?

Information is about an identifiable individual if:

- it reveals something of a personal nature about the individual, and
- it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information).

Consent

FIPPA is a **consent-based** legislation. This means that you need either **explicit or implied** consent before you may collect, use or disclose personal information.

Note: Consent in FIPPA refers to collection, use and disclosure of PI and may be withdrawn by an individual.

What is Valid Consent?

Whether it is explicit or implied, **consent must be**:

- **knowledgeable***;
- **voluntary**;
- **related to the information in question, and**;
- **given by the individual**.

*this means that the **individual knows why** the PI is being collected, used and disclosed and that they may provide or withhold consent to share or use it.

Privacy Best Practices: Collecting, Using & Sharing Personal Information

- As a general rule, clear consent is required to support collection, use or sharing personal information.
- Where possible, the collection of personal information should be directly from the individual.
- Collection, use or disclosure should not occur where non-personal information will serve the purpose.

Collecting PI at McMaster University

Collection and use of personal information is outlined in the university's Notice of Collection Statement to support university activities, including:

- Academic, administrative, employment-related, safety and security, financial and statistical purposes of the University
- To support the administration of admissions, registration, awards and scholarships, convocation, alumni relations and other fundamental activities.

Download the McMaster Notice of Collection Statement from the University Secretariat's website.

Questions About Collection and Use

1. Requesting documentation to support exam deferral:
   - Limit collection of personal health information
   - Retain documentation for short-term periods
2. Processing unrequested documentation containing personal or personal health information:
   - If not needed, let individual know where it should be sent (if known)
   - Avoid retaining personal or personal health information
3. Disclosure through escalation – when information shared with you requires disclosure to other offices:
   - Consent is Key! Also ensure that you have consent from the individual to share the information.
   - If consent is not provided, direct the individual to pertinent areas for additional support.

Working from Home: Practices

When working with documents containing personal information, from home:

- Retain and backup documents in secure locations
  - Requiring login, and limiting access
- Limit access to computing devices
- Prepare to share documents, prior to virtual meetings
- if you have been approved to hold confidential information on your **personal device**, the device must be **encrypted**
- Use caution when disclosing personal information via text, chat or email.

Remote Meetings & Consultation

Remote work relies on technology to meet with teams and clients (internal and external).

- Microsoft Teams & Zoom
  - A tool useful for informal meetings and consultation. Functionality allows for chat and sharing documents. Meetings may be recorded – creating a record for the event.
  - Recommendation: Documents should be shared through email, in order to ensure they are retained with related communications and documents. This also enables post-meeting confirmation of details noted during a meeting.
  - Unless the event will be published for public consumption, avoid recording meetings.

Privacy & E-Mail Communication

If sending an email containing personal information to an authorized recipient:

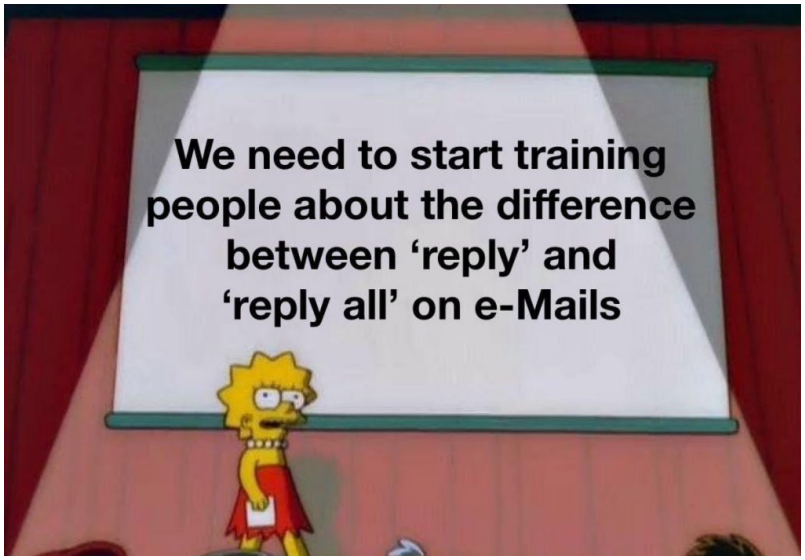
- **@mcmaster.ca** emails are ***not*** automatically encrypted and are ***not suitable*** to disclose personal information
- There are multiple options available to secure personal information, including:
  - Password protecting an attachment
  - Consider attaching a document in PDF format, rather than Word
  - Provide a link to the information accessible from a secure location (requires login or password credential for access)
  - Use confidentiality options in outlook to limit forwarding, downloading and printing emails and attachments

