Yukon

INFORMATION SHARING AGREEMENTS

TABLE OF CONTENTS

INFORMATION SHARING AGREEMENTS

Purpose

This document provides guidance for public bodies and organizations that are interested or required to share personal information.

What is Information Sharing?

Public bodies routinely collect information as authorized by the legislation governing programs, to conduct activities and provide services to the public. When sharing information between a public body and another public body or other organization, an Information Sharing Agreement (ISA) provides a written documentation that outlines the legal authorities for collection, use and disclosure when sharing information to ensure compliance with the Access to Information and Protection of Privacy (ATIPP) Act. An ISA outlines each organizations data protection practices and is used to ensure disclosures are authorized and over-collection of information does not occur.

What is an Information Sharing Agreement?

The Treasury Board of Canada Secretariat's Guidance on Preparing Information Sharing Agreements Involving Personal Information defines an information sharing agreement as a written record of understanding between government parties that outlines the terms and conditions under which personal information is shared between the parties. An adequate information sharing agreement should be in place between the parties to protect the personal information and personal health information involved and to ensure compliance.

Sharing may occur as a one party transfer, two party reciprocal exchange, and may occur as a single event or a regular on-going disclosure.

ISA examples:

One party transfer: one party is disclosing information, while the other party is collecting

Two party reciprocal exchange: both parties disclosing and collecting information.

Entering into a new Information Sharing Agreement may affect a public body's Personal Information Maps, which should be updated for each new disclosure.

When is an information sharing agreement required?

By conducting a Personal Information (PI) Map or Privacy Impact Assessment (PIA), a public body will identify disclosures to other public body's or organizations. Anytime a public body elects to share information, they should create an Information Sharing Agreement to provide a written agreement between the parties.

In order to ensure compliance with the ATIPP Act, a public body should identify the collection, use and disclosure of personal information, prior to engaging in the transfer of information to ensure legislative authority exists.

In each case, each party should review the need to collect personal or identifiable information to meet their objectives.

All ISA's should not exceed a maximum 3 year term, to ensure each party is conducting a periodic review and evaluating whether an ISA is still necessary.

Determining Need

Is there legal authority?

In some cases, sharing may be permitted under an Act, but may not be necessary and is at the public body or organization's discretion.

Is there a clear and justifiable reason to share?

Public bodies must ensure that the purpose to collect is justifiable and that unauthorized disclosure or unauthorized or over-collection does not occur.

Administrative convenience (collecting from another public body, rather than directly) or historical sharing is not a reason to justify information sharing. Collecting personal

information from another organization must be directly related to a program or activity the recipient is mandated to administer. Information should not be shared because it may be useful or is good to know.

Are there alternatives to sharing?

Sharing personal information is not required in all cases, and alternatives should be evaluated to reduce or eliminate risks to privacy.

De-identifying information may be a useful alternative, where identifiable personal information is removed from the information being disclosed. The disclosing party should ensure that the possibility to data-link cannot occur, and the ISA should provide written confirmation that the collecting party will not attempt to data-link to identify individuals.

Summarizing or aggregating data to provide information without identifiers are other recommended options.

In all cases, it's recommended to push information to another public body or organization in a secure manner, rather than pull from access to a system or database to reduce security risks.

Accuracy

The disclosing party must ensure they are disclosing accurate information in the time frame indicated by the agreement. The disclosing party should take care to provide accurate, complete and quality data as required for the identifying purpose. Prior to entering into an ISA, both parties should ensure the quality of data meets the intended use.

If a public body receives a Personal Information Correction Request that will affect the information sharing, they should respond within the time frames set out in the ATIPP Act and provide notifications as required.

Risk Assessment

Has a PI Map been completed for the program to evaluate the disclosure of PI?
Has a PI Map been completed for the program to evaluate the collection and use of PI?
Has a Privacy Impact Assessment been completed on the program the recipient may use to store and use the PI?

Supporting Documents

Documents which may assist public body's due diligence to evaluate and measure the risks of information sharing:

- Written proposal with justification outlining the benefits and risks of sharing
- Supporting legal analysis
- Privacy Impact Assessment(s) and Security Threat Risk Assessment (STRA)
- Risk mitigation plan

DRAFTING AN INFORMATION SHARING AGREEMENT

Drafting an Information Sharing Agreement may require with guidance from program staff, project managers, Designated Privacy Officers, Access and Privacy Officer (HPW), Information Management staff, Legal counsel, and IT staff (Systems Administrator, Security Specialist).

