Planning for Success: Privacy Impact Assessment Guide

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Acknowledgement

This guide is partially based on the Privacy Impact Assessment Guides and Tools developed by the Ministry of Government and Consumer Service (MGCS). The IPC commends the MGCS for its exemplary work in the area of privacy impact assessments. For more information about its tools and resources, contact the Information, Privacy, and Archives Division, MGCS, at 416-212-7061 or **Web.foi.mgcs@ontario.ca**.

CONTENTS

INTRODUCTION

This guide will help institutions subject to Ontario's *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and/or the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) conduct a privacy impact assessment (PIA) to assess compliance with the legislation.[1] Compliance is an essential foundation to protecting the right of privacy defined in the legislation.

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 your internal policies and protocols.[2] The guide can also serve as a starting point for your institution to develop its own PIA methodology. To address the needs of the project under consideration by your institution, you may need to alter or supplement the defined PIA process and analysis.

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 an 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 ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*** provides information on how to conduct a PIA involving personal health information.

[2] For example, Government of Ontario ministries and agencies must follow the *Corporate Policy on the Protection of Personal Information*, which defines PIA requirements and the need to consult with the Information, Privacy and Archives Division, MGCS, in defined circumstances. See Appendix E for links to the Ontario Public Service and other PIA resources.

BACKGROUND

WHY CONDUCT A PIA?

A PIA is a risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology, program, process or other activity may have on an individual's privacy. By completing a PIA, you will be able to guide your institution through a process that will identify the privacy impact and the means to address them. Privacy risks or impacts fall into two broad categories:

- **Risks to individuals**, including identity theft and other forms of fraud, adverse impact on employment or business opportunities, damage to reputation, embarrassment, distress or financial impacts.
- **Risks to institutions**, including the financial, legal and reputational impact of privacy breaches and the consequences of the failure 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 resulting documentation, will depend on the complexity of the project. Adapt the process to suit the needs of the project and your institution.

The benefits of conducting a PIA may include:

- The confirmation of the legal authority for the project to collect, use, retain and disclose personal information.
- The ability to demonstrate due diligence and evidence of compliance needed 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 Information and Privacy Commissioner of Ontario.
- The reassurance of individuals, other institutions, partners and your own management that best practices are being followed. PIAs may help promote better decision-making and a culture of privacy within an institution.
- The improvement of institutional transparency and better individual awareness, understanding and trust of your institution's information management practices.

- The improvement of operational efficiencies, especially when undertaken early and systematically. It can help minimize excessive and unnecessary collection, use, retention and disclosure of personal information, avoid costly design mistakes and retrofits, and perhaps identify simpler and less costly solutions at the start.

FIPPA and *MFIPPA* do not require that institutions complete a PIA. However, 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 technological tools used by institutions today.

WHEN TO CONDUCT A PIA

To be effective, PIAs should be started early in project development or design. Privacy protection must not be an afterthought. If the project involves personal information, you should consider privacy 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 needs to decide who will co-ordinate and carry out the PIA. Some institutions will have staff who are well-placed to conduct a PIA. Depending on the complexity of the project and the availability of staff with the necessary 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 and determine how the project should proceed to address identified privacy risks.

In most cases, an effective PIA will require consultation with and the involvement of 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, but the following overview may be a helpful orientation and reference.

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

- Collect specific information about the project, the key players and stakeholders and the type of and manner in which 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 benefits.

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. If it will not, you do not need to proceed further with the PIA process. However, you should document your conclusion and how you arrived at it in the project files. 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 quickly 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 *FIPPA* and *MFIPPA* defines personal information as ***recorded information about an identifiable individual*** (that is, a natural person). This 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.) and
- personal opinions and views.

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 in the context of the information

When determining if the project involves personal information, consider the context of the information to determine if it qualifies as personal information.

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.

