

PIAs and changes to MFIPPA

Zone 5

November 6, 2026

Agenda

- MFIPPA Changes: Privacy
- Policy and Governance for Compliance
- PIAs: what to know

Key Dates

April 24, 2026 – Royal Assent Achieved

July 1, 2026 – Changes to FOI process went into effect

January 1, 2027 – Privacy changes go into effect:

- **PIAs**
- **Privacy Breach Reporting**



Privacy Changes



This Photo by Unknown Author is licensed under CC BY-SA-NC

MFIPPA changes: Privacy

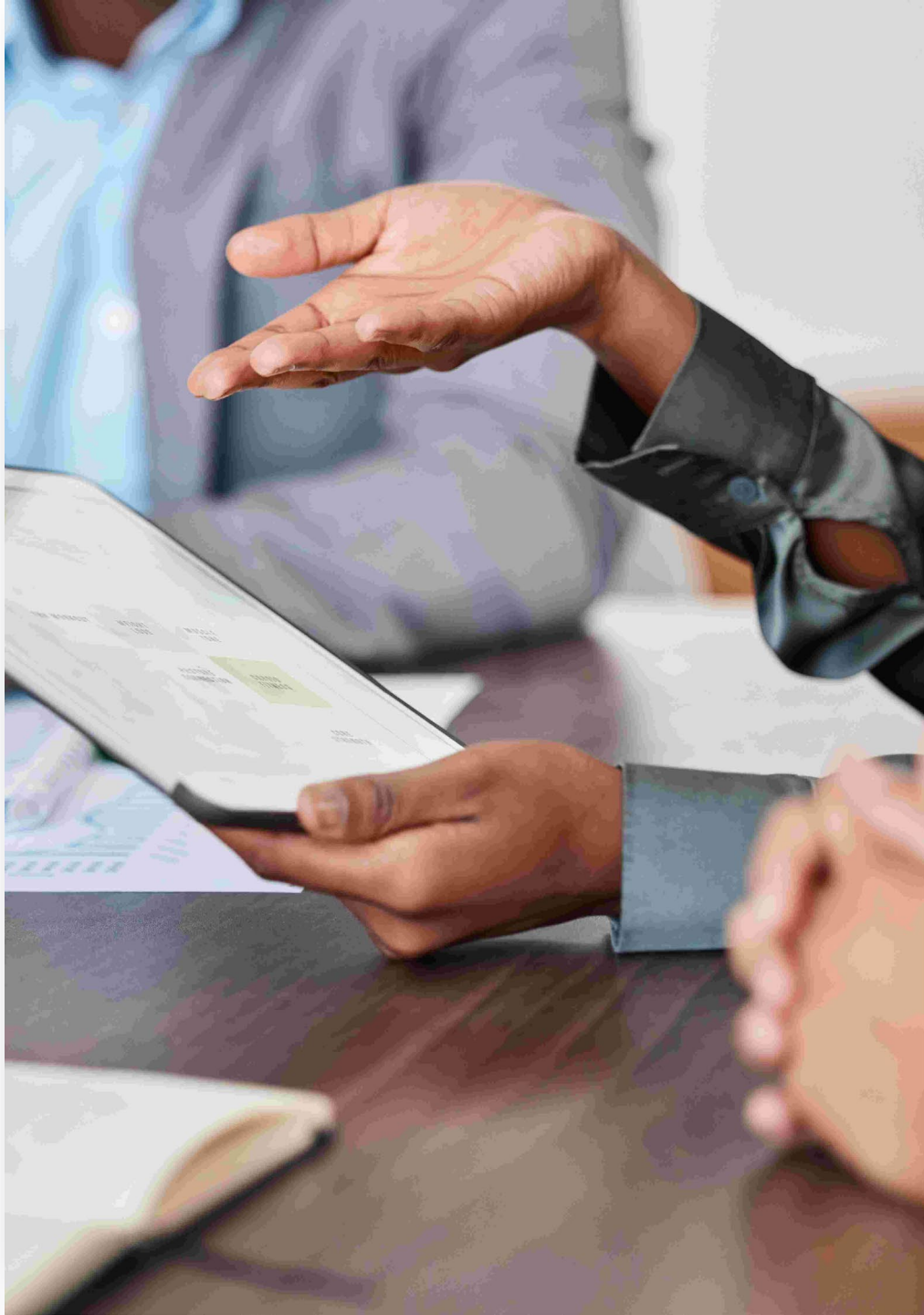
As of **January 1, 2027:**

- **Privacy Impact Assessments (PIAs)** will be mandatory BEFORE the collection of Personal Information (PI) occurs
- PIA content requirements are the same as those captured in Bill 194 (FIPPA) in 2025
- Privacy breaches must be reported to the IPC and the affected individual(s) WHEN THERE IS A REAL RISK OF SIGNIFICANT HARM (RROSH)



Governance for Compliance

- What needs to be in place to ensure that your municipality will be able to ensure compliance with the new privacy requirements?
- Ask yourself:
  - What is the level of privacy literacy in my municipality?



It’s Full Disclosure Time

- What is the level of privacy literacy within your organization?
  - How comfortable are you that a privacy breach would be recognized and reported properly?
  - Do you have a process to report breaches currently in place?
- What is Senior Management’s position on privacy?
  - Are they walking the walk? Or breaching the breach?
- What policies/training specific to privacy are in place?
  - Annual training is best, plus a test!

POLICIES

Think about the difference between a Privacy Policy and the more specific project-based guidance that should fall under it, e.g.:

- CCTV policy (What are the steps I need to take before I set up a camera? HINT: PIA)
- AI policy (any AI project that involves PI should include an AI Impact Assessment AND a PIA, probably a TRA as well)
- Procurement policy (extends to agreements, RFP language, etc.)
- Vendor requirements (standard, sets a bar and makes evaluation/contract management easier)
- Security policy (includes auditing requirements)



SUPPORT

In order to know what's going on (privacy related projects) and properly assess privacy risks, Privacy needs a seat at the table.

Is there currently a committee/group that someone from the Privacy team can attend to understand what new projects are coming down the pike that might involve privacy risk?



What this process might look like

- Privacy Policy states that any new project involving the collection/use/disclosure of PI will have to be vetted by the Privacy team
- IT meets monthly to discuss new technology projects
- Procurement meets weekly to discuss new procurements