When drafting an ISA,

- Be specific and precise
- Use plain language and ensure terms are clearly understood
- Build in flexibility to allow for amendments
- Published to allow for transparency

Title

When creating the title, be clear and specific and choose a name that speaks to the purpose of the agreement.

Parties

Identify parties to the agreement that are disclosing the personal information and the collecting party or parties.

Naming Conventions

Follow the naming conventions for government consistency:

Acronym (ISA) – Department Acronym (Ex: HPW) – Year – Number consecutively

ISA-XXX-20XX-XX

Example: ISA-HPW-2020-03

1 Accountability

Identify individuals from all parties who would be responsible for monitoring the implementation of the agreement's terms and conditions. This person will assume responsibility for privacy, security, and confidentiality issues (responding to a breach) and compliance with legislation.

Examples:

- Head of a Public Body, or
- Designated Privacy Officer with delegated responsibilities

2 Purpose of Agreement

Clearly identify the purpose of which the information is required and sharing is necessary to meet the program or activity objectives.

State:

- Type and minimum amount of information being disclosed
- Why the information currently needs to be shared between the parties
- Why personal identifiers are required – complete list in Appendix A
- What the original purpose for collection was
- Why indirect collection is required
- The advantages of sharing the information rather than utilizing alternative methods of achieving the same objectives
- All primary and secondary uses – will the collecting party be disclosing to a third party?
- Restrictions that may apply to one, some or all the information being disclosed

Examples:

- Program evaluation
- Audit
- Research
- Statistical Analysis
- Administration of program or service – personal information is used for determining or verifying eligibility for programs, administering program payments or overpayments, issuing or denying permits/licenses, processing appeals, etc.

- Compliance/regulatory activities – where information is used for detecting fraud or possible abuses of programs or services, harassment, etc. resulting in administrative consequences such as fines, discontinuance of benefits, audit of personal files or claims.

3 Authority

3.1 Identify authority to disclose information

Cite a specific section of legislation that gives you legal authority to disclose the information. Note: Limit the disclosure of information to what is absolutely necessary for the purpose identified in 2, Purpose of Agreement.

Example:

- Identify the governing Act for the program or activity under which the information was originally collected and any section that speaks to disclosure
- Identify the section of the Access to Information and Protection of Privacy Act that speaks to the disclosure

3.2 Identify authority to collect information

Cite a specific section of legislation that gives you legal authority to collect the information. Note: Limit the collection of information to what is absolutely necessary for the purpose identified in question 2, Purpose of Agreement.

3.3 Identify roles and uses of the information

Cite a specific section of legislation that gives you legal authority to use the information.

List users (by position title) that will have access to the information, including listing the types of information each user can access; the position(s) responsible for disclosing the information, and the position(s) responsible for collecting.

If the party collecting and using the information intends to disclose to a third party at the time the agreement is drafted, identify the third party and roles.

4 Protection of Privacy

4.1 Limitations on use or disclosure

Describe the authorized use and limits on further use (ex: third party disclosure).

- Identify how the information shared is to be used
- Secondary uses
- Third Party disclosures

Limitations or prohibitions on secondary uses and disclosures to a third party must be clearly stated in the agreement and agreed upon by both parties to avoid any conflicts or issues with non-compliance. Parties should review secondary use or disclosures against each party's legislation and the Access to Information and Protection of Privacy Act.

The party which holds custody of the original information, can impose prohibitions on any type of use to ensure security of the information. For example: If the collecting party wishes to share with a party not originally identified, they may wish to submit an amendment to the original agreement for review and evaluation.

Limitations to use reduces the possibility of using information in a way other than that described in 2 Purpose of Agreement, and mitigates the risk of termination of the agreement due to non-compliance.

4.2 How the information will be shared

Each party transferring data should ensure the most secure avenue is utilized. Provide details on how information will be transferred, including safeguards:

Example:

- Secure file transfer
- Encrypted portable drive
- Shared folder with limited individual access

Identify the frequency in which the information will be shared:

Examples of frequency:

- Real time
- Batch process
- Ad hoc
- Weekly
- Monthly
- Quarterly

Granting one party access to another party's database, system or program is not advised.

It is strongly recommended for ministerial public bodies to complete a Privacy Impact Assessment (PIA) and Security Threat Risk Assessment (STRA) if this is the requested option.

