AUGUST 2026

Appendix E to Policy ADM-017
By-law 69-2026

Planning for Success: Privacy Impact Assessment Guide for Ontario's Public Institutions



Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

This guidance by the Office of the Information and Privacy Commissioner of Ontario (IPC) is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws and advance best practices. It should not be relied upon as a substitute for the legislation itself or as legal advice. It does not bind the IPC, which may be called upon to independently investigate and/or decide an issue based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit **www.ipc.on.ca**.

Contents

Introduction 1

Background 2

Methodology 6

1. Preliminary analysis 7

2. Project analysis 9

3. Privacy analysis 15

4. PIA report 19

Appendix A:
Preliminary analysis
questionnaire 23

Appendix B:
Project analysis questionnaire 28

Appendix C:
Privacy analysis checklist 37

Appendix D:
PIA report template 62

Appendix E:
Additional resources 68

Document History

Publication Date	Document Title	Description of Changes
August 2026	Planning for Success: Privacy Impact Assessment Guide for Ontario's public institutions	Updated to incorporate the statutory requirements of MFIPPA in force effective January 1, 2027.
November 2025	Planning for Success: Privacy Impact Assessment Guide for Ontario's public institutions	Updated to incorporate the statutory requirements of FIPPA in force effective July 1, 2025, and to reflect current guidance, terminology, and resources.
May 2015	Planning for Success: Privacy Impact Assessment Guide	Initial publication

Introduction

This guide is intended for institutions subject to Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) or *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). It is meant to help institutions conduct a privacy impact assessment (PIA) in accordance with these laws and best practices.[1]

The guide provides institutions with step-by-step advice on how to do a PIA from beginning to end. It will complement and support any existing requirements for PIAs that are unique to your institution. You should consult with staff responsible for privacy, project development, and risk management within your institution to ensure you comply with any additional legal or policy requirements that may apply.[2] The guide can also serve as a starting point for your institution to develop or update its own PIA methodology and processes.

For the purposes of this guide, project refers to any work involving the collection, use, retention, disclosure, security, and disposal of personal information. This may include a new program, process, service delivery model, or information technology system, or changes to an existing program, process, or system.

Comments or questions

The Information and Privacy Commissioner of Ontario welcomes your comments or questions about this guide. Please direct them to **info@ipc.on.ca** or 416-326-3333/1-800-387-0073 (within Ontario).

1 The IPC's ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*** provides information on how to conduct a PIA involving personal health information regulated under that act.

2 For example, Ontario ministries and agencies are subject to requirements under numerous directives, policies and standards, such as those related to recordkeeping, access and privacy, procurement, information technology, and cybersecurity.

Background

Mandatory privacy impact assessments (PIAs) under FIPPA and MFIPPA

- **PIAs are expressly mandatory for all institutions subject to Part III of FIPPA as of July 1, 2025. PIAs are expressly mandatory for all institutions subject to MFIPPA as of January 1, 2027.**[3] Institutions must complete a written PIA before collecting personal information to evaluate privacy and security risks and outline prevention and mitigation steps, **unless a regulatory exception applies**.[4]
- The new PIA requirements apply to both recorded and unrecorded personal information.[5]
- PIAs must be done in writing, and contain, at minimum, the mandatory information set out in FIPPA and MFIPPA,[6] which includes:
  - the purpose for collecting, using or disclosing personal information and an explanation of why the personal information is necessary to achieve that purpose
  - the legal authority that the institution is relying on to collect, use or disclose the personal information
  - the types of personal information to be collected and, for each type, how it is intended to be used or disclosed
  - the sources of the personal information to be collected
  - the position titles of the institution's officers, employees, consultants or agents who will have access to the personal information
  - any limitations or restrictions imposed on the collection, use or disclosure of the personal information
  - the period of time that the personal information will be retained by the institution
  - an explanation of the administrative, technical and physical safeguards that would be used to protect the personal information and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information
  - the steps to be taken by the institution to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information, and to mitigate risks to individuals in the event of such a privacy breach

3 See sections 38(3)-(6) of FIPPA and sections 28(3)-(6) of MFIPPA. There are also specific PIA requirements for data integration units under Part III.1 of FIPPA. This guidance document is not a substitute for those requirements.

4 Future regulations made by the Lieutenant Governor in Council under FIPPA or MFIPPA may provide for exceptions to the requirement to complete a PIA before collecting personal information. As of the date of publication of this updated guidance, the government has not enacted any such regulations.

5 Sections 38(1) of FIPPA and 28(1) of MFIPPA, which apply to the PIA requirements in sections 38(3)-(6) of FIPPA and 28(3)-(6) of MFIPPA, expand the acts' general definition of personal information to include unrecorded personal information.

6 See section 38(3) of FIPPA and 28(3) of MFIPPA. Exceptions and additional information to be included in PIAs may also be prescribed in regulation. As of the date of publication of this updated guidance, the government has not enacted any such regulations.

- The steps set out in the PIA to prevent and mitigate risks must generally be implemented before collecting personal information.[7]
- Prior to making any significant change to the purpose for which the personal information is used or disclosed, institutions must update their PIAs and implement any additional steps necessary to prevent and mitigate risks subject to prescribed exceptions.[8]
- Institutions are required to provide the Information and Privacy Commissioner of Ontario with PIAs upon request.[9]

7 See section 38(4) of FIPPA and 28(4) of MFIPPA.
8 See section 38(5) of FIPPA and 28(4) of MFIPPA.
9 See section 38(6) of FIPPA and 28(4) of MFIPPA.

Why conduct a PIA?

A PIA is a risk management tool used to anticipate and address the potential privacy risks or impacts of a new or modified collection, use or disclosure of personal information, or of a proposed or existing information system, technology, program, process or other activity. Many institutions' policies require PIAs for projects involving personal information. For institutions subject to sections 38(3)-(6) of FIPPA or 28(3)-(6) of MFIPPA, conducting a PIA is a legal requirement that must be fulfilled before collecting personal information, subject to any exceptions set out in regulation.

Privacy risks or impacts fall into two broad categories:

- **Risks to individuals**, including the theft, loss, or unauthorized use or disclosure of personal information, which may lead to identity theft and other forms of fraud, adverse impacts on employment or business opportunities, damage to reputation, embarrassment, distress, or financial loss.
- **Risks to institutions**, including the financial, legal, and reputational impacts of privacy breaches, and the consequences of failing to comply with FIPPA and MFIPPA.

Carrying out a PIA does not need to be complex or time consuming, but thoroughness is necessary to ensure that potential privacy risks are identified and mitigated. The complexity of a PIA and the resulting documentation will depend on the complexity of the project and your institution's needs.

The benefits of conducting a PIA may include:

- meeting the legal requirements of sections 38(3)-(6) of FIPPA or 28(3)-(6) of MFIPPA and/or best practices
- demonstrating due diligence and evidence of compliance to support informed decision-making during the development of the project (this information may also be important in the event of a privacy breach or complaint to the IPC)
- reassuring individuals, other institutions, partners and your own management that legal requirements and privacy best practices are being followed
- reducing institutional risk by helping to promote more informed and risk-based decision-making and building a culture of privacy within your institution
- improving institutional transparency and enhancing individual awareness, understanding, and trust of your institution's information management practices
- being better prepared in the event of a privacy breach by documenting, in advance, the steps your institution will take to mitigate the risks of a privacy breach, and how it will respond in the event a breach occurs
- improving operational efficiencies, especially when undertaken early and systematically, by helping minimize excessive and unnecessary collection, use, retention and disclosure of personal information, avoiding costly design mistakes and retrofits, and identifying simpler and less costly solutions from the start

Further, PIAs are widely recognized as a best practice in Ontario, across Canada, and globally. They have become essential tools in the analysis of privacy implications associated with information management systems, programs, and technologies used by institutions today.

When to conduct a PIA

Under section 38(3) of FIPPA or 28(3) of MFIPPA, there is a general requirement to conduct PIAs before collecting personal information. Under section 38(5) of FIPPA and 28(5) of MFIPPA, PIAs must also be updated before making any significant change to the purpose for which personal information is used or disclosed.

Institutions should also conduct or update PIAs whenever there are new or changed personal information practices that have the potential to increase adverse impacts on individuals' privacy: for example, changes to technology platforms that house or process personal information, changes to the purposes to which the personal information will be put, or changes to retention periods for personal information.

To be effective, PIAs should be started early in project development or design to build in privacy protection throughout the project's lifecycle — from beginning to end. It is faster, easier and more economical to address privacy risks on a proactive basis during the project design than it is to retrofit privacy protection requirements once your program, process, or system has been implemented.

Responsibility for a PIA

Each institution must decide who will co-ordinate and carry out the PIA. Some institutions will have internal staff who are well-placed to conduct a PIA. Depending on the complexity of the project and the availability of expertise within your institution, you may need to hire an external specialist to conduct your PIA. Institutions also need to define who will review and approve the PIA (separately from who conducted it), who will be responsible for implementing recommendations to address identified privacy risks, and who will be responsible for updating the PIA on an as-needed basis.