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 the type of 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.;

- information that is not recorded, for example, collected orally;[3]
- whether previously separate information will be linked. Linking information can increase the potential of being able 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;[4]
- whether third parties, that is, parties outside of your program area or institution will be able to collect, use, disclose, retain, secure or dispose of any personal information;[5] and
- whether the project will involve personal information that is maintained for the purpose of creating a record that is available to the general public,[6] or excluded 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:

- an explanation of the project's purpose, scope and key objectives,
- an understanding of the information involved in the project, and whether or a 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 and
- a statement about whether you will need to proceed with the PIA, and reasons.

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 not, completion of the preliminary analysis confirms that no privacy

[3] While the definition of personal information in section 2(1) states that it includes recorded information about an individual, sections 38(1) of *FIPPA* and 28(1) of *MFIPPA* state that for the purposes of sections 38/28 and 39/29, personal information includes information that is not recorded.

[4] 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.

[5] While convenient and efficient, and oftentimes cost effective, the use of third parties can raise privacy concerns that must be addressed in your PIA.

[6] 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*.)

impact needs to be addressed and demonstrates that you have considered the privacy implications of the project.

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 analysis 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 step of the PIA process. It extends and deepens the information gathering activities begun in the preliminary analysis (Step 1) and involves the compilation of information needed to carry out a detailed privacy analysis (Step 3).

In this step you will need to define the details of the project so you will be able to identify its potential impact on privacy. Specifically, 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 third parties, that is, who will be doing what, when, how and why with the information and
- the technology involved with the project.

HELPFUL RESOURCE

Appendix B is a project analysis questionnaire that will prompt you to define and document the project.

ASSEMBLE 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 processes, roles and responsibilities, and required resources,
- **Information Technology:** relevant technology policies, practices and standards,

- **Security:** relevant physical, technical and procedural security safeguards and requirements,
- **Information Management:** relevant policies, practices and standards,
- **Legal:** applicable privacy legislation, enabling legislation, bylaws and other legal requirements, service level agreements, memoranda of understanding, contracts, etc.,
- **Procurement:** acquired or outsourced product and service solutions,
- **Risk Assessment:** risk assessment methodology,
- **Privacy:** issues, policies, practices, principles and applicable legislation,
- **Front End-Users of Information:** staff and other parties who will use the systems or information collected or created by the project with expertise on practical implications.

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

Adopting a team approach to assessing the project's privacy impact can be beneficial. Facilitated group discussions with the various areas impacted by the project may help you complete the PIA steps to identify and mitigate risks.

DEFINE SCOPE

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

The PIA's scope may not necessarily follow the scope of the project. For example, you need to determine whether:

- the privacy risks and impact apply to all aspects of the project or to only some parts of the project,
- your PIA will cover all associated business processes and technology. If the project will be using pre-existing technologies or processes in the same way as they have been used before, and which have already been analyzed to assess the privacy impact, you may not need to include them in your PIA,
- your PIA will only cover a specific change to an existing program, process or system, and does not need to consider the program, process or system overall and

- another area will be handling the analysis of parts of a joint project, and you only need to focus on one aspect of the project.

HELPFUL RESOURCE

Section 1 of the Project Analysis Questionnaire (Appendix B) can help you document the scope of your PIA.

ASSEMBLE RELEVANT BACKGROUND INFORMATION

Gather all project-related documentation, including information about business processes, workflow, information flows and business rules. Use existing documents to the greatest extent possible. Critical information may 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, third parties and stakeholders on existing and proposed activities relevant to the project.

DEFINE RELEVANT BUSINESS PROCESSES

Business processes refer to the various activities that will be completed during the course of the project following implementation, for example, what the program, system, application or process will involve. 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 the project will impact it (e.g., create a new application),

- 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 and
- if 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.

HELPFUL RESOURCE

Section 3 of the Project Analysis Questionnaire (Appendix B) can help you identify and document your business processes. Make sure you attach all relevant documentation to your completed questionnaire.

DEFINE SUPPORTING TECHNOLOGY

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

- How will the technology used or developed enable or support each step in the business process? Remember to include existing systems, technologies and applications that the project will be using.
- 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?

HELPFUL RESOURCE

Section 4 of the Project Analysis Questionnaire (Appendix B) can help you identify technology relevant to the project and document the answers to the above questions.

