The Guide to Completing a

PRIVACY IMPACT ASSESSMENT

Under the *Access to Information and Protection of Privacy Act, 2015*

ATIPP Office
Department of Justice and Public Safety
June 2016

Table of Contents

Part A – Introduction to Privacy Impact Assessments

The *Guide to Completing a Privacy Impact Assessment* is designed to assist public bodies in the province of Newfoundland and Labrador when completing a privacy impact assessment (PIA). A PIA ensures practices, programs and services are compliant with the privacy provisions in the *Access to Information and Protection of Privacy Act, 2015 ("ATIPPA, 2015")*.

This guide refers to PIAs being completed for 'projects.' This term is intended to cover the full range of activities and initiatives, either current or proposed that may have privacy implications, including:

- Programs;
- Policy proposals;
- Current or proposed legislation, including amendments;
- Current or proposed programs, activities, systems or databases;
- Changes to how information is stored;
- a new or increased collection, use or disclosure of personal information, with or without the consent of individuals;
- a large expansion of the number of people covered under a project;
- a shift from direct to indirect collection of personal information;
- a new disclosure of personal information for a common or integrated program or service;
- new data matching or increased sharing of personal information between programs or across institutions, jurisdictions or sectors;
- development of or a new or extended use of common personal identifiers;
- significant changes to the business processes or systems that affect the separation of personal information or the security mechanisms used to manage and control access to personal information; or
- the contracting out or devolution of a program or service to another level of government or the private sector.

What is a Privacy Impact Assessment?

A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimizing or eliminating that impact. It is used to ensure privacy issues are fully considered at an early stage of project development, particularly when there are significant privacy risks, and requires a team which includes members who have significant privacy expertise, technical expertise and knowledge about the project.

Why is a PIA necessary?

ATIPPA, 2015 requires a preliminary privacy impact assessment or a full privacy impact assessment be completed during the development of a program or service by a department or branch of the executive government of the province. The results of the preliminary assessment or the PIA must be submitted to the Minister responsible for the Department of Justice and Public Safety – ATIPP Office for review and comment.

When completing the PIA, a public body will review how personal information will be collected, used, access and/or disclosed, which includes reviewing:

- The type of personal information being collected;
- How personal information will be collected (i.e. directly from the individual or another source);
- Whether personal information will be disclosed, and to who (e.g. another public body, third party business, etc.);
- The purpose for the collection, use, access or disclosure (e.g. to determine eligibility for a service, for product registration, etc.);
- The manner in which individuals provide consent; and
- Which security safeguards (e.g., log–in credentials, single sign–on, access controls) will be implemented to protect personal information.

If a Preliminary PIA (PPIA) is completed, is a PIA necessary?

While PPIAs are required for all new departmental projects, PIAs are not. In most circumstances, if your public body has completed a PPIA, a PIA will not be required. However, there may be circumstances where a complete PIA will be required - these circumstances will be reviewed below.

When is a Privacy Impact Assessment Needed?

While not all projects require a PIA, one must be completed when a PPIA indicates that it is necessary. This determination is made by the ATIPP Office when they review a PPIA submitted by a public body. However, public bodies are able to initiate a PIA for projects on their own if they determine one is necessary.

For some projects, it may be obvious at the outset that a PIA will be required. In those circumstances, it may be appropriate to proceed directly to a PIA.

Factors to be considered when determining whether a complete PIA is necessary include, but are not limited to:

1. Number of impacted clients;
2. Amount of personal information being collected;
3. Whether personal information will be collected directly from individuals;
4. Sensitivity of personal information being collected (e.g. SIN, health information, etc.);
5. How many employees will have access to the personal information;
6. Whether there are access controls in place to protect personal information;
7. If there are audit capabilities on the database where personal information will be stored (for electronic records);
8. Whether third parties will have access to the personal information;
9. Whether personal information will regularly be disclosed; and
10. If the project is for a common or integrated program or service.[1]

[1] *A "common or integrated program or service" refers to a single program or service that is provided or delivered by two or more public bodies. The program or service may have several distinct components, each of which is provided or delivered by a separate public body. These components together comprise the common program or integrated service. Each public body partner must be integral to the program or service. For example, a nursing practicum program*

In addition to the 10 factors listed above, the ATIPP Office will take into consideration the following results from a PPIA when determining whether a PIA is necessary:

1. Personal information is required in order to achieve the desired outcome of the project;
2. Compliance with *ATIPPA, 2015* has been taken into consideration;
3. Security safeguards will be implemented to ensure protection of personal information; and/or
4. Policies and procedures are in place, and disseminated to employees, to ensure compliance with the privacy provisions of *ATIPPA, 2015.*

If a PIA is needed, when during a project should it be completed?

A PIA should begin at the early stages of development or changing a project that collects, uses, accesses or discloses personal information. Starting a PIA early in a project's development is important to ensure that the results of the PIA (e.g. privacy risks, mitigation strategies, recommendations, etc.) can be incorporated into the project design to ensure compliance with the privacy provisions of *ATIPPA, 2015*. Although a PIA may be started early in a project's development, some projects with IT components may take longer to complete depending on whether certain elements have been identified or defined (e.g. technical or security controls). Sometimes this information is not known or defined until later in the project.

It is also important to ensure that once a PIA is completed, and its findings are incorporated into the project, it is periodically reviewed by the public body responsible for the project, in consultation with the ATIPP Office, to ensure that any recommendations or risk mitigation strategies are being followed and to

requires the participation of both the post-secondary institution, and the health care body; the program would not function without the services of each body. Public bodies may have clients in common, but that factor alone does not make a program or service common or integrated.

determine if any additional steps should be taken to ensure compliance with *ATIPPA, 2015.* In addition, if there are significant changes to the project (e.g. additional personal information is collected, information will be moved from an internal server to a third party server, etc.) after the PIA is completed, it may be necessary for another PPIA to be completed.

