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.)						
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).[1]

	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[2]

	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.			

[1] 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.

[2] 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?			
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)?			
WILL THE PROJECT INVOLVE...	YES	NO	UNKNOWN
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.

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

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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y[3]	N[4]	IP[5]	NA[6]	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 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.

[3] **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

[4] **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.

[5] **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.

[6] **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					PRIVACY IMPACT/RISK	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?							
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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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?[7]
    - 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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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)?							

[7] 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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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?[8]
    - 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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Do all parties disclosing personal information have the legal authority for the disclosures?							
Have you documented the legal authority for the intended disclosures?							

[8] 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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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?							
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?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
INFORMATION SHARING AGREEMENT							
Will disclosures be documented and controlled by information sharing agreements or other means?							
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					PRIVACY IMPACT/RISK	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?[9]							
DISCLOSURE FOR FUNDRAISING PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for fundraising purposes?[10]							

[9] 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.

[10] 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					PRIVACY IMPACT/RISK	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.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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					PRIVACY IMPACT/RISK	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 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					PRIVACY IMPACT/RISK	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 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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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					PRIVACY IMPACT/RISK	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, laws/ regulations/ bylaws? Explain the disposal process.							
DEVICES/EQUIPMENT							
Will procedures be defined and documented for disposal of devices and equipment containing personal information?							
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?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
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.[11]

[11] See PIA requirements in section 38 of FIPPA and section 28 of MFIPPA.

Privacy Impact Assessment Template

Initiative Information	
Initiative Name:	
Institution:	
Program / Service Area:	
Initiative Description:	

Assessment Information	
PIA Status	*Initial PIA / Updated PIA*
Related / Previous PIA, if applicable	
Prepared By:	
Reviewed By:	
Approved By:	
Date Approved:	
PIA Version:	

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.

Type of Personal Information	Intended Use(s)	Intended Disclosure(s)

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.

Position Title	Department / Business Area	Personal Information / Type Accessed	Reason Access Required	Access Limitations, if applicable

6. Any limitations or restrictions imposed on the collection, use or disclosure of the personal information.

Limitations on Collection

Limitations on Use

Limitations on Disclosure

7. The period of time that the personal information would be retained by the institution, in accordance with subsection 30 (1).

Record Containing Personal Information	Retention Period	Source of Retention Period	Disposition

8. An explanation of the administrative, technical and physical safeguards and practices that would be used to protect the personal information in accordance with subsection 30 (5) and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.

Administrative Safeguards

Technical Safeguards

Physical Safeguards

Risks to Individuals

9. 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 from occurring, and to mitigate the risks to individuals in the event of such an occurrence.

Risk Identified	Step to be Taken	How the Step Addresses the Risk	Implementation Timing

10. Such other information as may be prescribed.

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**