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 those who may handle 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 involved:

- the public,
- clients,
- staff in other programs or institutions,
- information technology staff (e.g., a system administrator),
- external legal counsel,
- other governments,
- partners and vendors,
- auditors and
- law enforcement agencies.

HELPFUL RESOURCE

Section 5 of the Project Analysis Questionnaire (Appendix B) can help you identify and document the roles and responsibilities of all parties involved in the project.

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 types of records involved in each of the project's business processes (existing and proposed, paper and electronic),
- describe the groups or types of information that will be collected, accessed, used, retained, disclosed, secured or disposed of in each business process or activity and

- identify any sensitive personal information associated with the business processes, such as medical information, criminal history, etc.

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

HELPFUL RESOURCE

Section 6 of the Project Analysis Questionnaire (Appendix B) can help you document your answers to the above considerations. Attach to your completed questionnaire any supplemental documentation describing information relevant to the project.

DOCUMENT PERSONAL INFORMATION FLOWS

Once you have defined the business processes, supporting technology and information, identify the personal information involved and determine how it will flow through the business processes and technology. If the project will change an existing program or system, determine whether it will alter the current flow of personal information.

Map the flow of personal information in all formats, from creation or collection, until final disposition, for example, secure destruction or transfer to appropriate archives. This vital step will be the basis of your privacy analysis in the next step. 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. Descriptive information flow tables may be organized by some, or all, of the following categories:

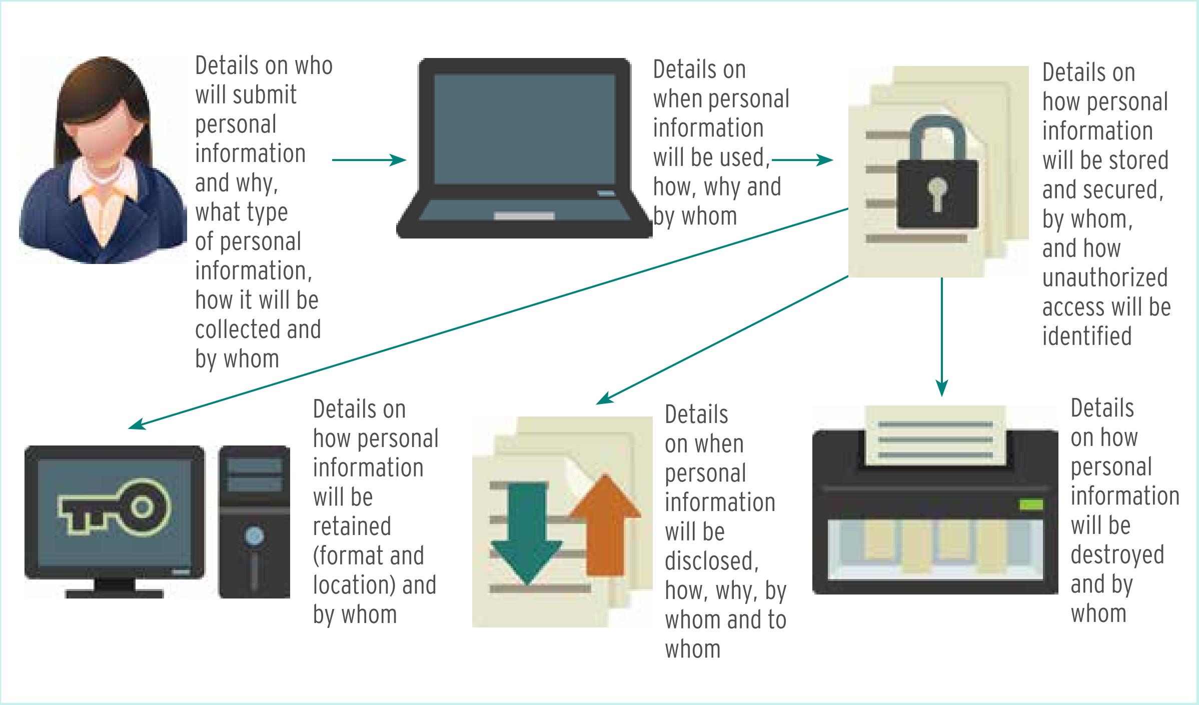
- personal information,
- source of information,
- collected by,
- collection method,
- purpose of collection,
- format of the information,
- purpose of use,
- used by,

- security control during information transfer,
- information repository format,
- storage retention site,
- purpose of disclosure,
- disclosed to,
- retention policy and
- disposal or destruction policy.