Who should be a part of the PIA Team?

If a PIA is to be completed, assembling the right team is essential. The team should include, but not be limited to a/an:

- Program Manager (team lead with the department/public body);
- IT representative (from OCIO for government departments) for projects with an electronic component (e.g. website, database, etc.);
- ATIPP Office representative – the Senior Privacy Analyst assigned to the public body;
- Solicitor (optional);

The Program Manager with the department/public body responsible for the project is expected to lead the completion of the PIA with support and input from any relevant individuals including the Senior Privacy Analyst from the ATIPP Office, the IT representative (if necessary), and the public body's solicitor.

Before the PIA is finalized, it must be reviewed by the following individuals:

- ATIPP Coordinator [Department/Public Body]
- IT Representative, OCIO [if projects have an electronic component]
- Information Management Director [Department/Public Body]

In addition to these team members, the PIA must have final sign-off from the following individuals upon completion:

- Head of public body (e.g. Deputy Minister, CEO, President, etc.);
- Program Manager (Team lead); and
- ATIPP Office representative

How to prepare for a PIA

Planning the PIA is an important step in the PIA process. You should consider the following:

- The privacy scope of the project;
- Who will be a part of the PIA team (see section above);
- The timeframe to complete the PIA (e.g. 1 month, 3 months, etc.);
- Other resources required to complete the PIA (e.g. whether other employees need to be consulted, whether the public or other stakeholders need to be consulted, etc.); and
- Steps that will need to be taken after the PIA, including implementation of recommendations and ongoing monitoring.

A project's privacy scope can increase depending on the risk of privacy impacts, for example, in circumstances where:

- The collection and/or storage of personal information will be outsourced;
- New legislation or new technology will be needed for handling or storing personal information;
- Personal information will be aggregated in databases;
- Personal information will be used for data-matching;
- Whether you are disclosing personal information and to whom it will be disclosed (e.g. public body, third party business, etc.);
- Providing personal information will be required;
- The type and sensitivity of personal information being collected, used, accessed or disclosed; and
- The size or complexity of the project.

Role of the ATIPP Office

As mentioned previously, *ATIPPA, 2015* requires a preliminary privacy impact assessment or a full privacy impact assessment be completed during the development of a program or service by a department or branch of the executive government of the province. The results of the preliminary assessment or the PIA must be submitted to the Minister responsible for the Department of Justice and Public Safety – ATIPP Office for review and comment.

Therefore, in addition to a Senior Privacy Analyst being a member of the PIA team, the ATIPP Office must also review the final PIA for assessment and provide any recommendations it deems appropriate. When recommendations are received from the ATIPP Office the public body must advise whether they accept the recommendations or not. At a predefined time (3 months, 6 months, etc.), the public body must follow-up with the ATIPP Office and advise on the progress of implementing any of the recommendations they agreed to.

The ATIPP Office is also available before it is determined that a PIA is necessary and can assist a public body in determining whether one is appropriate or required for a project.

Role of the Office of the Information and Privacy Commissioner (OIPC)

When a PIA is completed for a common or integrated program, *ATIPPA, 2015* requires that upon receipt, the Minister responsible for the Department of Justice and Public Safety – ATIPP Office, provide the OIPC with a copy for review and comment. Therefore, it is important to determine at an early stage in the development of a project, whether it is a common or integrated program (see footnote 1 of this document for definition).

Part B – Completing a Privacy Impact Assessment

This part of the guide will outline each section of the PIA template, providing additional guidance, definitions and instructions to maximize the accuracy and benefits of completing the PIA.

Executive Summary

The executive summary is meant to provide a high level overview of the project and should include the following information:

- Project description;
- Benefits of project;
- Why PIA was recommended (see PPIA);
- Privacy risks identified and mitigation strategies; and
- Final recommendations made to ensure compliance with *ATIPPA, 2015.*

1.0 Project Summary

The project summary section should review all aspects of the project at a level of detail in which an individual with no prior knowledge of the project would understand, including:

<u>Purpose of Project:</u>

- Why the project is being developed;
- What the project will entail (e.g. collecting date of birth to confirm identity, etc.);
- What procedures were in place prior to this project (e.g. confirming identity from name alone, etc.).

<u>Scope of Project:</u>

- a modification and/or upgrade of an existing project;
- a modification of business practices (e.g. forms will be emailed instead of faxed, etc.);
- a new project

Previous PPIA/PIA:

If the project is an upgrade or modification to a previously existing project, list whether a PIA or PPIA was completed before, and whether a privacy impact report (PIR) was provided by the ATIPP Office. If any of these were completed previously, indicate which one was completed and attach the relevant documents to the PIA.

Note – if the PIA is for a new project, answer "no – this is a new project."

Benefits of Project:

Outline what benefits will come from the project (e.g. providing additional services to the public, streamlining existing process, etc.). In addition, outline the benefits for clients of the project and why they outweigh the impact of collecting personal information.

Example of how to complete Project Description:

Purpose of Project:	*To provide online payment methods for clients of program A*	
Scope of Project:	*Is this project a new project or an upgrade or modification of existing project?*	*This is a new project*

Previous PPIA/PIA:	*Was a PPIA or PIA completed previously for this project?*	*N/A*
Benefits of the Project:	*This will allow additional methods for payments related to program A. It will cut down on human resources used to process payments manually, as well create a more accessible option for payment for users.*	

2.0 Information Flow Analysis

An information flow diagram and table are used to visualize how personal information that is collected for the project moves through the public body.

