

Information Sharing Agreement (ISA) Guide

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



## Table of Contents

Part One - Introduction.....	3
What is an Information Sharing Agreement (ISA)?.....	3
When do I need an ISA? .....	3
What is Personal Information?.....	4
Purpose of an ISA .....	4
Before drafting an ISA – Start a Conversation.....	4
Part Two: Contents of Agreement.....	6
Section 1: Purpose.....	6
Section 2: Authority to Collect, Indirectly Collect, Use or Disclose Personal Information .....	6
Section 3: Information to be Exchanged and Mechanism for Exchange .....	8
Section 4: Confidentiality, Use and Disclosure .....	8
Section 5: Information Management and Technology.....	9
Section 6: Ensuring Data Protection.....	9
Section 7: Accuracy .....	10
Section 8: Amendments.....	10
Section 9: Auditing Requirements .....	10
Section 10: Expiry .....	10
Section 11: Coordinating Office.....	10
Section 12: Notices.....	10

## Part One - Introduction

This Guide is meant to assist public bodies in determining when an Information Sharing Agreement (ISA) may be required, and if so, how to complete one.

Some of the information in this guide is drawn from and informed by the Treasury Board of Canada's Document [Guidance on Preparing Information Sharing Agreements Involving Personal Information](#).<sup>1</sup>

### What is an Information Sharing Agreement (ISA)?

An ISA is a written record of understanding between a public body and another entity that outlines the terms and conditions under which personal information is shared between the parties.

ISAs cover such topics as what personal information is to be shared, the authority for sharing the information, and what safeguards should be in place.

### When do I need an ISA?

ISAs should be put into place when:

1. A public body is sharing information with another entity; and
2. The information being shared is personal information.

The "other entity" can include any other provincial public body, a federal or international public body, or a corporation or organization that is not a public body, as defined by the **Access to Information and Protection of Privacy Act** (the Act).

'Sharing' can include situations where the public body is disclosing personal information, where the public body is receiving personal information, or where personal information is being exchanged.

Generally, ISAs are used where there is going to be a regular exchange of personal information between two or more entities; they are not usually required for information you share one time. However, they may be required if there is a one time plan to share a large volume of information or particularly sensitive information. If you are not sure, we encourage you to contact the ATIPP Office.

---

<sup>1</sup> *Guidance on Preparing Information Sharing Agreements Involving Personal Information* (Canada, 2010)

## What is Personal Information?

Personal information is defined in the Act as "recorded information about an identifiable individual" and includes information such as:

- Name
- Phone numbers
- Home address
- Race
- Religion
- Political Beliefs
- Age
- Sex, gender and sexual orientation
- Fingerprints, blood type and other inheritable characteristics
- Health care status or history
- Educational, financial, criminal or employment status or history
- Opinions about an individual
- An individual's personal opinion

Please note that this is not an exhaustive list. Additional information may be personal if it is recorded information about an identifiable individual.

Sometimes public bodies may share information that is de-identified or partially de-identified. For example, they may share statistics about individuals. If there is no possible way to use the information to identify individuals, an ISA is not required. However, sometimes statistical information may contain enough details to draw conclusions about individuals. If you are not sure, we encourage you to contact the ATIPP Office for assistance.

## Purpose of an ISA

An ISA is an important tool for:

- documenting the reasons for sharing personal information
- demonstrating compliance with ATIPPA, 2015 and other legislation when required;
- outlining each party's responsibilities respecting the handling and security of personal information;

An ISA does not provide the authority to share personal information. Rather, it documents the authority to share information and the commitments made by the parties on how that information will be collected, used and disclosed.

## Before drafting an ISA – Start a Conversation

The first step in creating an ISA is to have a conversation with the other public body you will be sharing information with. Having these discussions up front will help facilitate the drafting process. We recommend you consider the following questions in your initial discussion. You may not have all the answers initially. This is not an exhaustive list of the

mandatory considerations, but rather a list of the high level-questions to support initiating the ISA drafting process:

1. What is the purpose for the information sharing? Does the information need to be shared to accomplish this purpose?
2. What information is going to be shared?
3. Is the information sharing ongoing, frequent or one time?
4. Is the information sharing authorized by ATIPPA, 2015? Is there another Act that authorizes the information sharing?
5. Are the parties subject to the same laws or policies? For example, public bodies are subject to different legislation than private companies.
6. What are the partners' mutual expectations about notification and responses to an information incident/breach?
7. How will you ensure the personal information you are exchanging is accurate and up-to-date?
8. What safeguards are in place to prevent unauthorized collection, use and disclosure of the shared information?
9. How will you dispose of information that has been shared and is no longer needed (i.e. do you both have the same retention schedules)?
10. Do you need to consult with any privacy, security or legal experts before proceeding?
11. Should you conduct a PIA or PPIA before proceeding? It should be noted that for departments, section 72 of the Act requires that a PPIA or PIA be conducted when you are developing a program or service.

