Ministry of Public and Business Service Delivery and Procurement

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) Modernization

Privacy Impact Assessments and Preparing for January 1, 2027

Strategy, Artificial Intelligence and Data

November 6, 2026

Ontario

Privacy, Access and Cyber Security Policy Branch

Ontario Ministry of Public and Business Service Delivery and Procurement

Ezra Houser
Senior Manager, Privacy, Access and Policy Unit

Madeleine Hass
Senior Policy Advisor, Privacy, Access and Policy Unit

Privacy and Access Advisory Support:

Support available for:

- MFIPPA implementation
- Privacy breach preparedness
- Access and privacy practices
- Bill 97 readiness

access.privacy@ontario.ca

Thank you for the opportunity to join today's discussion. We look forward to continuing our work with municipalities to strengthen privacy, access and cyber security across Ontario.

What We'll Discuss Today

MFIPPA Modernization and Preparing for January 1, 2027:

- Key legislative changes under Bill 97, the Plan to Protect Ontario Act (Budget Measures), 2026, which received Royal Assent on **April 24, 2026**.
- What we're hearing from municipalities.
- Privacy Impact Assessments (PIAs): what they are and why they matter
- When a PIA should be considered and where to focus limited resources.
- Common implementation questions and considerations.
- OPS PIA Guidance, tools and supports.
- Other important MFIPPA updates, including:
    - Privacy Breach Reporting and access request changes.
- Looking ahead: preparing for implementation

What Changed in 2026?

<table>
<tr><th>Privacy – (in force Jan. 1, 2027)</th><th>Access</th><th>Accountability</th></tr>
<tr><td>Mandatory PIAs
Institutions must complete and maintain a PIA before collecting personal information for prescribed activities, in accordance with the new legislative requirements.</td><td>Access Request Timelines
The time limit for responding to access requests increased from 30 calendar to 45 business days, with updated rules respecting extensions and processing requirements.</td><td rowspan="3">Privacy Management and Documentation
The amendments place greater emphasis on identifying privacy risks, documenting decisions, and demonstrating compliance with legislative requirements.</td></tr>
<tr><td>Privacy Breach Reporting (PBR)
Institutions must report certain privacy breaches to the Information and Privacy Commissioner (IPC) of Ontario and provide notice where required.</td><td rowspan="2">Operational Impacts for Access Offices
Longer response timelines may affect request management, practices, reporting, workload planning, and records retrieval processes.</td></tr>
<tr><td>Real Risk of Significant Harm (RROSH)
Institutions must assess whether a privacy breach creates a RROSH to the affected individual when determining notification and reporting obligations.</td></tr>
</table>

What We're Hearing From Municipalities

Municipal Feedback	What We've Heard
Do we need a PIA for everything?	Municipalities need practical guidance on when a PIA is required and when updates to an existing PIA may be needed, in addition to a clear interpretation of legislative requirements and risk-based implementation guidance.
We are a small municipality with limited privacy resources	Municipalities need scalable tools that can be used regardless of organizational size or privacy maturity.
We share services with other municipalities	Municipalities are seeking guidance on joint procurements, shared systems, and collaborative approaches to PIAs.
How much detail is enough?	Municipalities want guidance on proportionality and the difference between simple and complex assessments.
We need a quicker way to determine whether a PIA is required.	Municipalities are looking for simplified screening tools, decision-making support, and visual approaches to triage projects.
What questions should we ask vendors and service providers?	Municipalities want practical procurement guidance and support evaluating privacy risks associated with third-party solutions

Privacy Impact Assessments: The Biggest Change

What is a PIA?

A Privacy Impact Assessment (PIA) is a tool that drives a process used to identify, assess, and mitigate privacy risks associated with a program, service, initiative, or technology that involves personal information.

When is a PIA Required?

Under MFIPPA a PIA is required before an institution collects personal information. A PIA must also be updated before making a significant change to the purpose for which personal information covered by the PIA is used or disclosed.

Why Are PIAs Important

A PIA provides a structured way to consider MFIPPA requirements and privacy risks in the context of a particular initiative.

Why Were PIAs Added to MFIPPA?

As municipalities increasingly rely on digital services, cloud solutions, data sharing arrangements, and emerging technologies, PIAs help ensure privacy considerations are addressed early and consistently.

Beginning January 1, 2027, MFIPPA will require institutions to complete and maintain PIAs for prescribed activities. FIPPA institutions have been subject to these requirements since July 2026.

Ontario

Where Should Municipalities Focus Their PIA Efforts?