Personal Information Table:

For each individual type of personal information being collected (e.g. name, date of birth, etc.) the following information must be included:

Personal Information: The type of personal information being collected (e.g. name, date of birth, etc.). This section should be as detailed as possible. For example, rather than writing "name", write "first and last name", "first, middle and last name", etc.

Purpose: The purpose for collecting the personal information (e.g. reason the personal information is required for the project) must be included so the public body can demonstrate why it is necessary and how it relates to the objectives of the project.

Collected by: Indicate who will be collecting the information (e.g. public body, third party contractor, etc.). Be as detailed as possible; for example, if you know which positions within the public body are collecting the information, include their titles rather than simply stating that the public body is collecting the information.

Used by: Indicate who within the in the public body will use the information (e.g. division, position, etc.). Be as detailed as possible; for example, if you know which positions within the public body will use the personal information, include their titles rather than only stating which division/s will use it.

Disclosed to: If applicable, indicate who the information will be disclosed to outside of the public body. Be as detailed as possible; for example, if you know which public bodies, third parties or organizations the personal information will be disclosed to list each entity, rather than stating that it will be disclosed to another public body or an outside organization (e.g. "The Department of Justice and Public Safety" rather than "another public body", etc.).

Information Source: The source/s for the collection of the personal information must be indicated (e.g. client application, third party, public body database, etc.).

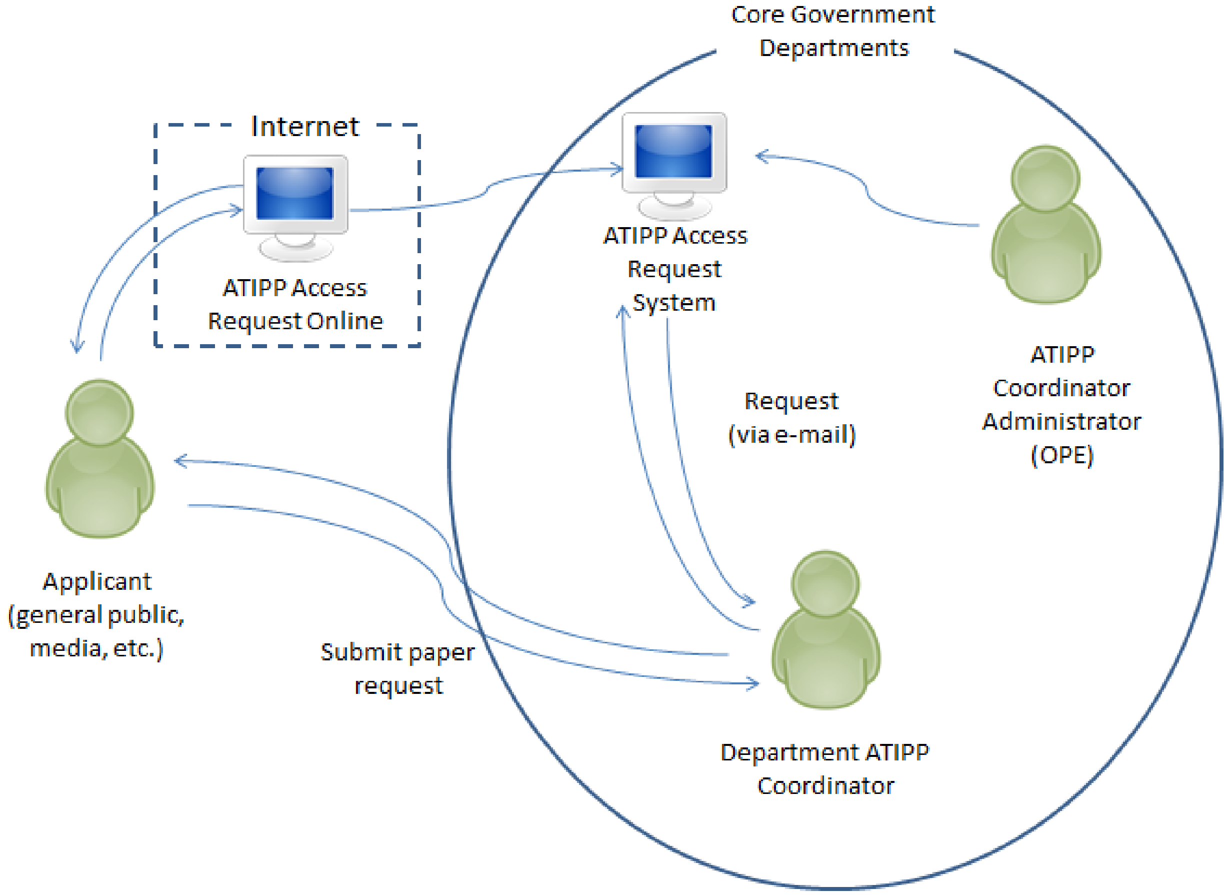
Example of how to complete Personal Information table:

#	**Personal Information**	**Purpose**	**Collected By**	**Used by**	**Disclosed to (if applicable)**	**Information Source**
1.	*First and last name*	*Identify and provide service to client*	*Case workers*	*Client services division – case workers, manager and director*	*Federal department A*	*Client application form*

Information Flow Diagram

The purpose of the information flow diagram is to provide a visual diagram of how personal information for the project will be collected, used and/or disclosed. The diagram should be as detailed as possible. You should also provide a written description of the diagram. For an example of an information flow diagram and written description refer to the next page:

A: Diagram


Core Government Departments
Internet
ATIPP Access Request Online
ATIPP Access Request System
Applicant (general public, media, etc.)
Request (via e-mail)
ATIPP Coordinator Administrator (OPE)
Submit paper request
Department ATIPP Coordinator

B. Description of Diagram

- *Paper Requests: The Applicant submits a paper request to the Department ATIPP Coordinator. The Coordinator enters the request into the ATIPP Access Request System.*
- *Online Requests: The Applicant enters their request online, which is automatically forwarded to the ATIPP Access Request system. The Department ATIPP Coordinator can access the details of the request through the ATIPP Access Request System.*
- *The ATIPP Coordinator Administrator also has access to the ATIPP Access Request System*

Note: There are various software programs that have the ability to create information flow diagrams, including Visio, Microsoft PowerPoint and Microsoft Word. The ATIPP Office would recommend using any existing software you may have to avoid any additional costs.