McMaster University

Privacy & E-Mail Communication

If sending an email containing PI to an authorized recipient:

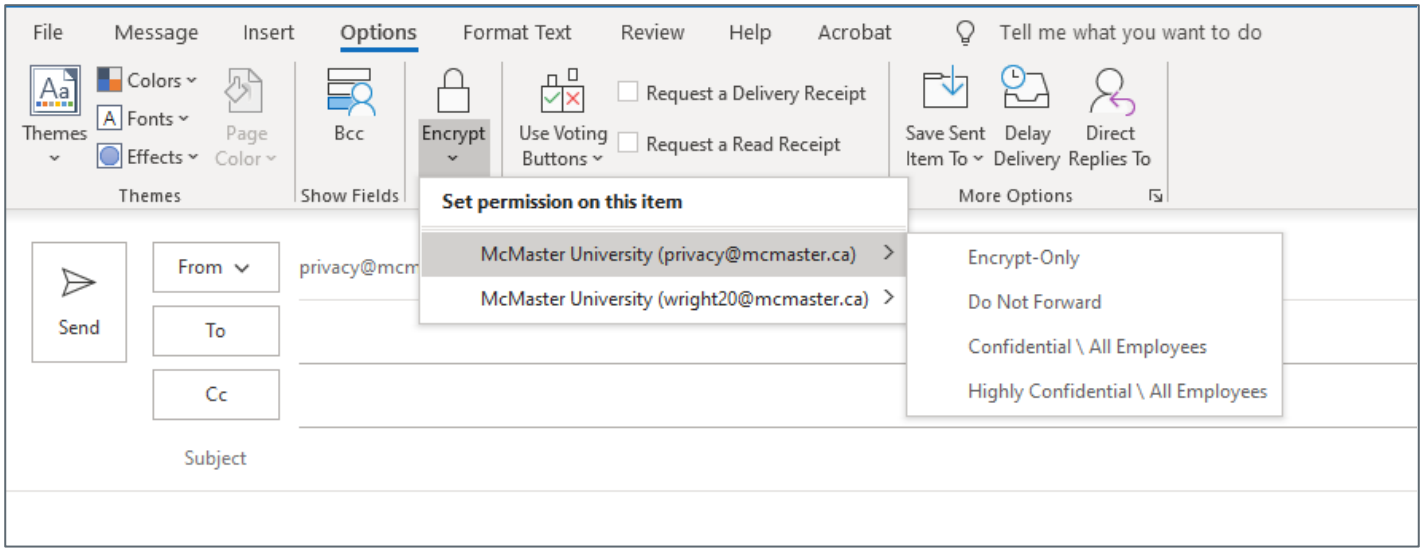
- **confirm** the email address of the recipient to avoid an inadvertent privacy breach
- ***do not*** send PI to a distribution list unless you can verify <u>all</u> recipients meet these rules



McMaster University

Outlook Security Function

In order to secure individual emails, Outlook does have functionality to limit a recipient from performing different activities with an email, including printing, forwarding, and revising the original email text.

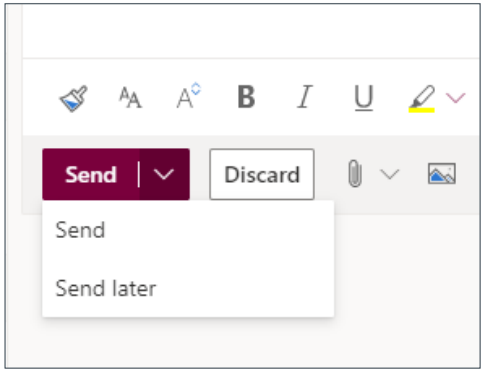


McMaster University

Delay Send Function in Outlook

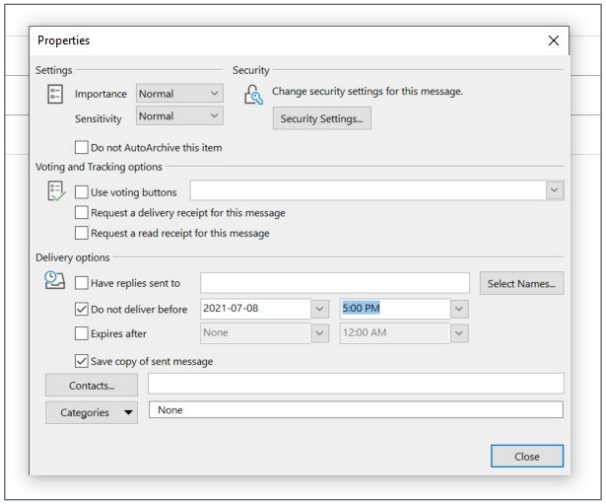
Using Outlook Online:

1. After composing your message, select the dropdown menu next to the **Send** button.
2. Select **Send later**
3. Select the date and time you'd like the email to be delivered and click **Send**.



Using Outlook for Windows:

1. In the message, click the **Options** tab.
2. In the **More Options** group, click **Delay Delivery**.
3. Under Delivery options, check the box for **Do not deliver before**, and select a date and time.
4. After you click **Send**, the message remains in the **Outbox** folder until the delivery time.



McMaster University

Managing Legacy Email Accounts

You may have gained access to a role-based email account, related to your role in the MSU or SRA.

- Review contents in the inbox and folders, and delete old emails that have no informational value. This is especially important for emails containing personal information.
- Clearly identify the purpose for folders, and use them consistently.
- Limit storing personal information in an email account – a better practice is to convert an email to pdf and store in a more secure location (which requires password protection).

Digital Storage of PI

- Documents containing PI should only be accessible to individuals who require access in the conduct of their role.
- Documents containing PI must not be stored on a laptop, computer hard drive or email account.

Approved Storage Locations:

- University approved storage solutions – OneDrive and MacDrive
  - Consider password protection for documents containing PI restrict access
  - Multi-factor Authentication (MFA)
  - Actively track access rights and privileges

McMaster University

Safeguarding Personal Information

Anyone handling PI ***must***:

- ensure that records of PI are **retained**, **transferred,** and **disposed** of securely
- take **reasonable steps** to ensure PI is protected against:
  - theft, loss, and unauthorized use or disclosure
  - unauthorized copying, modification, or disposal
- **notify supervisor** and **privacy office** at the first reasonable opportunity if PI is stolen, lost, used, or disclosed without authority.

University Secretary & Privacy Officer

Andrea Thyret-Kidd has over 25 years of experience as an administrative leader at McMaster University.

As Privacy Officer, Andrea is responsible for ensuring organizational compliance with FIPPA, PHIPA, Canadian Anti-Spam Legislation, and other relevant legislation, as well as providing advice and guidance on privacy compliance.

In the Privacy Office, Andrea is supported by Trudi Wright (Privacy & Records Management Specialist).

Privacy Office Activities

The University Privacy Office is responsible for several activities within the university community, including:

- Process Freedom of Information (FOI) Access to Information requests
- Conduct Privacy Impact Assessments for new systems, processes and activities
- Consult on privacy best practices and compliance
- Lead privacy incident investigations
- Develop training and tools to support privacy best practices

Access to Information Request Processing

The University Privacy Office receives two types of requests for access to information:

- **general records** regarding the operations of the University, faculties, and departments.
- **personal records** regarding the individual who is making the request.

Once a request is received; the Privacy & Records Management Specialist reviews the request to determine whether further clarification is needed to identify responsive records.

The University aims to meet the **30-day timeframe** to provide a decision letter and any responsive records to the requester.

Privacy Impact Assessment

A PIA is a risk management process that helps institutions ensure they meet legislative requirements and identify the impacts their programs and activities will have on individuals' privacy.

Conducting a PIA helps to ensure compliance with:

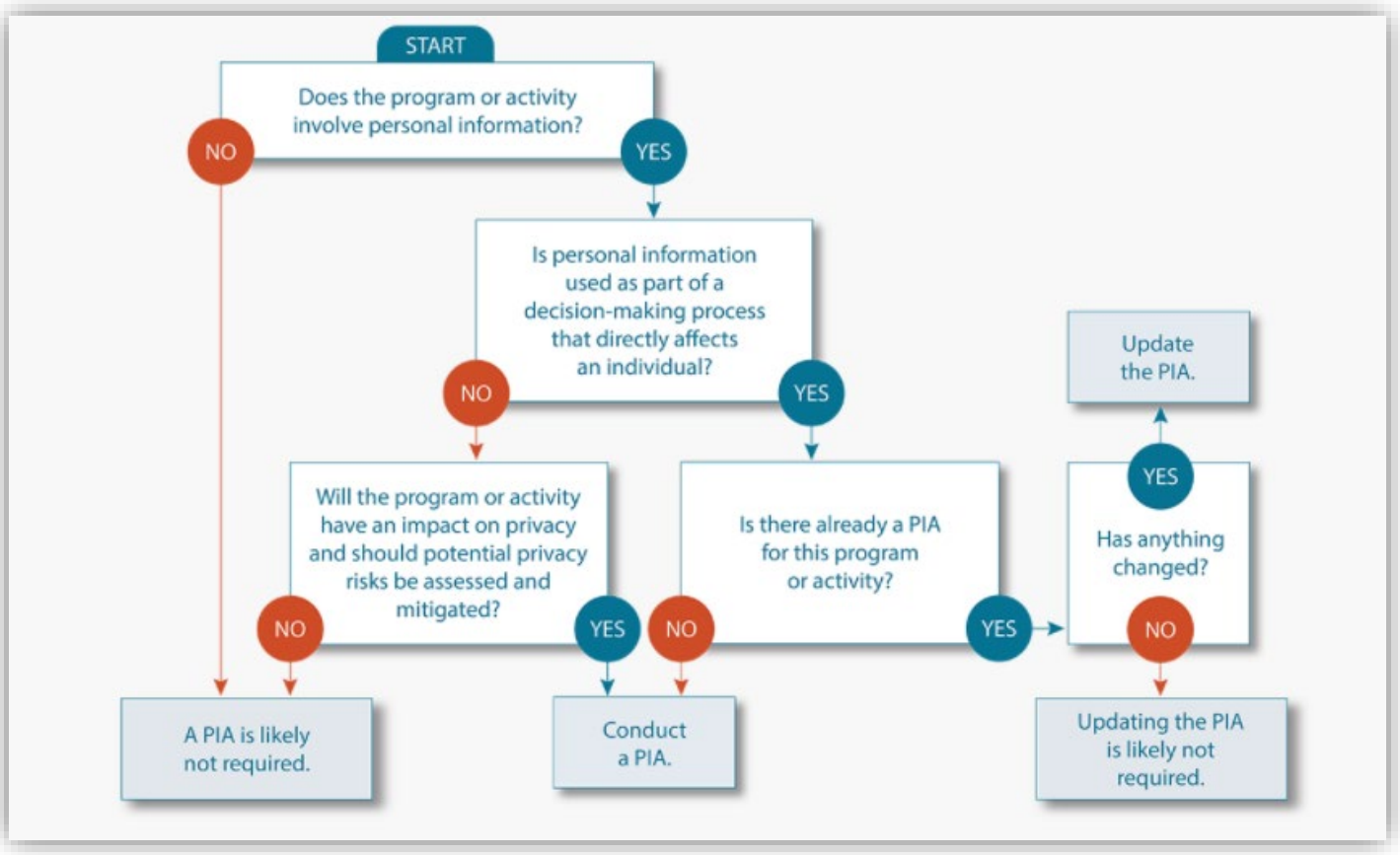
- legal requirements set out in FIPPA and PHIPA
- the institution or program's enabling legislation
- privacy and security best practices

While the university and its activities **must** comply with legal and policy requirements, they should also be designed to incorporate best practices and minimize negative impacts on the privacy of individuals. A PIA may not eliminate such risks altogether, but supports identifying and managing them.

PIAs are an early warning system, allowing the university to identify and mitigate risks as early as possible. They are a key tool for decision-makers, enabling them to deal with issues internally and proactively to safeguard privacy.

An effective PIA helps build trust with stakeholders by demonstrating due diligence and compliance with legal and policy requirements as well as privacy best practices.

When is a PIA needed?