Not every initiative presents the same level of privacy risk
When resources are limited, municipalities should prioritize initiatives that introduce new collections, uses, disclosures, technologies, or privacy risks.

✓ **New Programs and Services**
- Programs involving the collection of new personal information or personal information being collected for a new purpose.
- New user-facing services and service delivery models.

✓ **New Technology Implementations**
- Enterprise software implementations.
- Cloud-based solutions.
- SaaS platforms and managed service providers.
- Modernization or replacement of legacy systems.

✓ **Artificial Intelligence and Automated Tools**
- AI enabled applications.
- Automated decision-making tools.
- Technologies used to analyze, predict, or classify information about individuals.

✓ **Third Party Service Providers**
- Vendors handling municipal personal information.
- Shared service arrangements.
- Outsourced program delivery.

✓ **Third Party Service Providers**
- Expanding an existing program to collect additional personal information.
- New information-sharing arrangements.
- Changes to retention, access, or disclosure practices.

Low-Priority Examples
- Administrative changes that do not affect personal information.
- Routine updates to existing forums where information practices are unchanged.
- Minor operational/procedural changes with no privacy impact.

Common Question: Shared Services and Joint Procurements

Considerations for Municipal Partnerships

- Many municipalities use shared systems and services.
- Municipalities should clearly understand their respective roles and responsibilities.
- Shared assessments may support efficiency and reduce duplication.
- Participating institutions should consider local circumstances, business processes, and risks.
- Governance and accountability arrangements should be documented.

Municipalities shouldn't assume they need to start from scratch every time, but they should ensure any shared approach appropriately reflects their own operational realities, risks, and responsibilities.

Common Question: Do We Need a PIA for Everything?

Beginning January 1, 2027, institutions must:

- Complete and maintain a PIA before collecting personal information for prescribed activities.
- Update an existing PIA before making a significant change to the purpose for which the personal information is used or disclosed.

PIA Requirement is Not Retroactive

- Institutions are **not required to complete PIAs retroactively** for collections of personal information that occurred before January 1, 2027.
- For initiatives that existed before January 1, 2027, institutions should consider whether activities occurring after that date involve a **new or changed collection of personal information**.

Institutions should also consider conducting or updating a PIA where changes involving personal information could increase privacy impacts or risks, including:

- Introducing a new purpose for using or disclosing personal information.
- Expanding a program or service in a way that changes how personal information is used or disclosed.
- Introducing or modifying a technology, system, or process that changes personal information practices.
- Establishing or changing an information-sharing arrangement.
- Migrating personal information to a new platform, environment, or service provider.
- Implementing new functionality, analytics, automation, or AI tools that affect personal information.

Introducing the PIA Resource Suite

Supporting Municipalities in Preparing for January 1, 2027

To support implementation of the new PIA requirements, the Ministry has been developing a suite of practical resources designed to help institutions:

- Understand legislative requirements.
- Determine when privacy assessments may be needed.
- Conduct and document PIAs.
- Identify and mitigate privacy risks.
- Establish repeatable and scalable privacy review processes.

Our Approach

- ✓ Resources are designed to be practical and adaptable.
- ✓ Resources support institutions with varying levels of privacy maturity.
- ✓ Resources were informed by municipal engagement with stakeholder feedback.
- ✓ Resources are intended to support implementation, not replace institutional decision-making.

Two Templates to Support Different Municipal Needs

PIA Report Template (Released October 13, 2026)	**Enhanced PIA Report Template** (To be released in November/early December)
A streamlined, "legislation-based" compliance approach • Involve lower privacy risk or less complex personal information practices. • Require a practical and efficient assessment process. • Have limited organizational capacity or privacy resources. • Present fewer information-sharing, vendor, or technology considerations. • Benefit from a more focused assessment that still addresses core MFIPPA requirements.	**A comprehensive "best practice" approach for more complex initiatives** • Involve higher privacy risks or significant collections of personal information. • Introduce new technologies, platforms, or service delivery models. • Include multiple stakeholders, vendors, or information sharing arrangements. • Require more detailed analysis of privacy risks and mitigation measures. • Benefit from expanded documentation and governance.
Examples	
- Minor enhancements to existing programs. - Low-risk service improvements. - Low-risk or limited in scope technology implementations.	- Enterprise technology implementations. - Cloud-based service platforms. - AI-enabled solutions. - Shared service arrangements. - Major program modernization initiatives.



There is no one-size-fits-all approach to PIAs.
Municipalities should select the assessment approach that best aligns with the complexity, scope, and privacy risks of the initiative. The goal is to apply a level of analysis that is proportionate to the initiative being assessed.