3.0 Collection of Personal Information

This section of the PIA reviews the personal information that is collected and the authorization a public body has to collect it. It also reviews the manner of collection to ensure that the collection complies with the legislative procedures.

A: Type and Extent of Personal Information Collected

It is imperative to the process and PIA that the list of personal information involved in the project is accurate and complete. Question 3.1 asks you to confirm whether the personal information listed in the personal information table from section 2.0 is accurate and complete. If the answer is no, then you are required to provide details explaining why the list is incomplete (e.g. unsure if the project will collect other personal information at this point, etc.).

B: Authority for Collection

In order to collect personal information for a project, public bodies must have the authority to do so. This section reviews whether you have the authority to collect the personal information for your project:

Authority for Collection Table

To complete this table the list of personal information identified in the personal information table from section 2.0 of the PIA should be used.

For each individual type of personal information being collected (e.g. name, date of birth, etc.) the following information must be included:

Personal Information: The type of personal information being collected (e.g. name, date of birth, etc.). This section should be as detailed as possible. For example, rather than writing “name”, write “first and last name”, “first, middle and last name”, etc.

Purpose: The purpose for collecting the personal information (e.g. reason the personal information is required for the project) must be included so the public body can demonstrate why it is necessary and how it relates to the objectives of the project.

Legislative Authority: You must indicate what legislative authority you have to collect personal information for this project. The authority may come from either *ATIPPA, 2015* or another piece of legislation that applies to your public body (e.g. *Municipalities Act, 1999, Statistics Agency Act, etc.).* When completing this table:

- Any legislation that authorized the collection of personal information should be listed;
- If a certain piece of legislation only authorizes the collection of some of the personal information being collected this should be noted; and
- The specific sections, subsections or paragraphs of any legislation that authorizes the collections of personal information must be listed.

Example of how to complete the Authority for Collection Table:

#	Personal Information	Purpose	Authority
1.	*First and last name*	*To identify and provide service to clients*	*s.61(c), ATIPPA, 2015*

Question 3.2

The purpose of this question is to determine if this project will include data matching. Data matching occurs when information from different sources is gathered and compared (i.e. matched). Data matching can occur if a public body compares information from an already existing source they have or from an outside source. An example of data matching could be if you collect an individual’s annual income (source 1) and you compare the amount provided with the Canada Revenue Agency (source 2) to confirm the amount is correct.

C: Manner of Collection

To complete this table the list of personal information identified in the personal information table from section 2.0 of the PIA should be used.

For each individual type of personal information being collected (e.g. name, date of birth, etc.) the following information must be included:

Personal Information: The type of personal information being collected (e.g. name, date of birth, etc.). This section should be as detailed as possible. For example, rather than writing "name", write "first and last name", "first, middle and last name", etc.

Manner of Collection: How personal information will be collected (e.g. directly from the individual, from a third party, etc.) must be included to ensure compliance with the privacy provisions of *ATIPPA, 2015*, especially in cases where information will not be collected directly from the individual.

Legislative Authority: You must indicate what legislative authority you have to collect personal information for this project in the manner identified (e.g. directly from the individual, from a third party, etc.). The authority may come from either *ATIPPA, 2015* or another piece of legislation that applies to your public body (e.g. *Municipalities Act, 1999, Statistics Agency Act, etc.).*When completing this table:

- Any legislation that authorized the collection of personal information in the manner specified should be listed;
- If a certain piece of legislation only authorizes the collection of some of the personal information being collected this should be noted; and
- The specific sections, subsections or paragraphs of any legislation that authorizes the collections of personal information must be listed.

Example of how to complete the Manner of Collection Table:

#	Personal Information	Manner of Collection	Legislative Authority
1.	*First and last name*	*Directly from individual via application form.*	*62(1)(c)(i) ATIPPA*

D: Privacy Notices

In most cases, when collecting personal information directly from an individual, public bodies are required to include a privacy notice which includes the purpose for the collection, the legal authority a public body has to collect the information, and the contact information for someone who can answer any questions regarding the collection.

The PIA will identify which forms (electronic and paper) for this project include privacy notices, and whether they include all required information.

For each form used for this project where personal information being collected (e.g. name, date of birth, etc.) the following information must be included:

Form Name: Cite the name of the form and any reference numbers and versions of it.

Information Collected: Individually list all pieces of personal information that are collected on the form.

Privacy Notice: If there is a privacy notice on the form, copy the text of the notice into the table. If there is no privacy notice, provide an explanation.