For example:

PERSONAL INFORMATION	COLLECTED by? from? how? when? where? why? authority?	USED by? how? when? where? why? authority?	RETAINED by? how? how long? where? why?	SECURED by? how? when? where? why?	DISCLOSED by? to? how? when? where? why? authority?	DISPOSED OF by? how? when? where? why? authority?

Alternatively, information flow diagrams may be visual, such as the diagram illustration below:



Details on who will submit personal information and why, what type of personal information, how it will be collected and by whom
Details on when personal information will be used, how, why and by whom
Details on how personal information will be stored and secured, by whom, and how unauthorized access will be identified
Details on how personal information will be retained (format and location) and by whom
Details on when personal information will be disclosed, how, why, by whom and to whom
Details on how personal information will be destroyed and by whom

Upon completion, your project analysis documentation should show:

- How personal information will be collected, used, disclosed, retained, secured, and disposed of, including who is responsible and how technology will be used for each of these activities.
- Who will have access to personal information throughout its lifecycle, for what purposes and with what privileges. For example, who will process, browse or modify personal information including program and IT staff, other programs providing services relevant to the project, and your partners and third parties.
- How personal information will flow through existing and planned programs, systems or processes during each associated business process.
- How and when personal information will move beyond the custody of the institution, that is, in the custody of a third party.

HELPFUL RESOURCE

Section 7 of the Project Analysis Questionnaire (Appendix B) can help you document how personal information will flow through the project.

3. PRIVACY ANALYSIS

This step involves a detailed examination of the privacy risks arising from the project and the identification of solutions to be implemented to address them.

To be effective, this step should be informed by complete and accurate information about the project, as you will have developed through your project analysis, as well as by relevant privacy laws, regulations and other compliance requirements. In addition, your institution's practices related to privacy, information management, technology, security and risk management may 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 impact 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

A privacy impact is anything that could jeopardize or negatively impact an individual's privacy. For example, unauthorized collection, access, use, retention or disclosure of personal information can create a privacy impact, including identity theft and other forms of fraud, physical safety issues, such as stalking or harassment, financial loss, adverse impact 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 image 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*.

A privacy impact or risk can arise in a number of circumstances, including:

- failure to have the appropriate legal authority to collect, use or disclose personal information,
- use of inaccurate, insufficient or out-of-date information,
- use or disclosure of personal information when it is not needed (for example, where aggregate or de-identified information is sufficient to achieve the purpose or business objective),
- use of irrelevant personal information,
- use of personal information in ways that are not authorized,
- retention of personal information for longer than necessary,
- disclosure of personal information to individuals or institutions when not authorized,
- failure to keep information appropriately secure or
- failure to grant individuals the right to access or correct their own information.

IDENTIFY GAPS AND POTENTIAL PRIVACY IMPACT

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

The checklist will prompt you to examine the project to determine if it will comply with each of the identified privacy requirements. Consider existing privacy protection measures and planned actions that may apply to the identified requirements. Determine if these will address the requirement. 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.

ANALYZE FINDINGS

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

- **Objective:** Starting your analysis with the assumption that your desired outcome is to protect privacy to the greatest extent possible and to comply with *FIPPA* or *MFIPPA*.
- **Rationale for Involvement of Personal Information:** Applying the concept of data minimization and determining if there is a way to implement the project without collecting, using, retaining or disclosing personal information, or with less personal information involved.
- **Privacy Impact:** Considering the potential harm associated with each compliance gap and identifying the privacy risks or impact, if you are unable to mitigate or avoid them. In addition to possible non-compliance, think about the privacy impact on affected individuals and your institution:
    - What the affected individuals likely would think the impact would be, that is, try to put yourself "in the shoes" of the affected individual when assessing harm.