In most cases, an effective PIA will require consultation with various individuals who have specialized roles, expertise, and insight into the project.

Methodology

The PIA process generally follows four key steps, each of which is described in detail in this guide.

Step 1: Preliminary analysis

- Examine the project to determine if it will involve the collection, use, retention, disclosure, security or disposal of personal information.
- If you determine that the project WILL involve personal information, proceed with the PIA process. If the project WILL NOT involve personal information, you do not need to proceed with the PIA process.

Step 2: Project analysis

- Gather more specific information about the project, its scope and key characteristics, roles and responsibilities of parties, including third parties, the type of personal information involved and the manner in which the personal information will be collected, used, retained, disclosed, secured or disposed of.

Step 3: Privacy analysis

- Using information gathered in the previous step, identify FIPPA or MFIPPA requirements and potential risks and impacts to privacy.
- Consider ways to reduce or eliminate the risks and impacts identified.
- Assess proposed solutions and their relative advantages and disadvantages.

Step 4: PIA report

- Obtain approval to proceed with recommended solutions.
- Document your findings and chosen solutions in a PIA report.
- Proceed with the project, ensuring that the recommendations from your PIA are fully incorporated in the project plans and implemented.

1. Preliminary analysis

The first step is to determine if the project will involve personal information.[10] If it will not, you do not need to proceed further with the PIA process. Whatever the answer, you should document your conclusion and how you arrived at it. If the project will involve personal information, then you will need to continue with the PIA process.

Helpful resource

Appendix A is a preliminary analysis questionnaire that will help you determine if the project will involve personal information and, if so, identify the types of personal information that will be collected, used, retained, disclosed, secured and disposed of.

What is personal information?

Section 2(1) of both FIPPA and MFIPPA define personal information as ***recorded information about an identifiable individual*** (that is, a natural person). Sections 38(1) of FIPPA and 28(1) of MFIPPA expand the section 2(1) definition to specify that, for the purposes of the collection requirements under FIPPA and MFIPPA[11] personal information includes information that is not recorded. Among other things, this means that the PIA requirements in FIPPA and MFIPPA apply to unrecorded personal information as well as recorded personal information.

Personal information can include, but is not limited to:

- an individual's biographical details (name, sex, age, race)
- an individual's biological details (face, fingerprints, blood type, etc.)
- nationality
- religion
- marital status
- education
- medical or criminal history
- financial information
- identifying numbers, for example, social insurance numbers
- an individual's contact details (personal address, phone number, etc.)
- personal opinions and views

This list of personal information is not exhaustive. An institution may have other types of personal information in its custody or under its control, or additional information that may be considered personal information due to context. There must be a reasonable expectation that an individual can be identified from the information (either alone or when combined with other information) for the information to qualify as personal information.

10 In particular, note that PIAs are required before collecting personal information, subject to any exceptions set out in regulations, as of July 1, 2025 under FIPPA and January 1, 2027 under MFIPPA.

11 Sections 38 and 39 of FIPPA and sections 28 and 29 of MFIPPA.

Tip: Business versus personal information

Information that may seem personal, such as name and contact information, may not be personal information if that information relates to an individual's business activities, that is, they are acting in a professional capacity with respect to that information.

Therefore, it is important to consider the context when determining if the project involves personal information.

Preliminary analysis questionnaire

The preliminary analysis questionnaire (Appendix A) directs you to analyze and document certain aspects of the project and to identify whether it will collect, use, retain, disclose, secure or dispose of personal information and if so, the type of personal information involved.

The questions are designed to be completed by project staff or others without a background in privacy.

You are encouraged to complete the preliminary analysis early in the project so you can determine whether the PIA process and resulting analysis need to be built into the project planning. As a result, it is possible that you may not be able to answer some of the questions. If the answers are unknown when you complete your preliminary analysis, you should revisit it as you proceed with the project and its details become defined.

When completing the preliminary analysis questionnaire, consider all aspects of the project, and think about:

- information recorded in all media (for example, personal information may be stored in paper records, but it may also be stored in electronic media, including emails, video, phone records, computer logs, etc.)
- whether the project involves unrecorded information, for example, information collected orally
- whether previously separate information will be linked (linking information can increase the potential to identify an individual, even if the information itself is not considered personal information)
- whether you will be required to share personal information between programs, institutions or other organizations for the project[12]

12 Information sharing is the disclosure of personal information (including sale) for a specific purpose by the institution that collected the information, to another institution, to another government, to a person or group of persons or to an external organization. Consult your staff responsible for privacy to determine if your institution must comply with information sharing requirements (internal or external). For example, the OPS' Corporate Policy on the Protection of Personal Information defines mandatory requirements for an information sharing agreement.

- whether third parties outside your program area or institution (such as third party service providers) will be able to collect, use, disclose, retain, secure or dispose of any personal information[13]
- whether the project will involve personal information that is maintained for the purpose of creating a publicly available record[14] or excluded from the acts under section 65 of FIPPA and section 52 of MFIPPA (if it does, consult with your legal and privacy staff to determine if you should continue with the PIA process because, for example, other legislation or policies may define privacy requirements that must be complied with)

Once you have completed the preliminary analysis questionnaire, you should have:

- a description of the project's purpose, scope and key objectives
- an understanding of the information involved in the project, and whether or not personal information will be involved
- a description of the types of personal information that will be collected, used, retained, disclosed, secured or disposed of by the project
- a statement about whether you will need to proceed with the PIA, and reasons why or why not

If your analysis determines that the project will collect, use, retain, disclose, secure or dispose of personal information, you should continue with your PIA process. If your preliminary analysis concludes that personal information will not be involved, then a privacy impact assessment will not be necessary, subject to any possible changes over time.

Ensure the project lead and other relevant decision-makers are aware of and agree with your assessment and conclusion. Update the project plan, if required, to make sure all appropriate PIA steps and analyses are completed prior to implementation.

2. Project analysis

If the project will involve the collection, use, retention, disclosure, security or disposal of personal information, you should complete this second step of the PIA process. It extends and deepens the information gathering activities initiated as part of the preliminary analysis (Step 1) and begins to compile information that will be needed to carry out a more detailed privacy analysis (Step 3).

In this step, you will need to define the details of the project so as to identify its potential impact on privacy. Among other things, you will need to identify:

- key characteristics of the project that may create privacy risks
- the activities and business processes involved
- the flow of personal information in the project, including to and from third parties

13 The use of third parties can raise privacy concerns that must be addressed in your PIA. To learn more, refer to the IPC's guidance on ***Privacy and Access in Public Sector Contracting with Third Party Service Providers***.

14 The privacy rules defined in FIPPA and MFIPPA do not apply to personal information that is maintained for the purpose of creating a record that is available to the general public. See section 37 of FIPPA and section 27 of MFIPPA.

- who will be doing what with the information, including, when, how and for what purposes
- the technology or technologies involved in the project

Assemble the PIA team

Identify the subject matter experts needed to complete the project analysis questionnaire (Appendix B), including staff with knowledge in the following areas:

- **Business processes:** relevant business objectives, processes, roles and responsibilities, and required resources
- **Information technology:** relevant technology policies, practices and operational standards
- **Security:** relevant administrative, technical and physical safeguards, practices and measures
- **Information management:** relevant policies, practices, and standards, including applicable retention schedules
- **Legal:** applicable legislation, regulations, bylaws and other legal requirements, service level agreements, memoranda of understanding, contracts, etc.
- **Procurement:** rules and processes, acquired or outsourced product and service solutions
- **Risk assessment:** risk assessment methodology
- **Privacy:** applicable privacy laws, policies, practices, principles and best practices
- **Front end users:** staff and other parties who will use the systems or information collected or created by the project with knowledge and experience with the practical implications

Depending on the scope and complexity of the project, other areas, partners, and interested parties may need to be consulted.

Facilitated group discussions with the various areas impacted by the project may help you complete the PIA steps and better identify and mitigate risks.

Define scope

Define what will be in and out of the scope of your PIA and obtain agreement on the scope from all team members before you begin. Make sure the project lead and other relevant decision-makers approve the scope.

The scope of your PIA may not necessarily coincide with the scope of the broader project. For example, the privacy risks and impacts might arise in only some parts of the project, or your PIA may only need to cover a specific, narrow change to an existing program, process or system and not all aspects of the existing program, process or system.

Assemble relevant background information

Gather all project-related documentation, including information about business processes, workflow, information flows, and business rules. Much of this information may already be found in the project's business case and other project management documentation, previous privacy and security assessments, training materials, policies and procedures and business and IT design documents.

The type of information available will depend on whether you are creating something new or modifying an existing program, process or system and, potentially, the timing of your analysis. Where documentation is incomplete or unavailable, consult with key staff, partners, and other interested parties, including third parties, on existing and proposed activities relevant to the project.

