# PRIVACY MANAGEMENT Program (PMP) Workbook Guide

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


ATIPP Office
Department of Justice and Public Safety
May 2019

# Table of Contents

## Overview

In 2018, the Office of the Information and Privacy Commissioner released their Privacy Management Program Guidelines for public bodies, including a section on "Program Controls."

## Program Controls

The ATIPP Office has developed tools and resources that public bodies can use when developing a Privacy Management Program (e.g. policies and procedures, privacy breach protocol, etc.). These materials can be found on the ATIPP Office website at www.atipp.gov.nl.ca. These tools and resources include:

### a. Compliance Policies

The ATIPP Office has developed a Privacy Policies and Procedures Manual (which includes a privacy breach protocol) which is accessible to all public bodies. However, public bodies may find it necessary to develop additional policies for specific programs or services that they provide. Public bodies are encouraged to address the following privacy issues in any policies developed:

- Authority for collection, use and disclosure of personal information;
- Requirements for consent and notification;
- Accuracy of personal information;
- Individual access to and correction of personal information;
- Retention and disposal of personal information;
- Responsible use of information and information technology, including administrative, physical and technological security controls; and
- A process for handling privacy-related complaints.

The ATIPP Office privacy policies and procedures manual can be found on the Office's website at https://www.atipp.gov.nl.ca/info/.

### b. Risk Assessment Tools

The ATIPP Office has developed tools to assist with privacy compliance for specific projects:

- Preliminary Privacy Impact Assessment (PPIA) – this reviews new or existing programs to ensure compliance with the privacy provisions of the **Access to**

**Information and Protection of Privacy Act, 2015 (ATIPPA, 2015).** A PPIA can also be used to determine whether a full PIA is required.

- Privacy Impact Assessment (PIA) – a more in-depth tool used to review new or existing programs to ensure compliance with the privacy provisions of **ATIPPA, 2015.**

Public bodies (other than government departments) can modify these for their own purposes. The PPIA and PIA templates, as well as guides outlining various requirements, can be found on the ATIPP Office website at https://www.atipp.gov.nl.ca/info/privacyprotection.html.

While not legislatively required for existing programs (or for non-government department public bodies), it is recommended that a PPIA or PIA be completed on programs or services that collect, use or disclose personal information, to ensure compliance with **ATIPPA, 2015**.

Additionally, the ATIPP Office is available to assist public bodies by completing website reviews or general privacy reviews. While these are not as formal as a PPIA or PIA, they may identify potential issues or the need for a PPIA/PIA to be completed.

### c. Training

Privacy training is encouraged for all employees, tailored to their specific duties (where possible). Best practice would include training that is ongoing and sufficiently detailed to ensure employees have the knowledge to meet the public body's obligations. Training content should be updated periodically to reflect changes within the public body, **ATIPPA, 2015** and to best practices. Public bodies are encouraged to document training processes, and measure participation and success of the training with objective, consistent measurements.

The ATIPP Office is available to provide general privacy training to all public bodies. Additionally, the Office can work with public bodies to provide more specific training that may be required.

## d. Information Sharing Agreements/Memorandum of Understanding

To deliver services and programs, public bodies are sometimes required to share personal information with other public bodies or third parties (i.e. entities other than public bodies). Where the sharing of personal information is part of a program or service, information sharing agreements or memorandums of understanding are encouraged to be put in place to ensure that each entity that will have access to the personal information in question is aware of, and required to comply with the privacy provisions of **ATIPPA, 2015**.

The ATIPP Office is in the process of developing a template information sharing agreement. This will be made available once completed.

When entering into a memorandum of understanding, ensure there is a section that outlines requirements for the protection of personal information (e.g. security measures, breach reporting, what information will be shared and for what purposes, etc).

## e. Requests for Proposals

If a public body is releasing a request for proposal for a program or service that includes the collection, use, access or disclosure of personal information, it is encouraged to include a section regarding privacy and security requirements. When drafting an RFP, the ATIPP Office can assist in regards to the privacy and security requirements section.

## f. Privacy Management Workbook

The ATIPP Office developed a workbook designed to help public bodies evaluate their compliance with the privacy provisions of **ATIPPA, 2015**. Using this workbook as a guide may help to identify the areas where public bodies can improve their compliance. This guide provides instructions on how to complete the workbook (see below).

## Instructions for Completing the Privacy Management Workbook

- Senior management is encouraged to make a commitment to use the workbook, and should select a person to lead. Ideally, the person who leads should be familiar with **ATIPPA, 2015** and with the work of the public body. Senior management can also appoint other individuals to assist the lead. If there is no one available who is familiar with **ATIPPA, 2015** please feel free to seek assistance from the ATIPP Office.