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 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 if it is necessary to achieving the purpose or business objective. Limiting the amount of personal information you collect, use, retain and disclose will prevent an unnecessary privacy impact.

- o The impact on privacy broadly, not just those risks related to the management of personal information, for example, mandatory drug testing or visits to an individual’s home.
- o The scale of impact or size of the population affected, that is, mismanagement of even a small amount of personal information for each Ontarian could have a large impact.
- o The impact on your institution’s reputation if non-compliance was known, as well as implications on operations including costs to address the privacy impact after the project is implemented.

Understanding the privacy consequences or implications of your findings is a central part of your privacy analysis. This analysis 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 to minimize its impact on privacy. Consult with your institution’s privacy and legal experts if guidance is needed.

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:

- deciding not to collect, use or disclose particular types of personal information,
- creating retention periods that only keep information for as long as necessary and planning the secure disposal of information,
- implementing appropriate technological, procedural and physical security measures,
- ensuring that staff are properly trained and are aware of the potential privacy impact and appropriate privacy-protective measures to be followed,
- developing ways to safely anonymize and/or de-identify the information, where possible,
- 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,

- 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, create a complete notice of collection and make sure it is accessible to the project's clients,
- selecting third parties that will provide a greater degree of security and ensuring that agreements are in place to protect the personal information in the custody of the third parties and
- producing information sharing agreements that clarify what information will be shared, how it will be shared and with whom it will be shared.[7]

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

Your analysis of the effectiveness of each option will allow you to select the solutions that you believe will be most beneficial to 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. If the project is already compliant, indicate that no further action is required.

The action items that you identify are the "to do" list of items necessary to enable the project to protect privacy and comply with *FIPPA* and *MFIPPA*. This will be the mitigation strategy needed to minimize the project's privacy impact and should inform relevant staff as they proceed through the project.

HELPFUL RESOURCE

Use the Privacy Analysis Checklist (Appendix C) to document the action items related to each impact.

[7] An information sharing agreement will clarify the rights and obligations of all parties involved and ensure compliance with *FIPPA* or *MFIPPA*. The IPC has guidance on a **Model Data Sharing Agreement**.

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.

A 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 demonstrates privacy due diligence.
- It documents the results of your preliminary analysis, project analysis and privacy analysis. This is an important information management function because your findings, analysis and recommendations may be needed for future reference.

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.

Write your report so it can be readily understood by a non-technical audience, that is, not privacy, legal, technology or security experts. You should ensure there is sufficient detail and explanations, so that someone outside the project can understand how you came to your conclusions and recommendations.

OBTAIN APPROVAL

Appropriate approvals should be obtained to implement your recommended privacy risk mitigation strategy.

Approval of your PIA Report should be contingent on:

- the project's impact on privacy being fully and properly assessed,
- the decision-makers' understanding of the privacy risks and impact,
- the appropriate decision-makers' approving:
  - the mitigation strategy to address the identified privacy impact or
  - the acceptance of the privacy risks, that is, a decision to take no action to address, and being aware of the consequences of such action and

- all of the project's identified privacy gaps and impact having been appropriately addressed or accepted.

Once the action items to address identified privacy risks are approved, update your PIA report and project plan, if necessary. 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.

UPDATE YOUR FINDINGS AND PRIVACY ANALYSIS, AS REQUIRED

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

This ongoing assessment is an essential part of identifying and mitigating new issues and changes impacting privacy 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, that is, business process, information flows, roles and responsibilities, to ensure that new privacy risks have not been created by these changes,
- evaluate mitigation measures to determine if they are effective when implemented; update or revise, if necessary,
- identify and assess new, outstanding and remaining privacy gaps and impact, and identify new action items required to address privacy risks,
- 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 and
- update or supplement your PIA documentation, as required, ensuring you document:
    - the new privacy risks and impact and how they arose,
    - their likelihood, harm and priority for action and
    - your mitigation strategy 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.