Example of how to complete the Privacy Notices Table:

#	Form Name	Information Collected	Privacy Notice Included
1.	*Application for subsidy A*	*First and last name, annual income*	*Under the authority of sections 61(c) and 68(1)(c) of the Access to Information and Protection of Privacy Act, 2015, the personal information on this form will be collected and disclosed for the purpose of determining eligibility for the Subsidy A Program and administrative purposes. If you have any questions regarding this collection or disclosure please contact (709) 729-5555.*

E: Collection Accuracy

This section reviews the potential accuracy of the personal information being collected for this project through 2 questions:

Question 3.3

Question 3.3 asks whether the identity of the applicant is verified when being collected (e.g. photo ID, etc.). If the answer is no, then you are required to provide details explaining why verification will not occur.

Question 3.4

Question 3.4 asks whether the individual confirms that the information is complete and correct (e.g. declaration on form, etc.). If the answer is no, then you are required to provide details explaining why this will not occur (e.g. form is collecting general feedback on a program; since information is opinion rather than fact, requesting accuracy is inappropriate, etc.).

F: Collection Risk Analysis

To complete this section you must list each potential privacy risk that may be associated with the collection of personal information for this project and then include any risk mitigation strategies being implemented to mitigate these risks.

Example of how to complete the Risk Analysis-Collection Table:

Risk Analysis- Collection		
#	**Potential Risks with collection**	**Implemented Risk Mitigation Strategy**
1.	*That all public body employees would have access to sensitive client information*	*Access controls have been added to the database to limit employees with access to only those who require access for their job.*

4.0 Use of Personal Information

This section of the PIA reviews the use of personal information for your project.

A: Use

Question 4.1

Question 4.1 asks whether the public body collecting the personal information (i.e. your public body) will be the primary user of the personal information. If the answer is no, then you are required to list the other organization/s that will be using the personal information.

Personal Information Use Table

To complete this table the list of personal information identified in the personal information table from section 2.0 of the PIA should be used.

For each individual type of personal information being used (e.g. name, date of birth, etc.) the following information must be included:

Personal Information: The type of personal information being used (e.g. name, date of birth, etc.). This section should be as detailed as possible. For example, rather than writing “name”, write “first and last name”, “first, middle and last name”, etc.

Used by: Indicate who within the in the public body will use the information (e.g. division, position, etc.). Be as detailed as possible; for example, if you know which positions within the public body will use the personal information, include their titles rather than only stating which division/s will use it.

Used for Purpose of: Indicated why the personal information will be used (refer back to section 3B table in which the purpose for collection is outlined). For example, if you are collecting applicants’ annual income, you may list “used for the purpose of determining eligibility for program ‘A’ which has a maximum annual income cut off of $25,000.”

Legislative Authority: You must indicate what legislative authority you have to use personal information for this project (e.g. to determine eligibility for program, etc.). The authority may come from either *ATIPPA, 2015* or another piece of legislation that applies to your public body (e.g. *Municipalities Act, 1999, Statistics Agency Act, etc.).*When completing this table:

- Any legislation that authorized the collection of personal information in the manner specified should be listed;
- If a certain piece of legislation only authorizes the collection of some of the personal information being collected this should be noted; and
- The specific sections, subsections or paragraphs of any legislation that authorizes the collections of personal information must be listed.

Example of how to complete the Personal Information Use Table:

#	Personal Information	Used By	Used for Purpose of	Legislative Authority
1.	*First and last name*	*Employees in division A*	*To determine client eligibility for service A*	*s.66(1)(a), ATIPPA, 2015*

B: Additional Use

<u>Question 4.2</u>

Question 4.2 asks whether the personal information being collected will be used for any additional purposes (i.e. purpose other than original purpose for collection). If the answer is yes, you must complete the table below.

<u>Additional Use Table</u>

This section only has to be completed if you will be using the personal information that was collected for this project for a purpose other than the purpose originally identified.

For each individual type of personal information being used (e.g. name, date of birth, etc.) the following information must be included:

Personal Information: The type of personal information being used (e.g. name, date of birth, etc.). This section should be as detailed as possible. For example, rather than writing "name", write "first and last name", "first, middle and last name", etc.

Used by: Indicate who within the in the public body will use the information (e.g. division, position, etc.). Be as detailed as possible; for example, if you know which positions within the public body will use the personal information, include their titles rather than only stating which division/s will use it.

Original Purpose: Indicated why the personal information was originally collected to be used (refer to the Personal Information Use Table in this section). For example, if you are collecting applicants' annual income, you may list "used for the purpose of determining eligibility for program 'A' which allows a maximum annual income of $25,000."

New Purpose: List the new way in which the personal information will be used. For example, "applicant's annual income will also be used for the purpose of determining eligibility for program B, which allows a maximum annual income of $27,000."

Legislative Authority: You must indicate what legislative authority you have to use personal information for this project (e.g. to determine eligibility for program, etc.). The authority may come from either *ATIPPA, 2015* or another piece of legislation that applies to your public body (e.g. *Municipalities Act, 1999, Statistics Agency Act, etc.).*When completing this table:

- Any legislation that authorized the collection of personal information in the manner specified should be listed;
- If a certain piece of legislation only authorizes the collection of some of the personal information being collected this should be noted; and
- The specific sections, subsections or paragraphs of any legislation that authorizes the collections of personal information must be listed.

Example of how to complete the Additional Use Table:

#	Personal Information	Original Purpose	New Purpose	Legislative Authorization
1.	*Annual income*	*To determine client eligibility for service A*	*To determine client eligibility for service B which offers similar services to service A*	*s.69, ATIPPA, 2015*

C: Use Risk Analysis

To complete this section you must list each potential privacy risk that may be associated with the use of personal information for this project and then include any risk mitigation strategies being implemented to mitigate these risks.