Define relevant business processes

Business processes refer to the various activities that will be conducted during the project. These can include anything from technical processes (such as system back-ups or data processing) to administrative functions (such as reviewing applications, filing and archiving), to policy and ongoing monitoring of a program, system or process. You will need to consult with the subject matter experts in various areas to ensure that you have recorded all applicable activities.

Start by documenting, in a general manner:

- all existing and proposed activities associated with the project (paper based as well as automated), including all parties, technology, and information associated with each activity
- the current information technology environment of your institution, and how it may be impacted by the project
- how the project's business processes will relate to other existing or planned programs, systems or processes, including how information flows from one to another
- whether the project will change an existing program, system or process, and how it will impact or alter current business processes, information flows, roles and responsibilities

Define supporting technology

You should determine if the technology used or developed as part of the project has privacy implications. Identify and document the technology-related components of the project and think about the following:

- How will existing technology be used or new technology be developed to enable or support each step in the business process?
- How will each technology interact with personal information?
- Who will have access to personal information using each technology?
- Are there any back-end processes in these technologies that auto-create records or store information in a way that is not immediately accessible by the user?

Define roles and responsibilities

You should identify and document the roles and responsibilities of all parties to be involved in the project when implemented, noting who may have access to or manage personal information. Make sure to include all relevant partners and other third parties.

If the project will change an existing program, system, or process, determine whether it will change what types of personal information are collected, accessed, used, retained, disclosed, secured, or disposed of. You should also determine how those activities are undertaken, and who is responsible for the personal information throughout the project's lifecycle.

Think beyond dedicated program staff when identifying who will be involved in the business processes and information flows. For example, think about whether the following are or will be involved:

- the public
- clients
- other employees or officers of your institution
- staff in other programs or institutions
- information technology staff (e.g., a system administrator)
- external legal counsel
- other governments
- partners, vendors, or agents of the institution
- consultants
- auditors
- law enforcement agencies

Define relevant information

Consider the various types of information that will be collected, accessed, used, retained, disclosed, secured or disposed of during each business process and activity. In particular:

- identify all records involved (including existing and proposed, hard copy and electronic, etc.)
- describe the types of information that will be collected, accessed, used, retained, disclosed, secured or disposed of in each business process or activity (including recorded and unrecorded information, personal and non-personal information)
- identify any particularly sensitive personal information associated with the business processes, such as medical information, criminal history, etc.

Document personal information flows

Once you have defined the business processes, supporting technology and information, and identified the personal information involved, determine how it will flow through the business processes and technology.

If the project proposes to change an existing program or system, or link different datasets, determine whether it will alter the amount, type, sensitivity or source of personal information involved in the relevant business process.

Map the flow of personal information in all formats, from creation or collection until final disposition (such as, for example, secure destruction or transfer to appropriate archives). Use diagrams or descriptions that are readily understood by the project and decision-makers.

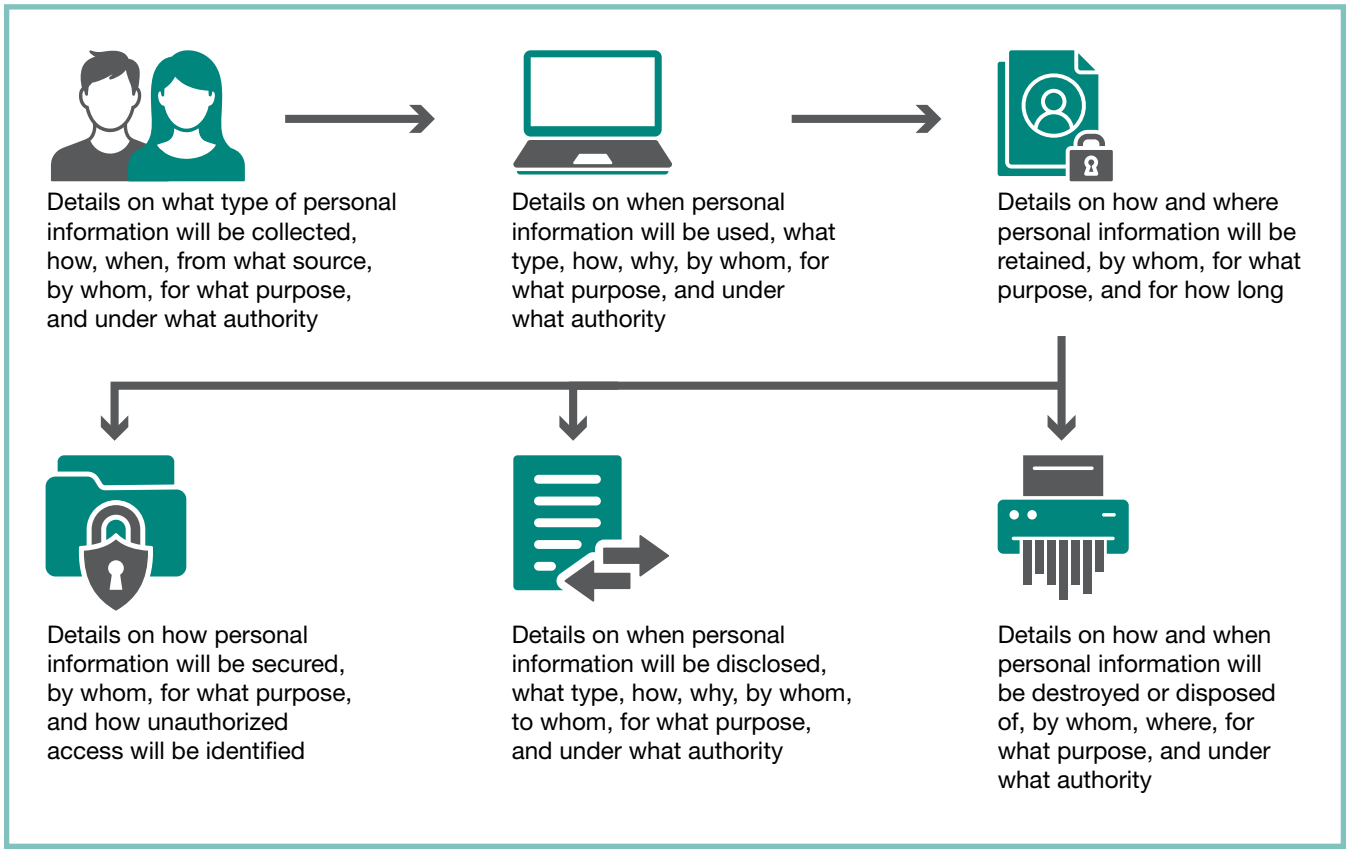
An information flow table or diagram can help you visualize personal information flows associated with the project. These may be organized by some, or all, of the following categories:

- personal information
- source of information
- collected by
- collection method
- purpose of collection
- format of the information
- purpose of use
- used by
- security control during information transfer
- information repository format
- storage retention site
- purpose of disclosure
- disclosed to
- retention policy
- disposal or destruction policy

For example:

Information flow for personal information						
TYPE	COLLECTED	USED	RETAINED	SECURED	DISCLOSED	DISPOSED OF
Details on personal information type	Details on how personal information will be collected, when, where, from what source, by whom, for what purpose, and under what authority	Details on how personal information will be used, when, why, by whom, for what purpose, and under what authority	Details on how and where personal information will be retained, by whom, for what purpose, and for how long	Details on how personal information will be secured, where, by whom, for what purpose, and how unauthorized access will be identified	Details on when personal information will be disclosed, how, when, why, by whom, to whom, for what purpose, and under what authority	Details on how and when personal information will be destroyed or disposed of, by whom, where, for what purpose, and under what authority

Alternatively, information flow diagrams may be visual, such as in this diagram:



3. Privacy analysis

This third step involves a detailed examination of the privacy risks arising from the project and the identification of potential solutions to address them. This will include any mitigation measures, or other limitations or restrictions imposed on the collection, use or disclosure of the personal information.

To be effective, this step should be informed by complete and accurate information about the project, as well as a solid understanding of relevant privacy laws, regulations and other compliance requirements. In addition, your institution's practices related to privacy, information management, technology, security and risk management will also be relevant to your analysis. Existing policies and procedures, or the lack thereof, can be a significant factor in your institution's ability to address privacy risks.

Helpful resource

Appendix C is a privacy analysis checklist that will prompt you to examine your legislative and other privacy requirements and determine and document whether the project will comply. If not, you will need to identify associated privacy risks and impacts and then define action items needed to mitigate them.

Note: Refer to the specific provisions set out in FIPPA or MFIPPA when you are using this checklist to ensure that you have considered all of the provisions of the legislation that may apply to the project.