Ontario

October Release – Foundational Resources

Product Name	Purpose	When to use it
PIA Guidance	Provides an overview of PIAs, including when a PIA is required, what a PIA must address, and key responsibilities under MFIPPA. It also explains how PIAs fit within the broader privacy framework and identifies tools and resources available to support institutions in conducting and documenting PIAs.	Use to orient as to what a PIA is and why they are important, when a PIA is required, what it must address, and related legislative requirements under MFIPPA. Also reminds users of other available tools and resources.
PIA Template	Provides a template institutions can use or adapt to document their PIA, along with a quick reference guide.	Use to document the PIA. The report template provides a structured format for recording initiative details, privacy analysis, findings, recommendations, and mitigation actions.
PIA Template User Guide	Provides more substantial guidance to support institutions in using the PIA Template to work through the PIA requirements in subsection 28(3). It connects each requirement to the related MFIPPA rules that inform the analysis, setting the full legislative context for the reporting requirements. Also provides practical tips, examples and key reminders.	Use as a companion as needed while completing the PIA Template. The guide explains how to complete each section, identifies what information should be documented, and provides practical tips, examples, and privacy considerations.

November Release: Expanding the PIA Resource Suite

The **Enhanced PIA Suite** was developed to supplement initial municipal supports with more detailed guidance, examples, and practical tools. It is may be suitable for institutions undertaking more complex initiatives, including those seeking to implement privacy best practices beyond the minimum legislative requirements.

Product Name	Purpose	When to use it
Enhanced PIA Template	Assists municipalities to achieve compliance with section 28(3), which requires a PIA to be conducted before new collections of personal information after January 1, 2027.	Conducting and documenting a PIA for an initiative that involves the collection, use, disclosure, retention, or disposal of personal information.
Enhanced PIA Template User Guide	Supplements the Enhanced PIA Report Template with guidance and advice on how to use it. It is intended for both new users with smaller initiatives and to scale to support experienced privacy professionals involved in more complex initiatives.	While completing the Enhanced PIA Template and instruction, examples, or best practices are needed.
Supporting Tools		
PIA Process Methodology	Provides a structured, repeatable approach for planning, conducting, documenting, reviewing, and maintaining PIAs. It guides institutions through each stage of the PIA lifecycle, helping project teams identify privacy risks, assess compliance with MFIPPA requirements, document findings and mitigation measures, establish accountability, and support ongoing monitoring as programs, services, or systems evolve.	For insights into recommended processes and approaches that can be helpful when planning and managing the overall PIA process. It can serve as a companion to support either of the PIA report templates.
Initial Assessment Questionnaire	A preliminary screening tool that helps determine whether an initiative involves personal information and whether a PIA may be required. It supports the early identification of privacy considerations by capturing key information about an initiative, its objectives, and the personal information involved.	At the outset of an initiative to gather foundational information about the program, service, system, or project and determine whether a PIA may be required.
PIA Compliance Checklist	A practical checklist that supports documenting and validating the core elements of a PIA, including personal information holdings, purposes of collection, legal authority, information sources, access controls, retention requirements, privacy risks, safeguards, and mitigation activities.	Before finalizing a PIA to validate that subsection 28(3) requirements and all required privacy considerations have been addressed.
Key Questions Tool	Helps to document the types of personal information collected, the purpose of its collection, legal authority, sources, access, limitations, retention period, and associated privacy risks and mitigation steps.	When identifying and documenting how personal information is handled and assessing privacy risks, compliance requirements, and mitigation measures.

How the PIA Resources Work Together

Need	PIA Resource
Understand PIA requirements	PIA Guidance
Triage the initiative by determining if a PIA is required	Initial Assessment Questionnaire
Gathering Information	PIA Information-Gathering Questions
Choose the most appropriate assessment approach	MVP PIA Suite or Enhanced PIA Suite
Conduct the assessment	PIA Process Methodology
Review and validate	PIA Compliance Checklist
Implement and track recommendations	MVP PIA Suite or Enhanced PIA Suite
Revisit/Update	- MVP PIA Suite or Enhanced PIA Suite - PIA Initial Assessment Questionnaire - PIA Process Methodology

What Should Municipalities Do Now?

Preparing for January 1, 2027

- Identify in the institution who is accountable for privacy decision-making.
- Review upcoming projects involving personal information.
- Establish a process to identify initiatives requiring privacy review.
- Familiarize staff with the PIA resources.
- Prioritize higher-risk initiatives.
- Begin integrating PIAs into project and procurement lifecycles.