Example of how to complete the Risk Analysis-Use Table:

Risk Analysis - Use		
#	**Potential Risks with use**	**Implemented Risk Mitigation Strategy**
1.	*That all public body employees could use it for additional purposes not authorized under ATIPPA, 2015.*	*Procedures have been updated to clarify when employees can use personal information and training has been provided to all employees regarding the changes to procedures.*

5.0 Disclosure of Personal Information

This section of the PIA reviews the disclosure of personal information (i.e. outside of your public body) for your project. If your project does not disclose any personal information you can move to section 6 immediately.

A: Disclosure

Questions 5.1

Question 5.1 asks whether the personal information being collected will be disclosed for this project (i.e. will be disclosed outside of your public body). If the answer is yes, you must complete the remainder of section 5. If the answer is no, you can move to section 6.

Questions 5.2

Question 5.2 asks whether the personal information being disclosed for this project will be disclosed to a third party other than a public body that falls under *ATIPPA, 2015* (e.g. federal department, external service provider, non-profit, etc.). If the answer is yes, you must attach the privacy provisions of any information sharing agreement or contract that was signed with the third party. This is to determine whether personal information that will be accessible to third parties will be protected in the same way that is required under *ATIPPA, 2015.*

Disclosure Table

This section only has to be completed if your project will be disclosing personal information.

For each individual type of personal information being disclosed (e.g. name, date of birth, etc.) the following information must be included:

Personal Information: The type of personal information being disclosed (e.g. name, date of birth, etc.). This section should be as detailed as possible. For example, rather than writing “name”, write “first and last name”, “first, middle and last name”, etc.

Disclosed to: Indicate which third parties the information will be disclosed to (e.g. department A, federal department B, Business ABC Inc., etc.). Be as detailed as possible; for example, if you know which divisions/positions within the third party the personal information will be disclosed to, include their titles rather than only stating which third party it will be disclosed to.

Purpose for Disclosure: Indicate why the personal information is being disclosed to the third party. For example, if you are disclosing applicants’ annual income, you may list “disclosed to federal department A to confirm annual income to determine eligibility for program ‘A’ which allows a maximum annual income of $25,000.”

Legislative Authority: You must indicate what legislative authority you have to disclose personal information for this project (e.g. authorized under s.68(1)(c) of *ATIPPA, 2015*, etc.). The authority may come from either *ATIPPA, 2015* or another piece of legislation that applies to your public body (e.g. *Municipalities Act, 1999, Statistics Agency Act, etc.).*When completing this table:

- Any legislation that authorized the disclosure of personal information in the manner specified should be listed;

- If a certain piece of legislation only authorizes the disclosure of some of the personal information listed this should be noted; and
- The specific sections, subsections or paragraphs of any legislation that authorizes the disclosure of personal information must be listed.

For a complete list of when disclosure of personal information is authorized under section 68 of *ATIPPA, 2015* please click here.

Can Purpose be Achieved Without Disclosure: At this point you must review the purpose of the disclosure listed in the table and determine whether this purpose can be accomplished without disclosing the personal information. If the answer is yes, then the personal information should not be disclosed. For example, if you intend to disclose someone's name, mailing address, annual income, email address and phone number in order to confirm eligibility for a service. When considering whether all of this information needs to be disclosed, you may determine that the email address and phone number, which were originally collected in order to communicate with the individual, do not have to be disclosed. In this case, you would remove these two categories from the personal information you disclose to confirm eligibility.

Example of how to complete the Disclosure Use Table:

#	Personal Information	Disclosed to	Purpose of disclosure	Legislative Authority	Can purpose be achieved without disclosure?
1.	*First and last name*	*Federal Department A*	*To determine eligibility for service*	*68(1)(b), ATIPPA, 2015*	*No*

B: When Disclosure is With Consent

In some of the cases where you are disclosing personal information, you may have listed your legislative authority to do so as section 68(1)(b) of *ATIPPA, 2015* which authorizes disclosure when the individual the personal information is about has consented to the disclosure, often times through an application form or consent form.

In these instances it is important to ensure that any application or consent forms are clear and understandable to ensure that consent is provided with understanding. In this section, you are required to review any application or consent forms for the project and check any consent criteria listed that were met in said forms. These criteria include:

The purpose for disclosure is clear and concise: meaning that the purpose is explained or written in plain and understandable language.

The person giving consent is authorized to give consent: in some cases an individual may be providing consent on behalf of another individual. If this is the case, you must have a way to confirm they are authorized to provide consent (e.g. are legal guardian, administrator of a deceased individual's estate, etc.).

Consent is voluntary: meaning that individuals, in no way feel coerced into giving their consent.

Consent is in writing or annotated: Consent should be obtained in writing (e.g. on a form, etc.). However, in cases where consent is provided verbally, the public body has procedures in place requiring employees to annotate an individual's file, or will follow-up in writing confirming consent.

An explanation of the impact of consent or providing consent is provided: meaning that an individual is aware of what will happen if they provide consent or do not provide consent (e.g. will receive benefit or will not receive benefit, etc.).

Individual is able to withdraw consent: meaning that individuals are aware they are able to withdrawn consent, and understand what withdrawing consent means (e.g. no longer eligible for service, etc.).

Example of how to complete Consent Criteria:

	Consent Criteria	**Criteria Met? Yes/No**
X	The purpose for disclosure is clear and concise	Yes

	Consent Criteria	Criteria Met? Yes/No
X	The person giving consent is authorized to give consent	Yes
X	Consent is voluntary	Yes
X	Consent is in writing or annotated	Yes
X	An explanation of the impact of consent or not providing consent is provided	Yes
X	Individual is able to withdrawn consent	Yes

C: Disclosure Risk Analysis

To complete this section you must list each potential privacy risk that may be associated with the disclosure of personal information for this project and then include any risk mitigation strategies being implemented to mitigate these risks.