Privacy impact or risk

A privacy impact is anything that could jeopardize or negatively impact an individual's privacy. For example, theft, loss or unauthorized collection, access, use, retention or disclosure of personal information can result in identity theft or other forms of fraud, physical safety issues such as stalking or harassment, emotional harms such as stress, financial loss, adverse impacts on employment or business opportunities, or damage to reputation.

A privacy impact can also affect your institution. The public can react strongly to a perceived loss of privacy. It can seriously damage your institution's public reputation and result in loss of public trust. It can also cause operational disruptions, affecting the continuity and quality of service. Your institution may also be at legal risk, for example, due to non-compliance with FIPPA or MFIPPA.

Various circumstances can give rise to a privacy impact or risk, such as:

- failure to have the appropriate legal authority to collect, use or disclose personal information
- use of inaccurate, insufficient or out-of-date information

- unnecessary use or disclosure of personal information (for example, where aggregate or de-identified information would instead be sufficient to achieve the purpose or business objective)
- collection, use, or disclosure of irrelevant personal information or of more personal information than what is needed
- retention of personal information for longer than necessary
- failure to keep information appropriately secure
- failure to grant individuals the right to access or correct their own information

Identify potential gaps in compliance

The privacy analysis checklist should be used to identify compliance gaps and the resulting privacy impact or risk. For each question, document your findings in order to conduct an analysis of each identified issue.

The checklist will prompt you to examine whether the project complies with each of the identified privacy requirements. If not, this is a "gap" in privacy protection and an area of potential non-compliance and privacy risk.

These findings should form the basis of your privacy analysis and be documented in the project's PIA report (Step 4).

Consult your information technology and management, security, legal and privacy experts to help you identify and evaluate potential risks and shortfalls in privacy protection.

Tip: Data minimization

Data minimization is the process of limiting the amount of data collected, used, retained or disclosed to only that which is needed to fulfil the purposes of the project. This process includes ensuring the data is destroyed as soon as it is no longer needed. The collection, use, retention or disclosure of unnecessary personal information is an invasion of privacy.

Therefore, as you identify personal information that will be involved in the project, consider carefully if it is necessary to achieve the purpose or business objective.

If not, it should not be collected, used, retained or disclosed. Limiting the amount of personal information you collect, use, retain and disclose will prevent an unnecessary privacy impact.

Analyze findings

Each finding should be analyzed to identify potential privacy risks and impact by considering:

- **Objective:** Start your analysis with the objective of protecting privacy and complying with FIPPA or MFIPPA to maintain public trust.
- **Data minimization principle:** Determine if there is a way to implement the project without collecting, using, retaining or disclosing personal information, or if not, then minimizing the personal information involved.
- **Privacy impact:** Consider the privacy risks or potential impacts resulting from each compliance gap from the perspective of the affected individuals as well as your institution:
  - Try to put yourself in the shoes of the affected individual when assessing harm.
  - Think of the impact on affected individuals, as well as the group(s) of which they are a part.
  - Assess the number of individuals affected, as well as the gravity of the impact. For example, mismanaging the personal information of even a few individuals could have a serious impact on them.
  - Consider the impact on your institution's reputation in the event of non-compliance, and its ability to maintain public trust.
  - Consider the impact on operations, including costs to address a privacy breach after it has happened, when it could have been avoided in the first place.

Understanding the privacy consequences or implications of any compliance gaps is a central part of your privacy analysis. This understanding is necessary to be able to identify action items needed to mitigate the privacy risks and make informed recommendations on how to implement the project in a manner that minimizes any adverse impacts on privacy.

Identify privacy solutions

For each impact, identify actions or possible solutions that will address possible compliance gaps and eliminate or reduce privacy risks. Some common solutions include:

- limiting the amount of personal information involved in the project or deciding not to collect, use or disclose particular types of personal information
- defining or shortening retention periods that will only keep information for as long as necessary and planning for the secure disposal of information
- implementing appropriate administrative, technological, and physical safeguards, practices, and measures
- considering the use of de-identification methods[15] or other privacy enhancing technologies to reduce risks to personal information

15 See the IPC's ***De-identification Guidelines for Structured Data***.

- ensuring that staff are properly trained and aware of the potential privacy impact and appropriate privacy-protective measures to be followed
- producing guidance for staff on how to use new programs, processes, and systems, and how and when it is appropriate to collect, use, access, disclose, and dispose of personal information
- limiting access privileges to only those staff or other individuals or parties who have a need to access personal information for the purpose of carrying out a legitimate business activity
- having staff sign confidentiality agreements on an annual basis to remind them of their obligations to keep personal information secure and of the possible consequences if they do not, in order to discourage lax behaviours or deviation from standard policies, practices, and procedures
- taking steps to ensure that individuals are fully aware of how their information is used and that they can contact the institution for assistance, if necessary (for example, by creating a complete notice of collection and making sure it is accessible to the project's clients)
- selecting third parties that can offer and deliver a greater degree of privacy and security protection, and ensuring that agreements are in place to protect the personal information when in the custody of those third parties
- producing information sharing agreements that clarify what information will be shared, how it will be shared, and with whom it will be shared[16]

Analyze each identified option and consider the potential effectiveness of the solution, and whether it will eliminate or reduce the impact or if it will make the risk acceptable.

Identify action items

Analyzing the effectiveness of each option will help you select the solutions that you believe will be most beneficial for the affected individuals, the project, and your institution. For each impact, identify the specific actions, the responsible party for each item, and the timing for implementation. These will be the mitigation steps needed to minimize privacy risks and potential impacts. Relevant staff should be informed of these and actively involved in implementing mitigation steps as needed.

The action items that you identify are the to do list of items necessary to address prior to project implementation. These will enable the project to achieve its desired objectives while also protecting privacy and complying with FIPPA and MFIPPA.

If the project is already compliant, indicate that no further action is required.

16 An information sharing agreement will clarify the rights and obligations of all parties involved and help with ensuring compliance with FIPPA or MFIPPA. The IPC has guidance on ***Privacy and Access in Public Sector Contracting with Third Party Service Providers***.

4. PIA report

Document the results of your PIA analysis in a way that serves the purpose of the project and supports your decision-makers.

Mandatory information to be contained in a PIA

As of July 1, 2025, under FIPPA and January 1, 2027, under MFIPPA, institutions must have written PIAs that contain, at minimum, the following elements:[17]

- the purpose for collecting, using or disclosing personal information and an explanation of why the personal information is necessary to achieve that purpose
- the legal authority that the institution is relying on to collect, use or disclose the personal information
- the types of personal information to be collected and, for each type, how it is intended to be used or disclosed
- the sources of the personal information to be collected
- the position titles of the institution's officers, employees, consultants or agents who will have access to the personal information
- any limitations or restrictions imposed on the collection, use or disclosure of the personal information
- the period of time that the personal information will be retained by the institution
- an explanation of the administrative, technical and physical safeguards that will be used to protect the personal information and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information
- the steps to be taken by the institution to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information and to mitigate risks to individuals

Institutions must provide a copy of their PIA to the IPC upon request.

A written PIA report can help you achieve several important purposes:

- It provides decision-makers with specific recommendations on how to address privacy impacts, and enables them to make informed decisions about how the project should proceed.
- It documents the results of your analysis that may be requested to be seen by the IPC as evidence of your institution's compliance or may be needed for future reference.
- It demonstrates privacy due diligence, and allows you to make a summary of your PIA publicly available to reassure Ontarians and maintain their trust in the project or initiative.

17 See all PIA related requirements in section 38 of FIPPA and section 28 of MFIPPA.

Helpful resource

Appendix D contains a template with instructions for a PIA report. The headings and description of recommended content can help you prepare and format your PIA report. The template should be adapted to meet your project's and institution's needs and legal requirements.

Write your report so it can be readily understood by a non-technical audience (those who are not privacy, legal, technology or security experts). Make sure to include sufficient details and explanations, so that someone outside of the project can understand how you came to your conclusions and recommendations.

Obtain approval

Appropriate approvals of your PIA should be informed by the results of your privacy analysis and your recommended steps to mitigate any privacy risks or impacts.

Approval of your PIA report by the relevant decision maker in your institution should be contingent on:

- a full assessment of the project's privacy risks and impacts
- the decision-makers' understanding of the privacy risks and impacts
- all of the project's identified compliance gaps having been appropriately addressed or accepted
- the decision maker's acceptance of the mitigation steps needed to address the privacy risks and impacts or their acceptance of those privacy risks and potential impacts, should they decide not to proceed with the recommended mitigation steps

Approvals should be properly documented and dated.

Once the action items to address identified privacy risks are approved for implementation, update your PIA report and project plan, if necessary. Institutions must generally implement the steps necessary to prevent and mitigate risks before the collection of personal information can begin.

A copy of your PIA report and all supporting documentation should be included in the project's files to ensure the project team and other key players can access this information, including for the purpose of providing it to the Commissioner upon request.