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 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. Changes to scope, business owner, legislative or regulatory authority, business processes, partners or third party service providers, technology, functionality, service delivery model, security and information requirements may create new privacy risks and trigger the need to update your privacy analysis and mitigation strategy.

When changes or developments occur that impact the project, your institution may need to revisit your PIA. It should document the analysis and approval in a manner that works for the project and institution. For example, your institution may decide to prepare an addendum to your PIA report.

CONCLUDING THE PIA PROCESS

Before you conclude your PIA process:

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

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, that is, 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, anonymized or de-identified information. Outline in the row below the process followed to aggregate, anonymize or de-identify the information and whether it is possible 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.)						
List the types of personal information involved in the project and indicate in the columns on the right whether this personal information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.) If third parties will be involved in the project, think about what they may be doing with personal information as well. (Add rows as necessary.)						

	COLLECT	USE	RETAIN	DISCLOSE	SECURE	DISPOSE
List each element of non-personal information that, when combined or linked, may enable identification of an individual, and indicate in the columns on the right whether that information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.)						

4.3 To whom does the personal information relate? List all the individuals whose personal information will be involved in the project, that is, the data subjects.

5. PRIVACY LEGISLATION

5.1 Identify applicable privacy legislation (check all that apply).[8]

	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.)			

[8] See the **Privacy Impact Assessment Guidelines for the Ontario *Personal Health Information Protection Act*** on how to conduct a PIA involving personal health information.

5.2 Public Records and Excluded Personal Information[9]

	YES	NO	UNKNOWN
Identify 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 row below.)			
Identify 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.)			

6. CONCLUSION

Indicate whether or not you will proceed with the PIA process and the reasons for your decision.

[9] 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.

APPENDIX B: PROJECT ANALYSIS QUESTIONNAIRE

1. SCOPE OF PIA

Define the scope of the PIA review and analysis, that is, 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 understandings, agreements, contracts and other relevant instruments).

3. PROJECT CHARACTERISTICS

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

	YES	NO	UNKNOWN
Involves creating a new program, process, service, technology, information system or other type of IT application			
Involves a change to an existing program, process, service, technology, information system or other type of IT application			
Involves procuring goods or services			
Involves outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information			

	YES	NO	UNKNOWN
Involves developing a request for bids, proposals or services			
Involves a process, system or technology for which the privacy risks are not known or well documented			
Involves creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases			
Involves information sharing (internal and external)			
Involves the need to identify, authenticate or authorize users – 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).

	YES	NO	UNKNOWN
Involves a change in business owner			
Involves a change to legislative authority			
Involves a change in users (internal and external) of a related process or system			
Involves a change in partners or service providers (internal and external)			
Involves a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of			
Involves a change to the purposes for which personal information will be collected, used or disclosed			
Involves a change from direct to indirect collection of personal information			

	YES	NO	UNKNOWN
Involves a change in roles and responsibilities, that is, who can do what, when, where, why and how with personal information			
Involves a change to, or elimination of, existing practices of anonymizing or de-identifying information			
Involves a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information, for example, hardware and software			
Involves a change to an information system or database containing personal information			
Involves a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records or the, creation of a new website to provide services to clients			
Involves a change in the security requirements or measures			
Other (Please specify change or proposed change below.)			

3.4 **If you answered yes to any of the above,** explain the change, that is, 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)**.**

	YES	NO	UNKNOWN
Involves technology designed to monitor, track or observe an individual or their transactions, for example, video cameras, cell phones and geospatial or location-based services			
Involves 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			
Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media			
Involves using analytics or performance measurements, for example, web analytics, social media analytics, or business intelligence tools			
Involves processing or storing of personal information in a virtual environment, for example, cloud computing			
Involves acquiring, or customizing, commercial software, hardware or IT support services by external vendors			
Involves developing, or customizing, software, hardware or IT support services "in-house"			
Involves creating information systems or other types of IT applications that will be populated by others, for example, clients of system or service will supply information			
Involves 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 other parties that will have access to, or use, the personal information, for example, other program areas, IT staff, legal counsel, etc.