Example of how to complete the Risk Analysis-Disclosure Table:

Risk Analysis - Disclosure		
#	**Potential Risks with disclosure**	**Implemented Risk Mitigation Strategy**
1.	*The third party does not fall under ATIPPA, 2015 and is not required to follow its privacy provisions*	*A privacy clause has been added to the contract with the third party requiring it to follow the privacy provisions of ATIPPA, 2015 in regards to the personal information disclosed.*

6.0 Safeguards and Security

Public bodies must take reasonable steps to protect personal information from misuse, interference and loss, as well as unauthorized collection, use, access, modification or disclosure.

Where the project involves an IT component, the IT representative from the PIA team should be involved in completing this section.

A-D: Physical, Administrative and Technical Safeguards, and Access Controls

Sections 6A-6D of the PIA outline common physical, administrative, and technical safeguards, and access controls that can be used to protect personal information in both paper and electronic formats. For each section list which safeguards will be in place for the personal information being collected, used, accessed or disclosed for this project. There is also an “other” option where you can include any additional safeguards that will be in place that are not already listed. If these include policies, procedures or other materials, please attach them to this PIA.

In the further details, please indicate if the safeguard is general or program-specific. For example, if passwords are required:

- You may indicate that this refers to a password to access your desktop computer (general safeguard), or
- You may indicate that access to the specific program files requires a password (program-specific password)

In order to answer this question you should consult with the IT representative from the PIA team (OCIO for government departments).

Example of how to complete A-D Tables:

A. Physical Safeguards

#	**Safeguard**	**Yes/No**	**Further Details**
1.	Locked Filing Cabinets	Yes	
2.	Secure Storage Areas	Yes	Storage is located in a locked room with access restricted to those who require access for their job.
3.	Secure Building Access	Yes	Employee ID required to access building.

#	Safeguard	Yes/No	Further Details
4.	Security Systems	Yes	
5.	Other	N/A	

B. Administrative Safeguards

#	Safeguard	Yes/No	Further Details
1.	Security Clearances/Background Checks	Yes	Done prior to employment
2.	Privacy Clauses in 3rd Party Contracts	Yes	
3.	Privacy Policies	Yes	General privacy policy, as well as policy on taking work home
4.	Account Management	Yes	
5.	Change Management	Yes	
6.	User Warnings	Yes	
7.	Other	Yes	Oath of confidentiality signed by new employees

C. Technical Safeguards

For a project with an electronic component, the IT representative on your PIA team may need to assist in completing this section.

#	Safeguard	Yes/No	Further Details
1.	Encryption	Yes	Any personal information taken out of the office is saved on an encrypted USB
2.	Secure disposal of electronic	Yes	Use shredding company A

#	Safeguard	Yes/No	Further Details
	records		
3.	Auditing capability	Yes	
4.	Other		

D. Access Control

For a project with an electronic component, the IT representative on your PIA team may need to assist in completing this section.

#	Access Control	Yes/No	Further Details
1.	User authentication	Yes	Username and login to access public body information
2.	Passwords	Yes	Access to specific systems require passwords
3.	Locking workstations	Yes	If person forgets to lock workstation, it automatically locks after 15 minutes of no use.
4.	User classifications (e.g. limiting users)	Yes	Electronic records have access restrictions
5.	Exit procedures	Yes	Access is removed immediately upon termination
6.	Other		

E: Positions with Access

Access controls for end users are one of the best ways to protect information by limiting the number of people who have access to it. Another function that provides increased protection of information is an audit function. Having software with auditing capabilities can help identify cases of inappropriate access or attempted access. The Positions with Access Table must be completed by listing any positions that will have access to the personal information collected for this project. This requires you to review the purpose of the project and determine who will need access to this personal information in order to fulfil this purpose.

Once it is determined which positions will need access to the personal information, each position should be reviewed to identify what functionality their position requires (e.g. access, ability to modify content, etc.).

Any position that does not require access, should not be provided access where a system allows for access controls.

In order to answer this question you may need to consult with you IT division (OCIO for government departments).

Example of how to complete Positions with Access Table:

#	**Position**	**Functionality Assigned to User**			
		Read/View	**Add Content**	**Delete**	**Modify**
1.	*Client Services Technicians (5)*	*Yes*	*Yes*	*No*	*Yes*

F: Preliminary Threat Risk Assessment (Pre-TRA)

The Preliminary Threat Risk Assessment (Pre-TRA Process) is an information risk assessment activity that is mandatory for all projects within the Office of the Chief Information Officer's (OCIO) System Development Lifecycle (SDLC). This process ranks information sensitivity and criticality in order to determine the required level of security within an IT solution and identifies additional risk assessments that must be completed during later phases of an OCIO project. At the conclusion of this process, project teams are provided a Risk Assessment Workbook that contains an *Information Security Classification* and *Pre-TRA Checklist*, completed by the OCIO's Information Protection (IP) Division. For more information about the Pre-TRA, see the Project Management section of the OCIO website.

Question 6.1 asks whether a Pre-TRA has been completed. If the answer is yes, this assessment must be attached to this PIA. In some cases, the OCIO may determine that the assessment should not be provided based on security concerns. If this is the case, please contact the OCIO's IP Division and have them provide a summary of the assessment.

G: Threat Risk Assessment (TRA)

A TRA is a detailed, structured process designed to help management understand the risks and issues with the implementation of a new application or infrastructure within a business environment. The outcome or objective of a TRA is to provide recommendations to maximize the protection of confidentiality, integrity and availability while still providing functionality and usability for business owners. Unlike other assessments that focus on IT systems, TRAs also look for threats within the business layer and as such, require significant involvement of client departments and review of client-side policies and processes. TRAs may be initiated by IT divisions (OCIO for government departments), but their completion is dependent upon the full support, commitment and involvement of client departments.