The template should be seen as a starting point. Please note that this template can be modified to meet the requirements of the parties. While obligations under the Act must be adhered to, some sections of the template ISA may not be required for very small or one-time exchanges of personal information. Similarly, more detailed may be required for certain types of exchanges of personal information.

## Part Two: Contents of Agreement

### Section 1: Purpose

In this section, you should clearly set out all the purposes for sharing the personal information. This should include a description of the project or service that the ISA relates to. It should also set out why the personal information in question needs to be shared in order for the program to operate.

Clearly identifying purposes is an important part of protecting privacy. If it is unclear why information is collected and why it is shared, there is a risk that too much personal information will be collected or that information will be collected that is not necessary.

Purposes may include:

- Authentication and verification: where personal information is compared and positively confirmed to identify individuals prior to granting access to programs or services;
- Administration of a program or service: where personal information is used for determining or verifying eligibility for programs, administering program payments or overpayments, issuing or denying permits/licenses, etc.;
- Compliance/regulatory activities: where information is used to detect fraud or possible abuses of programs or services; or
- Criminal investigations: where the information is used for purposes related to investigations and enforcement in a criminal context.

Please note that these are examples only – there may be many other different reasons why information is being shared – the key is to identify them.

### Section 2: Authority to Collect, Indirectly Collect, Use or Disclose Personal Information

Any collection, use or disclosure of personal information must be clearly authorized under the Act. The ISA should set out the authority for any collection, use and disclosure of information.

#### Collection:

Under the Act, information can only be collected for the following reasons:

- 61(a) the collection of information is expressly authorized by or under an Act;
- 61(b) that information is collected for the purposes of law enforcement; or
- 61(c) that information relates directly to an is necessary for an operating program or activity of the public body.

If you are citing 61(a) as the authority, you should also cite the other Act you are referring to, including the specific section of that Act which authorizes collection.

**Indirect Collection:**

Under the Act, personal information is generally collected directly from the individual the information is about. If you are collecting personal information from another source, you need to cite the authority for the indirect collection.

Indirection collection is allowed under the Act in the following circumstances:

- 62(a): another method is authorized by the individual, the Office of the Information and Privacy Commissioner, or an Act or regulation;
- 62(b): the act would allow disclosure of the information under section 68-71; or
- 62(c): the information is collected for an honour or award; for a court, judicial or quasi-judicial tribunal; for collecting a debt or fine; or for law enforcement

If you are citing 62(a) as the authority and referring to an Act or Regulation, you should also cite the other Act or regulation, including the specific section of that Act which authorizes indirect collection.

**Use of Information:**

The ISA should identify the authority for using the information. Under the Act, personal information may be used for:

- 66(1)(a): for the purpose it was compiled or for a consistent purpose;
- 66(1)(b): where the individual has identified the information and consented to its use; or
- 66(1)(c): for a purpose for which that information may be disclosed under sections 68 to 71.

Please note that for post-secondary institutions, there are some rules around using personal information for fundraising activities. These can be found in section 67.

**Disclosure of Information:**

The ISA should set out the authority for disclosing information under section 68, 70 or 71 of the Act. These sections of the Act authorize the disclosure of personal information for various reasons, including if another Act authorizes/requires the disclosure. If you are citing paragraphs 68(1)(d) or 68(1)(r) as your authority for disclosure, you should also cite specific sections of the Act or Regulation that provides the authority.

It should be noted that if two public bodies are involved in an exchange of information, you may need to cite two kinds of authority for the same exchange. For example, if Public Body A is providing a list of personal phone number to Public Body B, you need to cite

the authority for disclosure for Public Body A and the authority for collection for Public Body B.

### **Section 3: Information to be Exchanged and Mechanism for Exchange**

To complete this section you should refer to Schedules A, B and C of the ISA Template.

#### **Schedule A:**

Schedule A requires you to list each piece of information being disclosed, the individuals who will use the information, and the purpose of disclosing the information.