PARTY	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

7.1 **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 definition of personal information flow 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 your own purposes and needs. Adapt to meet the needs of the project and your institution, while ensuring you address all the identified questions. Consider each instance of how personal information is involved when completing the checklist. For example, when asked about authority to collect, consider all types of personal information you will collect.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y[10]	N[11]	IP[12]	NA[13]	EXPLANATION		
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 how the project will comply 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 on privacy, for example, 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) necessary for compliance with the privacy requirement or to mitigate or avoid a potential privacy impact.

[10] **Y (Yes):** You know the privacy protection requirement either has been met by existing measures or will be met by action planned before implementation

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

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

[13] **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:

- 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?
- Personal information should be collected directly from the individual to whom it relates, unless another manner of collection is authorized by the individual or statute.
- Notify the individual of the collection, including legal authority, purpose(s), and contact information of a person who can answer questions about the collection.
- See sections 28 and 29 of *MFIPPA* and sections 38 and 39 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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?							
Has responsibility for the collection been assigned to program staff or third party service providers?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
PURPOSE OF COLLECTION							
Has the purpose of the collection been defined? What is the purpose of the collection?							
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 missing components.							
MANNER OF COLLECTION/SOURCE OF PERSONAL INFORMATION							
Will personal information be collected directly from the individual? Explain the form of collection (for example, orally, hardcopy form, online portal, etc.)							
Will personal information be collected indirectly from another source, or covertly? Why?							
Will indirect collection comply with *FIPPA* or *MFIPPA*? Explain authority for indirect collection.							
CONTROLS							
Will the project only collect personal information for which there is legal authority?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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, for example, your institution, partners and other third parties, use personal information only with the authority to do so.
  - ○ Is the use for the purpose it was collected or for a consistent purpose?[14]
  - ○ 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 *M/FIPPA*?
- See section 31 of *MFIPPA* and section 41 of *FIPPA*.

[14] A consistent purpose is a use 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					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Do all parties using personal information have the legal authority for the use(s)?							
PURPOSE(S) OF USE							
Has the purpose of the use been defined? Explain 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, for example, program staff, consultants, agents, third party service providers, etc.?							
CONTROLS							
Will there be procedural, technical, and physical measures in place to ensure personal information will be used only for authorized purposes and by authorized parties? Explain measures.							
Will there be periodic reviews of the use controls 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, for example, your institution, partners and other third parties, 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?[15]
  - ○ 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 *M/FIPPA*?
- See section 32 of *MFIPPA* and 42 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Do all parties disclosing personal information have the legal authority for the disclosures?							
PURPOSE(S) OF DISCLOSURE							
Has the purpose of the disclosure been defined? Explain purpose(s).							
Will personal information be disclosed for other purposes?							

[15] 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.

	FINDINGS						
PRIVACY REQUIREMENT QUESTIONS	Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
Will disclosures of personal information be for purposes stated in the notice of collection or for a consistent purpose?							
MANNER OF DISCLOSURE							
Have all parties disclosing personal information been defined, for example, program staff, consultants, agents, third party service providers, etc.?							
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?							
CONTROLS							
Will there be controls in place to ensure personal information will be disclosed for authorized purposes, by and to authorized parties? Explain controls.							
Will there be periodic reviews of the disclosure controls to ensure effectiveness?							
DATA MINIMIZATION							
Is disclosure of all the personal information necessary for the project to proceed?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
DISCLOSURE FOR RESEARCH PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for research purposes?[16]							
DISCLOSURE FOR FUNDRAISING PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for fundraising purposes?[17]							

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 is able to:
  - correct their personal information,
  - have a statement of disagreement attached to the personal information if the correction is not made and
  - 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*.

[16] 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, and agrees to the terms and conditions of Ontario Regulations 460 and 823, section 10.