Question 6.2 asks whether a Threat Risk Assessment has been completed. If the answer is yes, this assessment must be attached to this PIA. In some cases your IT division may determine that the assessment should not be provided based on security concerns. If this is the case, please contact your IT division and have them provide a summary of the assessment. Where the IT division is the OCIO, contact the OCIO's IP Division to obtain a summary of the assessment.

H: Vulnerability Assessment (VA)

A Vulnerability Assessment (VA) is a series of manual and automated processes and procedures used to assess and prioritize security vulnerabilities in a system (i.e. application and/or infrastructure). Conducting a VA assists an organization in determining the security posture of the environment and the level of exposure to threats. A VA will identify vulnerabilities by evaluating if the system has the proper controls in place as they were designed and meant to be implemented. In order to ensure proper due diligence and maintain the integrity of risk assessment protocols, all VA's are conducted by independent (i.e. non-

Government) security assessors. With respect to OCIO projects, the OCIO's IP Division is responsible for oversight of VA activity and signing off on VA completion. For more information about VAs, see the Project Management section of the OCIO website.

Question 6.3 asks whether a Vulnerability Assessment has been completed. If the answer is yes, a summary this assessment must be attached to this PIA. In some cases your IT division may determine that the assessment should not be provided based on security concerns. If this is the case, please contact your IT division and have them provide a summary of the assessment. Where the IT division is the OCIO, contact the OCIO's IP Division to obtain a summary of the assessment.

I: Other Assessment

Question 6.4 asks whether any other security and/or information risk assessments have been completed (e.g. security design review, etc.).

J: Review of Security Safeguards

This section requires that you specify the frequency with which you will review security safeguards for this project. However, if this is a new project, reviews should occur more frequently initially to ensure any issues that arise during implementation are identified and resolved.

K: Use Risk Analysis

To complete this section you must list each potential privacy risk that may be associated with the security safeguards (or lack thereof) for this project and then include any risk mitigation strategies being implemented to mitigate these risks.

Example of how to complete the Risk Analysis-Security Safeguards Table:

Risk Analysis - Security Safeguards		
#	**Potential Risks with Security Safeguards**	**Implemented Risk Mitigation Strategy**
1.	*The database being used does not have an audit function.*	*Employees with access to the database are limited to those who require it. In addition, these employees will complete privacy training.*

7.0 Privacy Breach Reporting and Management

A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information. Such activity is “unauthorized” if it occurs in contravention of *ATIPPA, 2015*.

The most common privacy breaches occur when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information is stolen or personal information is mistakenly provided to the wrong person.

A: Policies and Procedures

Question 7.1 asks if there are any organizational policies and procedures for reporting and managing breaches. The ATIPP Office has developed a Privacy Breach Protocol, along with a general Privacy Policy and Procedures Manual that can be used by all public bodies; however, if you have any additional policies, procedures or protocols, please identify these and attach them to this PIA.

B: Previous Privacy Breaches

In this section you must identify any privacy breaches that your public body has had in the past 2 years. You will likely need to consult your public body ATIPP Coordinator or Privacy Officer/equivalent to complete this list.

Example of how to complete the Previous Privacy Breaches Table:

#	**Description**	**# of people affected**	**Days to respond**	**Reported to OPE**	**Reported to OIPC**
1.	*A letter with one client’s name, address and annual income was sent to another client in error.*	*1*	*10*	*Yes*	*Yes*

C: Privacy Breach Risk Analysis

To complete this section you must list each potential privacy risk that may be associated with a privacy breach for this project and then include any risk mitigation strategies being implemented to mitigate these risks. This section is intended to highlight privacy risks. For IT system security risks, that information would be contained within the corresponding risk assessment completed by the OCIO and referenced above in Section 6.

Example of how to complete the Risk Analysis-Privacy Breaches Table:

Risk Analysis- Privacy Breaches		
#	**Potential Risks of Privacy Breach**	**Implemented Risk Mitigation Strategy**
1.	*Employees could access personal information and use or disclose it for personal purposes*	*Oath of Employment*
2.	*Request may not actually be from client (i.e. their email address may be being used by someone else)*	*Implementation of identification verification procedures*
3.	*Inherent risks in sending personal information to a client via email*	*Policy developed to inform clients of risk and ask if they would like the information via a different medium, such as through the mail*

8.0 Recommendations
(to be completed by the ATIPP Office

This section is to be completed by the ATIPP Office, not the PIA team. For each section of the PIA, potential privacy risks have been identified and mitigations strategies listed. In this section, the ATIPP Office will review the PIA as a whole and provide any additional recommendations it deems appropriate.

When completing this section the ATIPP Office should review each risk identified in the PIA (and any others they determine may exist) and take into consideration the risk mitigation strategy being implemented for the project when determining the overall risk.

When determining the overall risk the ATIPP Office must use the Risk Assessment Methodology outlined in the ATIPP Office PPIA.

9.0 Final Sign-Off

Before the PIA is finalized, it must be reviewed by the ATIPP Coordinator for the department/public body, the IT representative with OCIO on the PIA team (if projects have an electronic component), and the IM Director for the department/public body.

Following the review and sign-off from the reviewers, you must receive final sign off on the completed PIA from the PIA team lead, Program Manager (if not Team Lead), the Senior Privacy Analyst from the ATIPP Office, and the head of your public body (e.g. Deputy Minister, CEO, President, etc.).