#### **Schedule B:**

Schedule B requires you to list all personal information being disclosed, the format in which personal information is being disclosed (e.g. paper, excel spreadsheet, etc.), and the manner in which personal information will be disclosed (e.g. email, registered mail, secure transfer, etc.).

#### **Schedule C:**

Schedule C should set out the safeguards that are in place for the transfer and retention of the personal information in question. For more information about safeguards, we encourage you to consult the ATIPP office or refer to the [Protection of Privacy Policy and Procedures Manual](#).

While all the personal information listed in the Schedules should be included as part of the ISA, feel free to modify the schedules as appropriate. For example, if there is a large amount of personal information being exchanged, it may be easier to combine Schedules A and B. Furthermore, if the ISA involves personal information being transferred in various ways or will be stored differently, it may be appropriate to include several versions of Schedule C to capture the different types of transfer or storage locations.

### **Section 4: Confidentiality, Use and Disclosure**

Section 4 of the ISA template establishes that the information will only be used for the purposes set out in the ISA. It also includes an agreement that only those individuals who need access will have it, and that they will only have access to the personal information they need (for example, if a file contains name and phone number but a particular employee only requires name, they will only have access to name).

When employees have access to personal information, public bodies must also ensure that access is removed if an employee leaves the position which required them to have access. In Schedule D, you should set out any policies or processes you have in place to remove employee access when it is no longer required.

## **Section 5: Information Management and Technology**

To complete this section, we recommend speaking to your Information Management Division to find out what policies are in place, including retention schedules required for Schedule G.

Please note that this section refers to a number of different Acts and policies. You should check that each of these Acts and policies applies to your public body; if they do not apply references to them should be removed.

In paragraph 5.4 you should set out who is responsible for information at various stages in the project.

Paragraph 5.9 requires parties to conduct a periodic review of Information Management Practices. You should consider whether these reviews should be separate or joint, and the appropriate timeframes for these reviews. A short term project may not require a review, but a long term project with frequent changes may require frequent reviews on an ongoing basis.

## **Section 6: Ensuring Data Protection**

This section sets out a number of obligations of each party to ensure the personal information involved is protected.

Section 6.2 obligates each party to advise of changes to employees, agents or contactors who will receive the personal information. The paragraph states that each party should be notified of changes within 24 hours. However, a shorter time frame may be appropriate where personal information is very sensitive. Similarly, a different time frame may be appropriate for paragraph 6.3.

Section 6.4 states that personal information will be kept inside of Canada. At certain times public bodies may choose to use a service that will store information outside of Canada – there is no requirement in the Act to store information within Canada. However, there is an increased risk to storing information outside of Canada if the foreign jurisdiction has weaker privacy legislation, or different intelligence legislation. Furthermore, if the information is stored in the European Union, there may be heightened privacy requirements under their General Data Protection Regulation (GDPR). Before storing information outside of Canada we recommend that you contact your solicitor to discuss these issues.

Section 6.6 sets out an obligation for parties to provide each other with activity reports. The parties should discuss what information should be contained in activity reports and how often they should be exchanged.

Section 6.7 requires parties to ensure that training is available to employees. All employees should be aware of general privacy requirements. The ATIPP Office can assist in providing general privacy training to public bodies. However, system-specific training may also be appropriate, and the parties should discuss what type of training should be made available.

### **Section 7: Accuracy**

The Act requires public bodies to make reasonable efforts to ensure information is accurate and complete where the information is being used to make a decision about the individual.

In addition, individuals can formally make requests for correction of personal information – any party with access to the information is obligated to respond to those requests appropriately.

This section ensures the parties will meet their obligations outlined in the Act.

### **Section 8: Amendments**

This section simply allows the parties to modify the agreement where both parties agree. It should be noted that any amendments must still ensure that the information is handled in accordance with ATIPPA.

### **Section 9: Auditing Requirements**

Auditing processes help ensure that the parties to an agreement adhere to the terms and conditions of that agreement. These processes ensure that the public body can audit the records to ensure that the agreement is being adhered to.

The parties should discuss an appropriate audit process and schedule. This section may be modified depending on what the parties decide.

### **Section 10: Expiry**

This section sets out when the ISA will expire, and notes that a review of activities is required before renewal.

### **Section 11: Coordinating Office**

This section identifies who the parties can consult with in the event that there is a dispute about the obligations of the parties under ATIPPA.

### **Section 12: Notices**

This section establishes how the parties will communicate.

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](mailto:ATIPPOffice@gov.nl.ca)