- While there should be a lead assigned to this process (as mentioned above), senior management (or those designated by senior management) is encouraged to participate in the process of using this workbook. For larger public bodies, this will include someone from each division where necessary.

- Decide if you are going to use one workbook for the public body as a whole, or by division. For government departments, a workbook should be used for each division unless the department is small or collects very little personal information.

- Some sections may not be relevant to a public body/division. For example, if a public body has not completed any privacy assessments, you can state "not applicable" in place of that section.

- If sections of the workbook are completed, the lead and senior management are encouraged review it to determine what gaps exist within the public body, and identify ways to mitigate risks associated with the gaps. Additionally, the workbook can be provided to the ATIPP Office for review. If provided, the ATIPP Office will review the workbook and provide the public body with a report which identifies potential risks and provide recommendations for mitigating such risks.

- Public bodies are encouraged to have the employee survey (Tab 13) completed by all staff where feasible. If this is not possible, please be sure to get a representative sample, including regional staff. This will provide a clearer picture of privacy compliance throughout the public body.

- A checklist for the workbook is provided at Tab 14 to identify the completion of sections of the workbook.

- If you need assisting completing this workbook, please contact:

  ATIPP Office
  Department of Justice and Public Safety

Phone: (709) 729-7072/1-877-895-8891
Email at ATIPPoffice@gov.nl.ca

## Definitions

- **Personal Information (p.2(u) of ATIPPA, 2015)**: Recorded information about an identifiable individual, including (but not limited to):
    - The individual's name, address or telephone number;
    - The individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
    - The individual's age, sex, sexual orientation, marital status or family status;
    - An identifying number, symbol or other particular assigned to the individual;
    - The individual's fingerprints, blood type or inheritable characteristics;
    - Information about the individual's health care status or history, including a physical or mental disability;
    - Information about the individual's educational, financial, criminal or employment status or history;
    - The opinions of a person about the individual; and,
    - The individual's personal views or opinions, except where they are about someone else.

- **Personal Information Banks:** A personal information bank is personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual (e.g. MCP, social insurance number, etc.). The information can be stored in electronic form or in paper form. For example, the Motor Vehicle Registration Division has a database of driver's licenses and vehicle registrations. As the database can be searched by vehicle or driver, it is a personal information bank. Not all collections of personal information are personal information banks. The key to determining whether a group of files, which contain personal information, is a personal information bank is whether the information is organized and retrievable by a personal identifier (e.g. name, MCP, etc.).

- **Privacy Breach:** 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**.

- **Preliminary Privacy Impact Assessment (PPIA):** A formal assessment of privacy compliance of a program or service. A PPIA will also identify whether a full Privacy Impact Assessment (PIA) may be required.

- **Privacy Impact Assessment (PIA):** A formal assessment of privacy compliance of a program or service. PIAs are more in-depth than PPIAs and are used when a project entails significant privacy risks.

- **Privacy Notice:** A privacy notice is required when collecting personal information (except in limited circumstances). The notice includes the purpose for the collection, the legal authority a public body has to collect the personal information, and the contact information of someone in the public body that people can contact if they have any questions about the collection of personal information.

- **Record:** Means recorded information in any form, including a computer file, an email, a photograph, handwritten information, paper files, a dataset and any other information that is recorded or stored in any manner. Please note that most of the questions in this document only refer to records which include personal information.

- **Safeguards:** measures taken to prevent unauthorized collection, use, access or disclosure of personal information. Safeguards in this context can include physical, administrative or technical safeguards:
    - **Physical Safeguards** – e.g. locked file cabinets, secure storage areas or records facilities, secure building access, etc.
    - **Administrative Safeguards** – e.g. security clearances and/or background checks, privacy clauses in third party contracts, privacy policies and/or procedures, accounts management, change management, etc.
    - **Technical Safeguards** – e.g. encryption, access controls, data recovery procedures, and secure disposal of electronic records.

    For a more detailed description of safeguards, please review section 8.1.1- 8.1.3 of the ATIPP Office's Privacy Policies and Procedures Manual at https://www.atipp.gov.nl.ca/info/pdf/Protection_of_Privacy_Policy_and_Procedures_Manual.pdf

## 1. Application Forms that Collect Personal Information

Instructions:

- Review the programs/services provided by your public body to identify any application forms that are used to collect personal information.
- Enter the required information for each application form in Tab 1 of the workbook:
    - Personal information collected – list each type of personal information that is collected (e.g. name, address, date of birth, etc.); and
    - Privacy notice – does the application include a privacy notice (see definitions) on the form.
- Add additional lines to the table as required.
- Attach a copy of each application form to the workbook.