Update your findings and privacy analysis, as required

As project implementation progresses, continue to assess the project's privacy risks and impacts to determine if you need to update your privacy analysis and PIA report.

Effective July 1, 2025, under FIPPA and January 1, 2027 under MFIPPA, institutions are generally required to update their PIAs and implement any additional prevention and mitigation steps **before** making any significant change to the purpose for which the personal information is used or disclosed.[18] Among other things, updates must include:

- the proposed change to the purpose for which personal information will be used or disclosed and an explanation of why the personal information is necessary to achieve the purpose and
- any additional steps to be taken by the institution to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information and to mitigate risks to individuals in the event of such an occurrence.

This ongoing assessment is an essential part of identifying and mitigating new privacy risks and impacts that arise during implementation.

As the project is implemented:

- monitor progress of privacy-related activities to make sure they are appropriately completed
- assess any changes to the project's implementation (such as business process, information flows, roles and responsibilities) to ensure that new privacy risks have not been created by these changes
- evaluate risk prevention and mitigation steps to determine if they are effective when implemented, and update or revise them if necessary
- identify and assess new, outstanding and remaining privacy gaps and impacts, and identify new action items required to address them
- alert the project lead and relevant decision-makers to any new privacy-related problems, and obtain appropriate approvals to address or accept the privacy risks
- update or supplement your PIA documentation, as required, ensuring you document:
    - the new privacy risks and impacts and how they arose
    - their likelihood, harm and priority for action
    - your mitigation steps to address the new privacy risks

The project lead and other appropriate decision makers should approve all significant changes impacting privacy and the acceptance of any privacy risks, and all such approvals should be documented.

18 See sections 38(3)-(5) of FIPPA and sections 28(3)-(5) of MFIPPA.

Tip: Monitoring and re-assessing

Ensuring the project protects privacy and complies with applicable privacy legislation is not a one-time activity. New issues and changes impacting privacy and compliance may also develop post project implementation.

Therefore, the party or parties responsible for privacy protection and compliance should, on an on-going basis, monitor developments or changes to key aspects of the project. For example, this may involve changes to the purpose for which personal information is used or disclosed, the project scope, business owner, legislative or regulatory authority, business processes, partners or third party service providers, technology functionality, service delivery model, security and information requirements. Such changes may create new privacy risks and trigger the need to update your privacy analysis and prevention and mitigation steps.

When changes or developments occur that impact the project, your institution may need to revisit your PIA and either change it or add to it. Your institution may decide to amend your original PIA or prepare and addendum to your original PIA report. Either way, any changes should be duly documented.

Concluding the PIA process

Before you conclude your PIA process:

- make sure all privacy-related decisions, analysis and actions are appropriately documented
- transfer your PIA documentation to the appropriate parties, such as the program area, or provide them with a copy, to enable ongoing privacy protection and the management of privacy risks once the program, process or system becomes operational

As of July 1, 2025, under FIPPA and January 1, 2027 under MFIPPA, institutions are required to provide a copy of their PIA report to the IPC upon request.[19]

19 See section 38(6) of FIPPA and 28(6) of MFIPPA.

Appendix A: Preliminary analysis questionnaire

1. Project and institution

PROJECT TITLE	
INSTITUTION	
DEPARTMENT	
PROJECT LEAD	

2. PIA lead

NAME AND TITLE	
INSTITUTION	
DEPARTMENT	
PHONE NUMBER	
E-MAIL	

3. Project description

Describe the project (for example, the program, system, application or activity) that is the subject of the PIA, including its purpose, scope, and key objectives. Attach relevant project documentation, if necessary.

4. Collection, use, and disclosure

4.1 Identify the kinds of information involved in the project (check all that apply).

	YES	NO	UNKNOWN
Information about individuals in their personal capacity			
Information about individuals acting in their business, professional or official capacity (for example: name, job title, and business contact information)			
Information about institutions (for example: for profit and not-for-profit institutions and government institutions)			
Aggregated or de-identified information. In the row below, outline the process followed to aggregate or de-identify the information and the potential to identify/ re-identify individuals from that information.			

4.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	COLLECT	USE	RETAIN	DISCLOSE	SECURE	DISPOSE
No personal information						
Unknown at this time (please explain why in row below).						

	COLLECT	USE	RETAIN	DISCLOSE	SECURE	DISPOSE
In the rows below, list the types of personal information involved in the project (add more rows as needed). If third parties will be involved in the project, think about what they may be doing with personal information as well.						
In the rows below, list each element of non-personal information that, when combined or linked, may enable identification of an individual (add rows as necessary).						

4.3 To whom does the personal information relate? List the individuals whose personal information will be involved in the project (in other words, the data subjects).

5. Privacy legislation

5.1 Identify applicable privacy legislation (check all that apply).[20]

	YES	NO	UNKNOWN
Freedom of Information and Protection of Privacy Act			
Municipal Freedom of Information and Protection of Privacy Act			
None or other (Please explain below.)			

5.2 Public records and excluded personal information[21]

	YES	NO	UNKNOWN
Does the project involve any personal information that will be maintained for the purpose of creating a record that is available to the general public? What is the type of personal information, and why and how is it made available to the general public? Please explain in the row below.			
Does the project involve any personal information that will be excluded from the application of the acts by section 65 of FIPPA and section 52 of MFIPPA? What is the type of personal information, and why is it excluded? Please explain in row below.			

20 See the ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*** for information about conducting a PIA involving personal health information regulated under that act.

21 Consult with your legal and privacy staff to determine if you should continue with the PIA process, and if other legislation or policies define privacy requirements that must be complied with.

6. Conclusion

Indicate whether you will proceed with the PIA process and the reasons for your decision. (Institutions must complete a written PIA before collecting personal information, unless a regulatory exception applies.)

Appendix B: Project analysis questionnaire

1. Scope of PIA

Define the scope of the PIA review and analysis. What aspects of the project are in and out of scope?

2. Project authority

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understanding, agreements, contracts and other relevant instruments).

3. Project characteristics

3.1 Identify key characteristics of the project (check all that apply).

DOES THE PROJECT INVOLVE...	YES	NO	UNKNOWN
creating a new program, process, service, technology, information system or other type of IT application?			
a change to an existing program, process, service, technology, information system or other type of IT application?			
a new collection of personal information?			
procuring goods or services?			
outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information?			
developing a request for bids, proposals, or services?			
a process, system or technology for which the privacy risks are not known or well documented?			
creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases?			
information sharing (internal and external)?			
the need to identify, authenticate or authorize users – including public and/or internal staff?			
other activities that may impact privacy? (Please explain below.)			

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed project analysis questionnaire.

3.3 Identify any changes that will result from the project (check all that apply).

WILL THE PROJECT INVOLVE...	YES	NO	UNKNOWN
a change in business owner?			
a change to legislative authority?			
a change in users (internal and external) of a related process or system?			
a change in partners or service providers (internal and external)?			
a change in the amount, type of, or ways that personal information is collected, used, disclosed, retained, secured or disposed of?			
a change to the purposes for which personal information will be collected, used, or disclosed?			
a change from direct to indirect collection of personal information?			
a change in roles and responsibilities (such as who can do what, when, where, why and how with personal information)?			
a change to, or elimination of, existing practices of de-identifying information?			
a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information (for example: hardware and software)?			
a change to an information system or database containing personal information?			

WILL THE PROJECT INVOLVE...	YES	NO	UNKNOWN
a change of medium or service delivery channels (for example: the automation of manual processes, conversion from paper to electronic records, or the creation of a new website to provide services to clients)?			
a change in the security requirements or safeguards, practices, or measures?			
other changes (please specify change or proposed change below)?			

3.4 If you answered yes to any of the above, explain the change(s), including what specifically will change and why it is necessary. Attach all relevant documentation to your completed project analysis questionnaire.

3.5 Document any additional business processes identified from your analysis of the factors identified in the guide. Attach all relevant documentation to your completed project analysis questionnaire.

4. Technology

4.1 Identify technology-related characteristics of the project (check all that apply).

DOES THE PROJECT INVOLVE...	YES	NO	UNKNOWN
technology designed to monitor, track or observe an individual or their transactions (for example: video cameras, cell phones, and geospatial or location-based services)?			
logging information, usage or preferences (for example: IP addresses, traffic data, access or transaction logs, cookies, or other mechanisms for recording an individual's use of technology)?			
public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media?			
using analytics or performance measurements (for example: web analytics, social media analytics, or business intelligence tools)?			
processing or storing of personal information in a virtual environment (for example, cloud computing)?			
acquiring or customizing commercial software, hardware, or IT support services by external vendors?			
developing or customizing software, hardware, or IT support services in-house?			
creating information systems or other types of IT applications that will be populated by others (for example, clients of a system or service will supply information)?			
a system or application that will automatically collect, use, disclose or retain personal information?			
other (Please explain below.)			

4.2 If you answered yes to any of the above, provide an explanation of the technology (that is, purposes, why necessary, and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed project analysis questionnaire.