Privacy attending these two meetings (for a while, at least) will build internal knowledge about which projects might need a PIA (final say is always Privacy's)

Anything that falls outside of these two meetings should be caught by managers, etc. who have received privacy training that explicitly states their accountability



Which will require a PIA (or at least a consultation)?

- Parks and Recreation wants to update the current CCTV system at all the public facilities
- A consultant has been brought in to work on a plan to increase tourism for your municipality. They will be conducting surveys with residents and using their responses to build a report to Council
- Your IT department would like to introduce an AI tool to provide meeting summary notes
- The Mayor’s office would like to reach out to former donors to gauge their interest in donating to a new project



Raising Privacy’s Profile

How do we do this?

- Training
- Communications
- Pooping of the pants



Talking PIAs

- A PIA is a risk assessment tool for identifying privacy risk
- There is no standard PIA template, but many public organizations in Ontario use the IPC guideline
- Not every project will require a PIA: it is as important to set up privacy governance in your institution, so that projects that involve PI can be put through the PIA funnel
- Often, a preliminary PIA or screen tool can be used to assess whether a PIA is necessary



This Photo by Unknown Author is licensed under CC BY

PIA content requirements

1. Purpose for collecting/using/disclosing PI and why it is necessary
2. Legal authority for C/U/D
3. Types of PI C/U/D and how it will be used/disclosed
4. Sources from which the PI will be collected
5. Position titles of officers, employees, consultants, or agents who have access to the PI
6. Any limitations on C/U/D



PIA content requirements

- Retention period for PI
- Administrative, technical, and physical safeguards that will protect PI, along with a summary of risks to individuals in the event of a theft, loss, or unauthorized use or disclosure
- **Steps the institution will take to prevent or reduce the likelihood of such a theft, loss, or unauthorized use or disclosure, and the steps to mitigate risks to individuals if such an event occurs** (prevention and mitigation steps)
- Any additional information that may be prescribed in regulation



IPC PIA Guide contains all of the requirements on the previous list. Just sayin’

https://www.ipc.on.ca/en/resources/planning-success-privacy-impact-assessment-guide-ontarios-public-institutions



Preliminary assessment

On January 3, 2027, Joe, Director of Human Services, approaches you about a new project that he thinks might require a PIA.