[17] *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.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
STANDARD OF ACCURACY							
Will there be measures in place to make sure personal information is not used, unless it is accurate, complete and up-to-date? Provide details of measures.							
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 process.							
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 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.
- Take all reasonable 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 of *MFIPPA* and Ontario Regulation 460, sections 3 and 4 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
SECURITY MEASURES							
Will measures be used to secure the personal information? Explain each physical, technical and procedural measure.							
CONTROLS							
Will security policies and procedures 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?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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 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					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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* section 30(1) and Ontario Regulation 823, section 5; *FIPPA* section 40(1) and Ontario Regulation 460, section 5.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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 measures be in place to ensure that personal information will be retained for a minimum of one year after its last use?							
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?							
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 regulations/bylaws applicable to the institution.
- Take all reasonable steps 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 steps 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 steps 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) of *MFIPPA*, section 3 of *MFIPPA* and Ontario Regulation 459 and section 40(4) of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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, regulations/bylaws? Explain disposal process.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
DEVICES/EQUIPMENT							
Will procedures be defined and documented for disposal of devices and equipment containing personal information?							
CONTROLS							
Will controls 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 controls to ensure effectiveness?							
RECORD–KEEPING							
Will details of the disposal of personal information be recorded?							
Will 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:

- You should apply common management principles, for example, 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 privacy policies and practices, and commit to ongoing improvement in compliance.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	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, partners, vendors and other third parties? Explain accountability.							
TRAINING							
Will operational policies, procedures or practices 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 procedures and protocols 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*?							

APPENDIX D: PIA REPORT TEMPLATE

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 and
- 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 and
- 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 and
- project partners and stakeholders.

PRIVACY

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

- **Personal Information:** Briefly describe the type of personal information involved in the project and the individuals to whom it relates. Note whether the project will have a broad impact, involve significant amounts of personal information about any individuals, or 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*, and 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.
- **Stakeholders:** Identify relevant stakeholders and their importance to your Privacy Analysis. Indicate any consultation conducted or planned, the purpose and results.

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 and the use of technology related to those business processes. Identify who does what and 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 and 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 need to provide an overview, as well as detailed descriptions of component parts.

PRIVACY ANALYSIS

Explain the results of your completed privacy analysis, including:

- your findings,
- the privacy impact related to each finding,
- your recommendations on what needs to be done to protect privacy and comply with *FIPPA* or *MFIPPA* and
- priorities and proposed timelines and responsibility for implementation.

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

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

CONCLUSIONS

Include any final remarks relevant to your PIA. For example, indicate whether the purpose of your analysis was successfully achieved or 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/all of the identified privacy risks,
- could result in an unjustified invasion of privacy or
- 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 mitigation strategy.

APPROVAL

The project lead and other relevant decision-makers should approve the PIA Report acknowledging, in writing, that they understand the findings and recommendations, and authorize implementation of the mitigation strategy/action items or acceptance of the privacy risks.

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 and
        - information flow diagrams.
    - Privacy Analysis Checklist and
- 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*

- **A Mini Guide to Ontario's *Freedom of Information and Protection of Privacy Act***
- **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*

- **A Mini Guide to Ontario's *Municipal Freedom of Information and Protection of Privacy Act***
- **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

- **Model Data Sharing Agreement (1995)**

OTHER PIA GUIDANCE

- IPC, **Privacy Impact Assessment Guidelines for the Ontario *Personal Health Information Protection Act*** (2005)
- Ministry of Government and Consumer Services, PIA Guides and Tools, contact the Information, Privacy, and Archives Division at 416-212-7061 or **Web.foi.mgcs@ontario.ca**
- Office of the Privacy Commissioner of Canada, **Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada** (2011)

- Treasury Board Secretariat of Canada, **Directive on Privacy Impact Assessments** (2010) and **Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks Guidelines** (Archived)
- United Kingdom Information Commissioner's Office, **Conducting privacy impact assessments code of practice** (2014) and **Privacy impact assessment and risk management** (2013)
- Australia, **Guide to Undertaking PIAs** (2014)
- United States Department of Justice, **Impact Assessment Guidance**
- PIA Watch, **PIA Guidance Material**

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three *Acts*, the Commissioner:

- Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction.
- Investigates complaints with respect to personal information held by government or health care practitioners and organizations.
- Conducts research into access and privacy issues.
- Comments on proposed government legislation and programs.
- Educates the public about Ontario's access and privacy laws.

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

May 2015