5. Roles and responsibilities

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role.

INSTITUTION/THIRD PARTY	PROJECT ROLE

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose, secure, or dispose of personal information <u>on behalf</u> of your institution.

INSTITUTION/ THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE

5.3 Identify any location outside of Ontario where personal information may be retained or stored and the third parties involved.

PERSONAL INFORMATION	LOCATION	THIRD PARTY

5.4 List all position titles of the officers, employees, consultants, or agents of your institution who will have access to the personal information. For example, program area staff (by title), IT staff, legal counsel, etc.

POSITION TITLE	RELATIONSHIP TO PROJECT	PROJECT ROLE

5.5 Identify how other institutions or third parties will be bound to follow relevant privacy and security requirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
contracts				
memoranda of understanding				
agreements (service level and trade)				
other (Please explain below.)				

6. Relevant information

Document what and how all types of information relate to each business process and activity relevant to the project. Consider the factors identified in the guide. Attach all related documentation to your completed project analysis questionnaire.

7. Personal information flows

Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project's and your institution's needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your identified flows of personal information throughout the project to your completed project analysis questionnaire.

Appendix C: Privacy analysis checklist

Answering the following questions can help you to identify the privacy risks that need to be addressed and the steps to be taken to ensure compliance with FIPPA or MFIPPA. You can use the table below to organize your work, or it can be adapted to meet the needs of the project and your institution. Be sure to address all the identified questions and consider each instance of how personal information is involved when completing the checklist. For example, when asked about authority to collect, consider all the types of personal information you will collect.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y[22]	N[23]	IP[24]	NA[25]	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
Review each question and determine how each relates to the project. **Note:** Do not use the checklist as a substitute for the legislation. The statutory provisions have been summarized here.	Put a check mark (√) in the appropriate column for each question. This will create a visual representation of the project to assist with complying with FIPPA or MFIPPA. If your findings differ depending upon the type of personal information involved, add rows to document and explain the differences for each type.				Outline how you arrived at your findings. Provide as much information as is available, particularly if action is planned, but not yet implemented. Outline any options or alternatives that were, or need to be, considered. Explain why no action has been taken or planned for each "N" finding, and why requirements are "NA" to the project.	For each finding, outline the potential impact or risk to privacy. For example: a theft, loss or unauthorized use or disclosure of the personal information, non-compliance with FIPPA or MFIPPA, increased intrusiveness into the private lives of individuals, or it does not meet the public's expectation of privacy.	For each finding, identify the action(s) (steps) necessary for compliance with the privacy requirement or to mitigate or prevent a potential privacy impact or risk.

22 **Y (Yes):** You know the privacy protection requirement either has been met by existing safeguards, practices or measures or will be met by action planned before implementation

23 **N (No):** You know nothing has been done or is planned to address this privacy protection requirement; there is a possible privacy risk and "gap" in the project's compliance. If nothing has been done or planned, explain why.

24 **IP (In Progress):** You do not know the answer to the question at this time; more information or analysis is required and, until such time, there is a potential privacy risk and gap.

25 **NA (Not Applicable):** You know this privacy protection requirement is not applicable to the project. Note: Be sure to check with your FIPPA or MFIPPA Coordinator and Legal Counsel.

A. Collection

Key requirements:

- A written PIA report must be prepared before collecting personal information.
- For each collection of personal information, ensure that the institution collects personal information only if it has the authority to do so. Consider the following:
  - Is the collection expressly authorized by statute?
  - Will the personal information be used for law enforcement purposes?
  - Is the collection necessary for the proper administration of a lawfully authorized activity?
  - Why is personal information necessary to achieve the purpose of the collection?
- Personal information must be collected directly from the individual to whom it relates, unless another manner of collection is authorized by the individual or other statutory provision.
- Notify the individual of the collection, including legal authority, purpose(s), and contact information of a person who can answer questions about the collection.
- Risk prevention and mitigation steps must generally be implemented by the institution before collecting personal information.
- See sections 28 and 29 of MFIPPA and sections 38 and 39 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
AUTHORITY							
Is the collection of personal information authorized under FIPPA or MFIPPA or another act?							
Do all parties collecting personal information have legal authority for the collection?							
Have you documented the legal authority for the intended collection?							
Has responsibility for the collection been assigned to program staff or third party service providers?							
PURPOSE OF COLLECTION							
Has each purpose of the collection been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
NOTICE TO INDIVIDUAL							
Will notice of collection be provided to the individual(s)? Explain timing, method, and exemptions from notice, where authorized.							
Will the notice of collection comply with FIPPA or MFIPPA? Explain how or if there are missing components.							
MANNER OF COLLECTION/SOURCE OF PERSONAL INFORMATION							
Will personal information be collected directly from the individual? Explain the types, sources and form of collection.							
Will personal information be collected indirectly from another source, or covertly? Why?							
Will indirect collection comply with FIPPA or MFIPPA? Explain the authority for indirect collection.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will the project only collect personal information for which there is legal authority?							
Will there be any limitations or restrictions imposed on the collection of the personal information?							
Will there be periodic reviews of the collection controls to ensure effectiveness?							
DATA MINIMIZATION							
Is personal information necessary for the project to proceed?							
Is collection of all the personal information necessary? Why or why not?							

B. Use

Key requirements:

- For each use of personal information, ensure that all parties involved in the project, including your institution, partners and other third parties, use personal information only with the authority to do so. Consider the following:
  - Is the use for the purpose it was collected or for a consistent purpose?[26]
  - Is the use authorized by the individual to whom it relates?
  - Does the use comply with another statute?
  - Is the use for other purposes permitted by FIPPA or MFIPPA?
  - Why is personal information necessary to achieve the purpose of the use?
- Before making any significant change to a purpose for which personal information is used, update the PIA report to, among other things, reflect the proposed change and implement additional risk prevention and mitigation steps.
- See sections 28 and 31 of MFIPPA and sections 38 and 41 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
AUTHORITY							
Do all parties using personal information have the legal authority for the use(s)?							
Have you documented the legal authority for the intended use(s)?							

26 A consistent purpose is a use of personal information that the individual to whom the personal information relates might reasonably expect at the time of collection.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
PURPOSE(S) OF USE							
Has each purpose of use been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							
Will personal information be used for other purposes?							
Will uses of personal information be for purposes stated in the notice of collection or for a consistent purpose?							
MANNER OF USE							
Have all parties using personal information been defined by position title (for example: program staff, consultants, agents of the institution, third party service providers, employees, officers etc.)?							
Have you indicated how each type of personal information will be used?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will there be administrative, technical, and physical safeguards, practices, and measures in place to ensure personal information will be used only for authorized purposes and by authorized parties? Explain the safeguards, practices and measures.							
Will there be any limitations or restrictions imposed on the use(s) of the personal information?							
Will there be periodic reviews of the use safeguards, practices and measures to ensure effectiveness?							
DATA MINIMIZATION							
Is use of all the personal information necessary for the project to proceed? Why or why not?							

C. Disclosure

Key requirements:

- For each disclosure of personal information, ensure that all parties involved in the project disclose personal information only with the authority to do so. Consider the following:
  - Is the disclosure for the purpose for which it was collected or for a consistent purpose?[27]
  - Is the disclosure authorized by the individual to whom the personal information relates?
  - Does the disclosure comply with another statute?
  - Is the disclosure for other purposes permitted by FIPPA or MFIPPA?
  - Why is the personal information necessary to achieve the purpose of the disclosure?
- Before making any significant change to a purpose for which personal information is disclosed, update the PIA report to, among other things, reflect the proposed change and implement additional risk prevention and mitigation steps.
- See sections 28 and 32 of MFIPPA and sections 38 and 42 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
AUTHORITY							
Do all parties disclosing personal information have the legal authority for the disclosures?							
Have you documented the legal authority for the intended disclosures?							

27 A consistent purpose is a disclosure of personal information that the individual to whom the personal information relates, that is, the data subject, might reasonably expect at the time of collection.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
PURPOSE(S) OF DISCLOSURE							
Has each purpose of disclosure been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							
Will personal information be disclosed for other purposes?							
Will disclosures of personal information be for purposes stated in the notice of collection or for a consistent purpose?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
MANNER OF DISCLOSURE							
Have all parties disclosing personal information been defined (for example: program staff, consultants, agents, third party service providers, employees, officers, etc.)?							
Have you indicated how each type of personal information will be disclosed?							
Has the manner of disclosure been defined (for example: oral, mail, email, etc.)?							
Will the disclosures be documented and how?							
INFORMATION SHARING AGREEMENT							
Will disclosures be documented and controlled by information sharing agreements or other means?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will there be administrative, technical and physical safeguards, practices and measures in place to ensure personal information will be disclosed for authorized purposes, by and to authorized parties? Explain the safeguards, practices and measures.							
Will there be any limitations or restrictions imposed on the disclosures of the personal information?							
Will there be periodic reviews of the disclosure safeguards, practices and measures to ensure effectiveness?							
DATA MINIMIZATION							
Is disclosure of all the personal information necessary for the project to proceed?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
DISCLOSURE FOR RESEARCH PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for research purposes?[28]							
DISCLOSURE FOR FUNDRAISING PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for fundraising purposes?[29]							

28 Before such a disclosure, there should be a defined and documented process that makes sure the researcher demonstrates why identifiable information is required for the research purpose. The researcher must agree to the terms and conditions of Ontario Regulations 460 and 823, section 10.