## 2. Personal Information Banks (PIBs)

Instructions:

- If you are unsure of what a PIB is, please refer to the key definitions section of this workbook.
- Review the programs/services provided by your public body to identify any PIBs.
- Enter each PIB in Tab 2 of the workbook and include the following information:
    - Purpose of PIB – the reason that information is collected (e.g. to provide a specific service to the public, etc.);
    - Personal information collected – list each type of personal information that is collected (e.g. name, address, date of birth, etc.);
    - Legal authority for collection – cite specific section of the legislation that authorizes the collection of personal information (e.g. p.61(c) of **ATIPPA, 2015**, etc.);
    - Legal authority for use – cite specific section of the legislation that authorizes the use of personal information (e.g. p.66(1)(a) of **ATIPPA, 2015**, etc.);
    - Legal authority for disclosure – If you disclose any of the personal information in the PIB, cite the specific section of the legislation that authorizes the disclosure (e.g. p.68(1)(b), etc.);
    - Is access restricted? – is access to the PIB limited to those employees who require access for their job?; and
    - Are there retention schedules? – are there schedules that outline when personal information can be deleted/destroyed.
- Add additional lines to the table as required.

NOTE: if your authority to collect or disclose personal information is based on another piece of legislation, please ensure you cite the specific section of that Act or regulation (for the purposes of disclosure), which authorizes the collection or disclosure.

## 3. Privacy Assessments (PPIAs or PIAs) – Part 1

Instructions:

- In Tab 3 of the workbook, list the programs or services in your public body where personal information is collected, used or disclosed, and include the following information:
    - Whether a PPIA/PIA was completed – if unsure, consult with your public body's ATIPP Coordinator. For government departments, the ATIPP Office may be able to assist. If the answer to this question is "no" then the remainder of the table does not need to be completed;
    - If a PPIA/PIA was completed – indicate which type of assessment was completed; and
    - Where recommendations provided – if reviewed by the ATIPP Office, a privacy impact report (PIR) would have been issued which includes a section for recommendations. Check the PIR to see if any recommendations were made, and then confirm whether the recommendations were followed.
    - If none, or only some of the recommendations were followed, list which ones were not.
- Add additional lines to the table as required.
- Attach a copy of each PPIA/PIA to the workbook.

## 4. Privacy Assessments (PPIAs or PIAs) – Part 2

Instructions:

Of the programs and services where a privacy assessment was not completed, list the top five where the completion of an assessment would be beneficial. This list can be based on various factors including, but not limited to:

- The sensitivity of the personal information involved;
- The number of people whose information is involved; and
- The types of people who have access to the personal information (e.g. public body employees, third parties, etc.).

## 5. Privacy Breaches

Instructions:

- In Tab 5 of the workbook, list all privacy breaches that have occurred in your public body since June 1, 2015, including the following information:
    - Date of breach – when the breach occurred;
    - Division – indicate which division (if applicable) within your public body where the breach occurred (e.g. financial services, human resources, etc.);
    - Reported to ATIPP Office – was the breach reported to this Office;
    - Reported to OIPC – was the breach reported to this Office;
    - Type of breach – indicate whether the breach was intentional (e.g. accessed information for non-work purposes, etc.) or accidental (e.g. letter mailed/emailed to the wrong person, etc.);
    - Number of people affected – list the number of people whose information was involved;
    - Personal information breached – list the personal information that was breached (e.g. name, email address, MCP, etc.); and
    - Actions taken since breach occurred – indicate what your public body has done to mitigate similar breaches from occurring in the future (e.g. additional training, updating procedures, etc.).
- Add additional lines to the table as required.
- The ATIPP Office may be able to assist in identifying privacy breaches that have occurred.

## 6. Information Sharing Agreements (ISAs)

Instructions:

- In Tab 6 of the workbook, list all programs or services where personal information is shared with another public body or third party, including the following information:
    - Information shared – list each public body or third party with whom that personal information is shared;
    - ISAs in place – are ISAs in place with each public body or third party with whom that information is being shared;
    - If yes, date ISA was signed – enter date;
    - If yes, end date – enter the date that the ISA expires/ends;
    - If yes, do ISAs comply with OIPC requirements? – a list of the requirements sent out by the OIPC can be found at https://www.oipc.nl.ca/pdfs/audit_of_information_sharing_agreements.pdf; and
    - If the answer to the above question is "some", list which requirements were not followed.
- Add additional lines to the table as required.