McMaster University

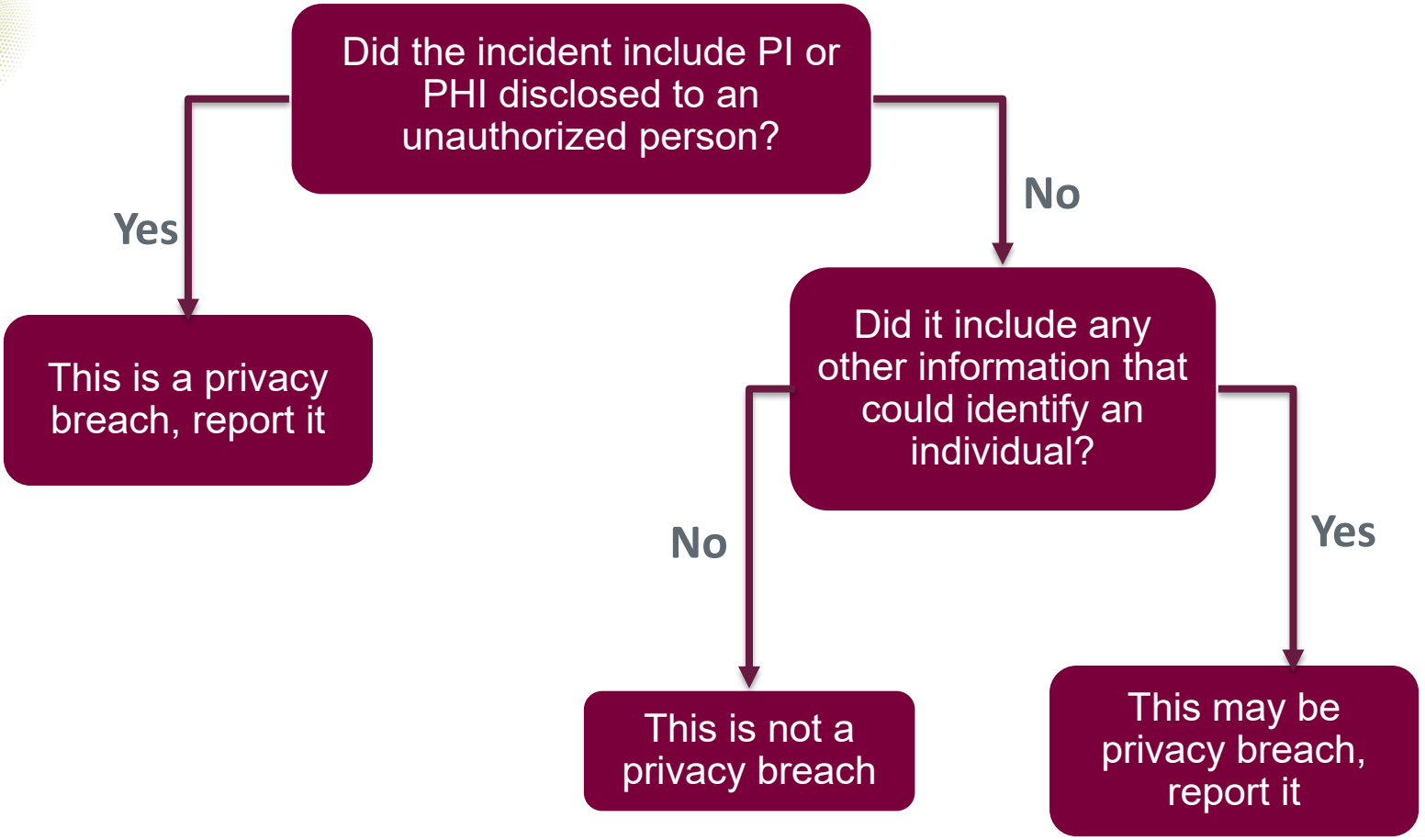
What is a Privacy Breach?

A privacy breach occurs when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws.

Like all public sector organizations, the University is required to have a privacy breach response plan.

McMaster University

Step 1: Confirm the Breach



McMaster University

6 Steps in Managing a Privacy Incident

1. Confirm and Contain
2. Full Assessment
3. Notification
4. Mitigation and Prevention
5. Reporting
6. Lessons Learned

McMaster University

Privacy Consultation

All University departments are governed by relevant legislated provisions affecting personal privacy and access to information, such as:

- Personal Health Information Protection Act (PHIPA)
- Freedom of Information and Access to Privacy Act (FIPPA)
- Health Protection and Promotion Act
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Canadian Anti-Spam Legislation
- Extra-Canadian Compliance (e.g. GDPR, DPA)

The Privacy Office is available for consultation on privacy best practices, and the development of forms and processes where PI (including PHI) is likely to be involved.

Thank you

McMaster Privacy Office

https://secretariat.mcmaster.ca/privacy/

privacy@mcmaster.ca