Some initial questions to ask Joe before embarking on the PIA process:

- Does the project involve the collection/use/disclosure of personal information?
- If no, a PIA is not required. If yes:
  - What PI is involved?
  - What is the purpose? Is it authorized under the Municipal Act or other legislation?
  - Provide a data flow map to show who will have access to the PI at what stages and how it will move within/without systems



PIAs

- The previous list are the go/no go questions that will (hopefully) frame the project for you and give you a sense of the scope of PI involved and the associated risk
- A list of data elements is crucial. A project that involved name and email address will have a much lower risk profile than a project that uses employee number, etc.
- Remember that even if the PI involved in the project looks like it might not be high risk, you also need to consider the potential for that PI to be matched with other PI that may be otherwise available (e.g. infection rates in a small community during COVID pandemic)



Preliminary assessment

- Joe has confirmed that the project (an HR management tool) WILL include PI, but insists that a PIA is not necessary, because a Threat and Risk Assessment (TRA) has already been completed for the project by the third-party vendor
- Does this meet the MFIPPA PIA requirement?



A word about vendors…

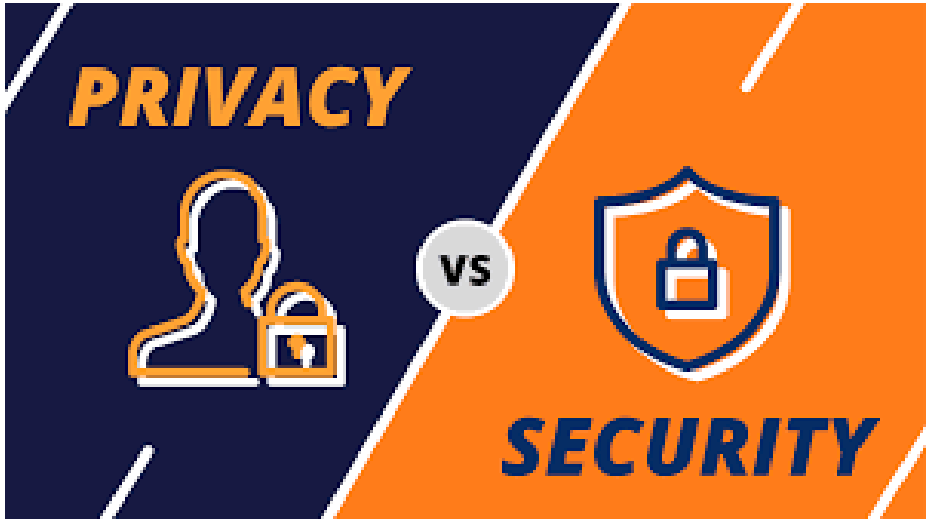
Don’t take them for their word

- Check their profile to see if they have had any major breaches
- Check their website: do they have privacy language there (more than just standard website-cookies info)? Do they have a CPO?
- Ask about their privacy program. Do they train their employees on privacy (not just security)? Do they audit their employees access to PI? Do they conduct PIAs on their own products?



This Photo by Unknown Author is licensed under CC BY-SA-NC

Security is not Privacy



- Security protects the asset (information, the organization)
- Privacy protects the individual
- A TRA (or security assessment) does not consider the risk of harm to the individual or the organization
- A TRA asks questions like: “Is the system safe from hackers?” where a PIA asks: “Are we legally permitted to C/U/D this information?” and “Which employees (your organization and the vendor) are allowed access to it and for what purpose?”