## 7. Contracts

Instructions:

- In Tab 7 of the workbook, list all active contracts that include services involving the collection, use, access or disclosure of personal information. Include the following information:
    - Third party – list the third party to contract;
    - Privacy provisions – indicate whether the contract includes a section regarding privacy. If the answer is no, the remainder of the table can be left blank;
    - Sub-contractors – do the privacy provisions of the contract extend to sub-contractors;
    - Breach reporting – is there a requirement in the contract for the third party to report any privacy breaches that may occur to the public body; and
    - End of contract – does the contract outline what happens to any personal information in the possession of the third party once the contract is over/is terminated? If yes, is the information provided to the public body or retained by the third party, or are other measures in place.
- Add additional lines to the table as required.
- Attach a copy of each applicable contract to this workbook.

PLEASE NOTE: only include contracts that involve the collection, use, access or disclosure of personal information.

## 8. Requests for Proposals (RFPs) and Public Tenders

Instructions:

- In Tab 8 of the workbook, list all RFPs and public tenders your public body has released in the past two years, which include services involving the collection, use, access or disclosure of personal information. Include the following information:
    - Description – provide a general description of the program or services the RFP/tender is seeking; and
    - Privacy/security requirement – the RFP/tender includes a section on privacy/security requirements.
- Add additional lines to the table as required.
- Attach a copy of each applicable RFP/tender to this workbook.

## 9. General Security and Safeguards Questionnaire

Instructions:

Answer yes, no or unsure to each question in this section.

## 10. Destruction of records

Instructions:

- Answer yes, no or unsure to each question in this section.

## 11. Employee requirements/training Table

Instructions:

- Answer yes, no or unsure to each question in this section.

## 12. Monitoring Checklist

Instructions:

- Answer yes, no or unsure to each question in this section.

In an effort to ensure that your public body is in compliance with the privacy provisions of **ATIPPA, 2015**, and taking the appropriate measures to ensure the personal information it collects, uses, access and discloses is properly protected, it is encouraged to complete this checklist on an annual basis.

## 13. Employee Survey

Instructions:

- Have all staff complete this questionnaire. If not able to have all staff complete this, please ensure you have a representative sample if your staff complement complete it.
- While provided in excel format, public bodies may wish to consider completing the employee survey electronically where appropriate. This may result in a larger number of staff completing the survey.
- For public bodies that have decided to use a workbook for each division, it may be appropriate to group certain divisions together for the purposes of this questionnaire (divisions that are small and do not collect very much personal information) in an effort to ensure the results remain anonymous.
- For public bodies that have a small number of staff, you may consider it appropriate to remove some or all of the demographic questions to ensure the results remain anonymous.

While this survey does not collect the names of the individuals completing the surveys, it is possible in smaller public bodies/divisions, that the demographic information being collected could identify individuals. Therefore, when sending the survey you should

include a privacy notice stating "The information in this form is collected for the purpose of assessing our organization's compliance with the **Access to Information and Protection of Privacy Act, 2015**. The information is collected under the authority of s. 61(c) of the Act. If you have any questions, please contact [insert contact information of lead]." This notice is included in Tab 13.

In an effort to ensure that your public body is in compliance with the privacy provisions of **ATIPPA, 2015**, and is taking the appropriate measures to ensure the personal information it collects, uses, access and discloses is properly protected, it is encouraged to complete this survey on an annual basis.

## 14. Gaps/Risks

While completing this workbook, you may identify particular gaps in relation to safeguards or potential risks in how your public body currently collects, uses, accesses and/or discloses personal information. For example, you may learn that:

- particular forms that contain sensitive personal information are stored in unlocked filing cabinets;
- there are no access controls on various folders within your shared drive, meaning every employee has access to information, even those who don't need access;
- employees are not informed of policies and procedures that the public body has;
- employees have been using un-encrypted USBs to save records that include personal information; or
- employees are not aware of what to do if they cause a breach or become aware of a breach.

If you come across any gaps or risks, they should be listed in Tab 14. Having these gaps/risks identified in a central location will assist you in dealing with them moving forward.

## 15. Required documentation checklist

Use this section to identify the sections you have completed and attached all documentation relating to the workbook.

Note: Please make a note if a portion of the workbook was not completed as it is not applicable. For example, if your public body/division has had no RFPs or contracts, note that this section was not completed as your division did not have any RFPs or contracts.

If you have any questions regarding this workbook, please contact:

ATIPP Office
Department of Justice and Public Safety
Phone: (709) 729-7072
Email: ATIPPoffice@gov.nl.ca