29 FIPPA defines when disclosure of personal information by educational institutions or hospitals may be done for fundraising purposes. Before such disclosures, ensure the requirements, as defined in sections 42(2) and (3), have been met.

D. Accuracy and correction

Key requirements:

- Take reasonable steps to ensure personal information is not used or disclosed unless it is accurate, complete and up to date.
- Ensure that every individual can:
  - correct their personal information
  - have a statement of disagreement attached to the personal information if the correction is not made
  - require a notice of the correction or the statement of disagreement to be sent to anyone to whom the personal information was disclosed within the year before the above action was taken
- See sections 30(2) and 36 of MFIPPA and 40(2) and 47 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
STANDARD OF ACCURACY							
Will there be steps in place to make sure personal information is not used, unless it is accurate, complete and up-to-date? Provide details of the steps.							
CORRECTING THE PERSONAL INFORMATION							
Will there be a defined and documented process for the processing of a request for the correction of personal information? Provide details of the process.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CORRECTION REQUESTS/STATEMENT OF DISAGREEMENT							
Will there be a defined and documented process for individuals to request the correction of their personal information? Provide details of the process.							
CONTROLS							
Will controls be in place to ensure that only authorized personnel will be able to add, change, or delete personal information?							
Will there be periodic reviews of the controls to ensure effectiveness?							

E. Security

Key requirements:

- Take all reasonable measures to prevent unauthorized access to personal information in your custody or control, taking into account the nature of the record to be protected.
- Access should be restricted to only those individuals who need the personal information for the performance of their duties.
- Explain the safeguards, practices and measures that will be used to protect the personal information.
- Summarize any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of personal information
- Take all reasonable safeguards, practices and measures to protect personal information against loss or theft, unauthorized access, use or disclosure, inadvertent modification, destruction or damage, taking into account the format of the record to be protected.
- See Ontario Regulation 823, section 3 as well as sections 28 and 30(5) of MFIPPA, and Ontario Regulation 460, sections 3 and 4, as well as sections 38 and 40(5) of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
SECURITY MEASURES							
Will safeguards, practices and measures be used to protect the personal information? Explain each administrative, technical and physical safeguard, practice and measure.							
Will risk prevention and mitigation steps be implemented before collecting the personal information?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will security safeguards, practices and measures be defined and documented to protect the confidentiality, integrity and availability of personal information?							
Will testing and periodic reviews be conducted to ensure that personal information is only collected, accessed, used, disclosed, retained and disposed of when authorized and is not stolen or lost?							
Will all actions relating to the collection, use, disclosure, retention, correction, copying or disposal be logged and subject to auditing and monitoring?							
Will procedures be defined and documented on how to identify, report, investigate and address the theft, loss and/or unauthorized access, collection, uses and/or disclosure of personal information?							

F. Requesting access to personal information

Key requirements:

- Ensure that every individual has a right of access to their personal information in the institution's custody or control.
- Make sure that personal information in the institution's custody or control is retrievable.
- Verify the identity of persons requesting access to their personal information.
- See section 36 of MFIPPA and section 47 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
ACCESS REQUESTS							
Will the management of personal information change or restrict individuals' right of access to their personal information?							

G. Retention

Key requirements:

- Personal information should be retained for at least one year after use to provide the individual with a reasonable opportunity to access their personal information.
- The individual's consent should be obtained in order to dispose of personal information prior to one year after use.
- Ensure compliance with other relevant records retention laws, regulations, bylaws or other requirements.
- See MFIPPA sections 28(3), 30(1), 30.1(8) and Ontario Regulation 823, section 5; FIPPA sections 38(3), 40(1), 40.1(8) and Ontario Regulation 460, section 5.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
RETENTION SCHEDULES							
Will there be defined and documented policies, procedures, and other requirements related to the retention of personal information?							
REASONABLE OPPORTUNITY FOR ACCESS							
Will safeguards, practices and measures be in place to ensure that personal information will be retained for a minimum of one year after its last use?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
MEDIUM AND LOCATION OF RETENTION							
Has the medium and format of the personal information to be retained been defined?							
RETENTION PERIOD							
If the personal information has not been used, will it be retained for only as long as necessary to meet its purpose? How long will it be retained?							
How long will personal information that has been used be retained?							
CONTROLS							
Will procedures be defined and documented related to consent for early disposal of personal information?							
Will there be periodic reviews of the retention requirements and consent procedures to ensure effectiveness?							

H. Disposal and destruction

Key requirements:

- Personal information must be disposed by either securely destroying it or transferring it to the appropriate archives.
- Make sure personal information is only destroyed when authorized by an appropriate party and in accordance with records retention laws/regulations/bylaws applicable to the institution.
- Take all reasonable safeguards, practices and measures to protect the security and confidentiality of personal information to be destroyed throughout the process, that is, when personal information is stored, transported, handled and destroyed.
- Take all reasonable safeguards, practices and measures to protect the security and confidentiality of personal information to be transported to archives throughout the process, that is, when personal information is stored, transported and handled.
- Take all reasonable safeguards, practices and measures to destroy personal information so it cannot be reconstructed or retrieved.
- Keep an accurate record of the disposal, including what personal information was destroyed or transferred and on what date it was destroyed or transferred.
- Do not include personal information in your record of disposal.
- See Ontario Regulation 823 and section 30(4) and (5) of MFIPPA, and Ontario Regulation 459 and sections 40(4) and (5) of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
MANNER OF DISPOSAL							
Will procedures be defined and documented for the secure disposal, for example, transfer to archives or destruction of personal information in accordance with applicable records retention schedules, laws/ regulations/ bylaws? Explain the disposal process.							
DEVICES/EQUIPMENT							
Will procedures be defined and documented for disposal of devices and equipment containing personal information?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will safeguards, practices and measures be defined and documented to ensure only appropriate personal information will be disposed of or destroyed, and only by authorized parties after obtaining appropriate approval?							
Will there be periodic reviews of the disposal safeguards, practices and measures to ensure effectiveness?							
RECORD-KEEPING							
Will details of the disposal of personal information be recorded?							
Will safeguards, practices and measures be defined and documented to ensure no personal information is captured in the disposition record?							

I. Privacy management

The questions in this section relate to privacy management throughout your institution. They are not limited to the project's information system, technology, or program, but address your institution's privacy maturity, capability, and readiness to undertake the project. The emphasis is on accountability and training.

Key requirements:

- Apply common management principles, such as planning, directing, controlling and evaluating the personal information collected, used, disclosed, retained and destroyed by institutions.
- Establish and follow disciplined and consistent practices for the management of personal information.
- Educate staff about privacy, as well as legislative and other relevant requirements.
- Periodically review safeguards, practices, and measures, and commit to ongoing improvement in compliance.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
ACCOUNTABILITY							
Will accountability for managing personal information throughout its lifecycle be defined to include parties involved in the project(for example: your institution, **officers, employees, consultants or agents of your institutions**, partners, vendors and other third parties)? Explain accountability.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
TRAINING							
Will operational safeguards, practices, and measures related to the protection of personal information be needed?							
Have all parties requiring training on operational, security, and privacy aspects of the project been identified?							
Has the individual responsible for ensuring that all parties receive appropriate training been identified?							
AUDITS							
Will safeguards, practices, and measures be developed and documented to evaluate whether the personal information is accessed, collected, used, retained, disclosed, secured, and disposed of in a manner that is consistent with FIPPA or MFIPPA, or if it is stolen or lost?							

Appendix D: PIA report template

Mandatory information to be contained in a PIA

As of July 1, 2025, under FIPPA and January 1, 2027, under MFIPPA, PIAs are mandatory before collecting personal information (subject to any prescribed exceptions) and must contain, at minimum, the information set out in section 38 of FIPPA or section 28 of MFIPPA:

1. The purpose for which the personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose.
2. The legal authority for the intended collection, use and disclosure of the personal information.
3. The types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed.
4. The sources of the personal information that is intended to be collected.
5. The position titles of the officers, employees, consultants, or agents of the institution who will have access to the personal information.
6. Any limitations or restrictions imposed on the collection, use, or disclosure of the personal information.
7. The period of time that the personal information would be retained by the institution, in accordance with subsection 40(1) of FIPPA or 30(1) of MFIPPA.
8. An explanation of the administrative, technical and physical safeguards, practices and measures that would be used to protect the personal information in accordance with subsection 40(5) of FIPPA or 30(5) of MFIPPA and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.
9. The steps to be taken by the institution,
    i. to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and
    ii. to mitigate the risks to individuals in the event of such an occurrence.
10. Such other information as may be prescribed.