4.3 Data Quality/Accuracy

Identify the parties who have custody and control of the information and how accuracy will be measured.

4.4 Retention and Disposal

Provide the retention and disposal schedule information for each party. If applicable, attach as an appendix.

4.5 Individual Access

Speak to any limitations on individuals accessing the information.

4.6 Safeguards

Detail what physical, technical and administrative safeguards will be in place to safeguard the information and ensure only authorized users will have access to it.

Administrative measures: policies and procedures to protect the privacy and security of personal information, staff training on privacy, limiting access to information on a "need-to-know" basis, and the reliability of employees having access to the information.

Technical measures: passwords, audit trails, encryption, firewalls and other technical security safeguards to minimize the risk of unauthorized individuals accessing personal information.

Physical measures: such as locked files, restricted access to offices and other areas where personal information is stored.

4.6.1 Privacy Breaches

Detail what the procedures are in the event of a privacy breach, including policies and procedures in place for responding and investigating the breach.

Ex: Immediately upon discovering or suspecting a breach may have occurred, the employee must contact the Designated Privacy Officer listed in section 1 Accountability.

List Legislation, Regulation, policies, and other guidance documents related to the public body, as well as the other party's response procedures.

5 Terms of Agreement

5.1 Term of Agreement

The term of the agreement should not exceed a maximum of 3 years, to allow for the review of the ISA.

The start date should occur after both parties have signed and agreed to all the terms.

5.2 Modification or Termination of Agreement

Outline how an amendment or termination would occur.

Upon written mutual agreement, both parties may terminate this agreement before the end date. Provide clauses or reasons for amending an agreement.

Example:

- To extend the date; up to a maximum of 3 years; or to extend the original agreement past the original 3 year end date. If the latter, each party must

undertake a review to ensure the terms of the agreement are still relevant for the purpose
- Significant program changes of either party
- The addition or removal of subsequent use
- The addition or removal of a third party disclosure

5.3 Termination for Non-Compliance with Agreement

Provide terms for determining non-compliance, and notification to terminate to the other party.

5.4 Personal Information Maps

Attach the completed Personal Information maps as an appendix.

6 Parties

Provide signing block for each party. Add more as required.

INFORMATION SHARING AGREEMENT TRACKING LOG

Purpose

In order to ensure compliance with the terms of the Information Sharing Agreement, it is recommended that disclosures or exchanges of information are adequately recorded on the ISA file by the disclosing institution, so that recipients of any incorrect information can be informed and provided with accurate revised information.

- Use the Information Sharing Agreement Tracking Log as a cover page to document disclosures
- Watermark documents as Confidential, if sharing identifiable information
- Add the ISA number into the header or footer of the document along with the date

Completing the Tracking Log

Information Sharing Agreement Number

Enter the ISA number related to the disclosure.

Date of Disclosure

Add the date of the disclosure.

Authorized Disclosing Official

Add the name of the disclosing official authorized in the agreement, and add signature above. It may be the Head of the Public body, Designated Privacy Officer, or other individual as outlined in the ISA terms.

Authorized Collecting Official

Add the name of the disclosing official authorized in the agreement, and add signature above.

Disclosing

Each party transferring data should ensure the most secure avenue is utilized. Provide details on how information will be transferred, including safeguards:

Example:

- Secure file transfer
- Encrypted portable drive
- Shared folder with limited individual access

AMENDING AN INFORMATION SHARING AGREEMENT

Purpose

An Information Sharing Agreement can be amended at any time. An amendment is used to document any change to the agreement and requires the approval of both parties to come into effect.

Using the Information Sharing Agreement Amendment template, provide clauses or reasons for amending or terminating an agreement.

Example:

- To extend the date; up to a maximum of 3 years; or to extend the original agreement past the original 3-year end date. If the latter, each party must undertake a review to ensure the terms of the agreement are still relevant for the purpose
- The addition or removal of subsequent use
- The addition or removal of a third party disclosure
- Termination of the agreement for non-compliance

Terminating an Information Sharing Agreement

Drafting an Amendment for Termination

- Add ISA #
- Add start date of the ISA
- Add date of termination and use the following terms

This amendment is for termination of the Information Sharing Agreement under section 5.3 Termination for Non-Compliance.

[List reasons for termination or termination for non-compliance]

On this date [add date], [Name of Party] will cease all information sharing with [Name of Party].

[Add any termination clauses, return of information, and destruction of information if applicable]