Privacy Breach Reporting



Mandatory Breach Reporting

To the IPC and affected individual(s) IF the there is a real risk of significant harm

Significant harm:

Bodily harm

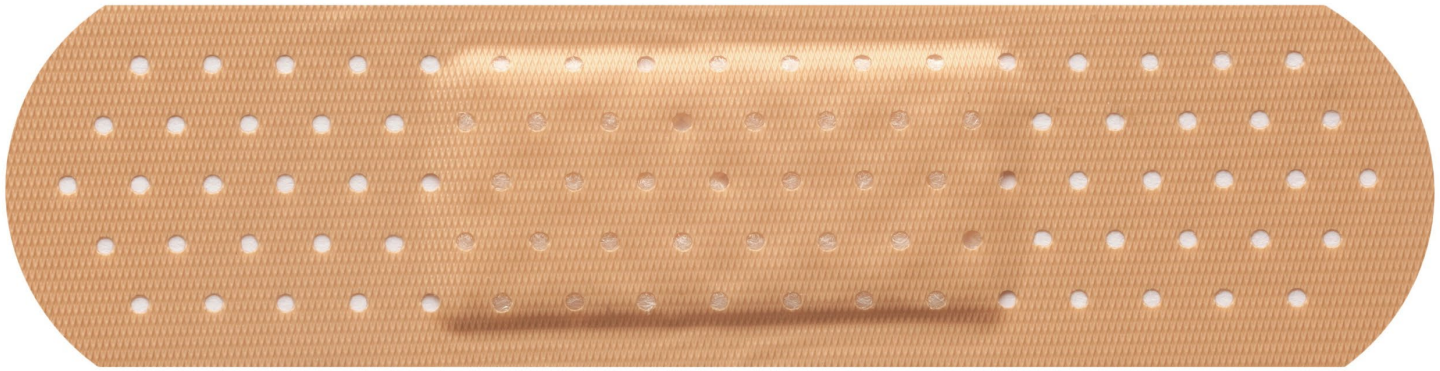
Humiliation

Damage to reputation

Financial loss

Identity theft

Property damage



RROSH

Consider:

- Sensitivity of PI and probability that it will/has been misused
  - E.g. health or financial information vs. name and email address
  - Unique identifier
  - Context: can the information be matched with other, publicly-available information?
- What is the likelihood of harm?
  - E.g. information was left at an internal copier and one person saw it and reported the breach, vs. a Sharepoint security breach that leads to external access to employee PI
- Determine the resulting risk level to the individual/institution

Risk Table

	Negligible Likelihood (L0)	Low Likelihood (L1)	Medium Likelihood (L2)	High Likelihood (L3)
High Potential Harm (H3)	Low 3	Medium 4	High 5	High 6
Medium Potential Harm (H2)	Low 2	Medium 3	Medium 4	High 5
Low Potential Harm (H1)	Negligible 1	Low 2	Medium 3	Medium 4
Negligible Potential Harm (H0)	Negligible 0	Negligible 1	Low 2	Low 3

Moving forward (next steps)



Short term:

- Expedited PIA or screen
- Policy, training materials, communications for PIA:
  - When (in what circumstances) should they be done?
  - Who is responsible for initiating a PIA (hint: it's not you)?
  - PIA process map
  - PIA responsibilities (who does what, who signs off on risk acceptance?)
- Privacy Breach Response Plan
  - Policy, training materials, communications for PBRP
    - Emergency response team (for high profile/high risk breaches) may include:
      - Legal
      - IT
      - HR
      - Communications
    - Who is responsible/accountable?
    - Process map

Moving forward (next steps)

Long term:

- Privacy policy
- PIA SOP/standard
- Privacy governance
  - What seat at what table do you need to be at to ensure that privacy projects are being properly vetted/privacy breaches are being properly managed?
- Enterprise-wide training
- Privacy Breach Response Plan

Further down the road:

- Coordination of PIAs and TRAs
- Auditing protocols



Upcoming Training Opportunities

- PIA workshop (hybrid) November 30 at Toronto Region Conservation Authority
- Additional PIA workshops on demand
- Onboarding/Offboarding Councillors (on request)

Seshat does PIAs!

else.khoury@outlook.com