Risk prevention and mitigation steps outlined in the PIA must generally be implemented before collecting personal information. It is important that you review both new and existing legal requirements when preparing your PIA report and ensure that it includes all required information.[30]

30 See PIA requirements in section 38 of FIPPA and section 28 of MFIPPA..

Provincial and municipal institutions should use this PIA report template as a best practice document but not as a substitute for the legislation. You should consult with your legal and privacy staff if you have questions about completing a PIA and ensuring compliance with FIPPA or MFIPPA.

Title page

Include the project name, institution/department, date, and the identity of the party who completed the PIA process and prepared the PIA report.

Executive summary

- Provide reviewers and decision-makers with an overview of the project.
- Summarize your key findings, recommendations, and action items.
- Note any outstanding privacy impact.

Table of contents

Include main headings, subheadings, and appendices to enable reviewers to readily locate information.

Introduction

Explain:

- the objective of the project
- the purpose of the PIA Report and the attached appendices
- the response being sought and timelines

Background

General

Provide high-level context for your analysis and findings, including, but not limited to:

- **PIA:** Briefly describe the PIA process including the purposes and outcomes of the preliminary analysis, project analysis, and privacy analysis. Attach completed questionnaires and checklists and supporting documents.
- **Scope:** Briefly describe what is in-scope and out-of-scope in your PIA. Note any related projects, programs, or systems, relevant PIA work, or other risk analysis undertaken by other parties.
- **Glossary:** Explain specialized terms and acronyms used in your PIA analysis and documentation.

Project

Provide a summary of the project including as much detail as is necessary to enable reviewers and decision-makers to understand the project in the context of your privacy analysis. Include the following, in addition to any specific information that you believe is necessary:

- description of the project
- accountability for the project
- related initiatives and linkages
- project partners and interested parties

Privacy

Provide context for your analysis of the project's impact on privacy, including, but not limited to:

- **Personal information:**

  Describe the:

  - purposes for which personal information is intended to be collected, used, and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose
  - types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed
  - source(s) of personal information to be collected, including the category(ies) or class(es) of individuals represented in those sources

  Among other things, note whether the project will have a broad impact, involve significant amounts of personal information about any individuals, or involve sensitive information.

- **Legal authority:** Identify the legal authority for the project and for collecting, using, and disclosing personal information. Include references to:
  - enabling legislation for the project
  - applicable privacy legislation, for example, FIPPA or MFIPPA
  - related agreements with partners, agents, and other third parties
- **Privacy roles and responsibilities:** Identify the individuals and parties (internal and external to your institution) responsible for protecting privacy. Explain their roles and responsibilities.

- **Access roles and responsibilities:** Identify the position titles of those who will have access to the personal information, including all officers, employees, consultants or agents of the institution.
- **Limitations:** Identify any limitations or restrictions imposed on the collection, use or disclosure of personal information.
- **Retention period:** Explain the period of time that the personal information would be retained by the institution.
- **Interested parties:** Identify relevant partners and interested parties and their importance to your privacy analysis. Indicate any conducted or planned consultation, the purpose, and the results.
- **Administrative, technical, and physical safeguards, practices, and measures:** Explain all safeguards and practices that would be used to protect personal information from theft, loss or unauthorized use or disclosure.
- **Risks to individuals:** Identify and summarize any risks to individuals in the event of a theft, loss, or unauthorized use or disclosure of the personal information.

Business processes and information flows

You should explain relevant businesses processes, both existing and planned, including:

- changes to existing processes
- the key roles and responsibilities
- the use of technology related to those business processes

Identify who does what, as well as why, when, where, and how they do it.

Describe how personal information will flow through the business processes and technology. Describe how personal information will be collected, used, retained, disclosed, secured, and disposed of, including changes to:

- existing information flows
- amounts or types of personal information involved
- who will have access to the personal information and be responsible for it throughout its lifecycle

Use plain language and organize this information in a way that makes sense for the project. For example, a complex project may require a broad overview as well as more detailed descriptions of its component parts.

Privacy analysis

Explain the results of your completed privacy analysis, including:

- your findings
- the privacy impact and risk(s) related to each finding
- your recommendations on what needs to be done to protect privacy and comply with FIPPA or MFIPPA
- your risk prevention and mitigation steps to:
    - prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and
    - mitigate the risks to individuals in the event of such an occurrence
- priorities and proposed timelines and responsibility for implementation

From this section, the reviewers and decision-makers should have a clear understanding of:

- the legal authority for the project (legislative and other instruments)
- the project's privacy risks
- the work that needs to be undertaken by the institution to protect privacy to comply with applicable privacy legislation
- outstanding, remaining, or unmitigated privacy risks and other issues impacting privacy and how they will be addressed

Conclusions

Include any final remarks relevant to your PIA. For example, indicate whether the purpose of your analysis was successfully achieved or if outstanding privacy work must be completed, etc.

Note key characteristics of the project including, but not limited to, whether it:

- could enhance privacy protection and compliance with privacy requirements
- could be designed to avoid, eliminate, or reduce some or all of the identified privacy risks
- could result in an unjustified invasion of privacy
- will involve new technology, business rules, or processes for which the privacy risks are not known or well documented

Next steps

Highlight any required follow-up to your privacy analysis, such as the timing and priorities for implementing your risk prevention and mitigation steps, or requirements to update the PIA in the future.

Determine and document where your organization will maintain the final approved PIA report. Ensure that this location is known and accessible within the institution (for example, in a centralized PIA repository maintained by the privacy office), so that it may be easily retrieved for review, updating, and providing to the IPC if required.

Approval

The project lead and other relevant decision-makers should approve the PIA report and acknowledge, in writing, that they understand the findings and recommendations, and authorize implementation of the risk prevention and mitigation steps/action items, or acceptance of the privacy risks. This includes documenting in the PIA report the steps to be taken:

i. to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and

ii. to mitigate the risks to individuals in the event of such an occurrence.

Attachments

Attach relevant documentation to support the findings and recommendations in this report. Examples of possible attachments include, but are not limited to:

- explanation of FIPPA and MFIPPA provisions (e.g., custody and control)
- list of documents reviewed and interviews conducted
- copies of cited forms
- completed PIA documents, including:
    - preliminary analysis
    - project analysis
        - business process diagrams
        - roles and responsibilities chart
        - information flow diagrams
    - privacy analysis checklist
- summary of recommendations and action items

Appendix E: Additional resources

Ontario privacy legislation, regulations, and other guidance

The *Freedom of Information and Protection of Privacy Act* (FIPPA)

- ***The Freedom of Information and Protection of Privacy Act***
- **Disposal of Personal Information – R.R.O. 1990, Reg. 459**
- **General – R.R.O. 1990, Reg. 460**

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)

- ***The Municipal Freedom of Information and Protection of Privacy Act***
- **General – R.R.O. 1990, Reg. 823**
- **Institutions – R.R.O. Reg. 372/91**

Other IPC guidance

- ***Privacy and Access in Public Sector Contracting with Third Party Service Providers***
- ***De-identification Guidelines for Structured Data***
- ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act***

PIA guidance from other sources and jurisdictions

- Government of Ontario, ***Freedom of Information and Protection of Privacy Manual***
- Government of Ontario Recordkeeping, Access and Privacy Advisory Services at 416-327-1600 or **access.privacy@ontario.ca**
- United Kingdom Information Commissioner's Office, **Data protection impact assessments** (2023)
- Office of the Australian Information Commissioner, **Guide to Undertaking PIAs** (2021)
- United States Department of Justice, **Impact Assessment Guidance**

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The Information and Privacy Commissioner of Ontario oversees compliance with several laws, which protect the access and privacy rights of Ontarians. These laws include:

- ***Freedom of Information and Protection of Privacy Act*** **(FIPPA)**
- ***Municipal Freedom of Information and Protection of Privacy Act*** **(MFIPPA)**
- ***Personal Health Information Protection Act*** **(PHIPA)**
- **Part X of the *Child, Youth and Family Services Act* (CFYSA)**
- ***Anti-Racism Act***

The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under these acts, the commissioner:

- **resolves access to information appeals**
- **investigates privacy complaints**
- **provides comment on proposed government legislation and programs**
- **reviews organizations' privacy policies and information management practices**
- **conducts research into access and privacy issues**
- **educates the public, media and other interested parties about Ontario's access and privacy laws and current issues affecting access and privacy**

Planning for Success:
Privacy Impact Assessment Guide for Ontario's Public Institutions

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Bloor Street East,
Suite 1400
Toronto, Ontario
Canada M4W 1A8

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

August 2026