Best Practices for Information Sharing Agreements

This document outlines best practices for developing information sharing agreements when sharing personal information as defined by The Freedom of Information and Protection of Privacy Act (FOIP) and The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP).

Office of the
Saskatchewan Information
and Privacy Commissioner

Best Practices for Information Sharing Agreements

What is Information Sharing?

The Government of Alberta issued a resource titled, *Guide for Developing Personal Information Sharing Agreements*. The Guide defines information sharing as follows:

> "**Information sharing**" means the exchanging, collecting, using or disclosing of personal information by one public body or other organization with another public body or other organization for certain purposes. The sharing may be carried out using any transmission method and may take place over any time period.

Further, the Guide clarifies the roles of each public body as follows:

> If a public body discloses personal information under an information sharing agreement, it is a **source** of personal information and must comply with the disclosure provisions of the FOIP Act…The data sharing agreement is the means for safeguarding the personal information once it has been disclosed.
>
> If a public body collects personal information under an information sharing agreement, it is a **recipient** of personal information and must comply with the collection provisions of the FOIP Act…
>
> If a public body which is a **recipient** of personal information uses the information that is has collected through the arrangement, it must comply with the accuracy and use provisions of the FOIP Act…

Personal information is defined in subsection 24(1) of *The Freedom of Information and Protection of Privacy Act* (FOIP)/23(1) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

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.

When is an Information Sharing Agreement Required?

Whenever a public body is planning to engage in information sharing, it is best practice to have a written information sharing agreement in place that conforms to the best practices described in this resource. Public bodies should also ensure that all collections, uses and disclosures of personal information in the information sharing activities are authorized by FOIP or LA FOIP.

Several subsections in FOIP, LA FOIP and their Regulations stipulate that an agreement must be in place for information sharing (example: information sharing for the purposes of a common or integrated service described in section 17.1 of the FOIP Regulations/10.1 of LA FOIP Regulations). When this occurs, the agreement should be in writing and follow the best practices outlined in this document. In some instances, the regulations describe what an information sharing agreement should contain ; however, it is also best practice to include all elements described in this resource as well.

In 2017, amendments were made to FOIP, LA FOIP and their Regulations. The amendments introduce the concept of an information management service provider (IMSP). See the definition in subsection 2(1)(e.1) of FOIP/ FOIP, LA FOIP and the Regulations. Public bodies are required to have an information sharing agreement in place when engaging an IMSP. See section 13.1 of the FOIP Regulations/8.2 of the LA FOIP Regulations.

Why is an Information Sharing Agreement Important?

Tom Wright, a former Ontario Information and Privacy Commissioner, pointed out in his paper *Model Information Sharing Agreement* that:

> Sharing personal information between two organizations runs counter to two of the most fundamental principles of data protection – that personal information should be collected directly from the individual to whom it pertains, and should only be used for the purpose for which it was collected (with limited exceptions). Therefore, where possible, sharing should not occur without exploring less privacy-invasive means of meeting a specific objective.

What are Best Practices for Creating Information Sharing Agreements?

The Institute for Citizen-Centered Service (ICCS) produced a set of *Guidelines for Best Practice* as they relate to Government-to-Government personal information sharing agreements. This tool highlights six best practices and is intended to address the need to better manage privacy risks and to achieve greater transparency, control and accountability.

The following are the recommended six best practices covering the lifecycle of an information sharing agreement (ISA). The first three steps contain best practices recommended before proceeding with an ISA:

Step One: Identify Need and Determine Risk Factors

Essential Requirements: Sharing personal information under your care should only be considered when both the following circumstances exist:

- You have legal authority.
- There is a clear justifiable need in the current period of time.

Other important requirements include:

- Security measures taken to safeguard information such as the location of databases and the method of transfer.
- Consultation with your legal and privacy experts covering the framing of the ISA to the implementation and follow-up of the agreement.
- Justifying the ISA by explaining exactly why personal information must be shared and specifying what information is to be included.

Best practices include:

- Obtaining consent and providing notice.
- Restricting the amount of personal information collected to a minimum.
- Carrying out the collection, use and disclosure of personal information on a need to know basis.
- Ensuring that the information is "pushed" (given to the other party) and not pulled (taken by the other party).
- Conducting a preliminary assessment of risks.

Step Two: Explore Alternative Strategies

Sharing personal information is a last resort because of the inherent privacy risks. Be sure to explore whether objectives of the program or service can be accomplished without the disclosure of personal information. Alternatives include:

- A summary of information rather than specific identities.
- De-identified information (removing all personal identifiers).
- Aggregated data such as a range of ages instead of specific ages.

Step Three: Conduct Risk Assessment

Take a detailed look at the privacy risks using recommended tools that include:

- A Privacy Impact Assessment (PIA) that measures compliance not just against established legal standards but universal privacy principles.
- Communications planning that includes public reporting.
- Consultation with your departmental privacy, security and legal experts and the privacy official for your jurisdiction (such as a Privacy Commissioner or Ombudsman).

Steps four through six contain best practices after deciding to proceed with an ISA:

Step Four: Document

It is best practice to document your decision to proceed, justifying the decision and outlining a plan to mitigate risk. Documentation should include, but not be limited to a justification, cost benefit analysis and a Privacy Impact Assessment and a risk mitigation plan to address all risks. It is important that you also ensure that the ISA is supported by sound information management practices.

Step Five: Create an ISA

Best practices in creating an ISA include:

- Appointment of an oversight body consisting of people in your department familiar with privacy and security issues who can offer guidance and support.
- Ensuring that privacy and legal experts review and approve each ISA.
- Using plain language to ensure all terms are fully explained.

Your ISA should include these key components:

- Identities, roles and responsibilities of the parties
- What information is being disclosed and collected and the purpose(s) of each
- The frequency and duration of information exchanged
- The legal authority to disclose and collect information
- The methods and security measures for transferring and storing the information
- Procedures in the event there is a privacy or security breach
- Limitations for collection, use, disclosure and retention
- Provisions for accuracy of the information
- Indemnification
- Compliance monitoring

Step Six: Monitor and Follow Up

It is best practice to monitor the effectiveness of the agreement. This is done through audit trails, self-assessments, audits, verification systems, certificates of assurance and measurement techniques related to your government's obligations in the agreement.

These best practices are consistent with those recommended by the Treasury Board of Canada in its Guidelines for federal government organizations titled, *Guidance on Preparing Information Sharing Agreements Involving Personal Information.*

In December 2008, the Access and Privacy Branch with the Ministry of Justice produced a resource titled, *Personal Information Sharing Agreements (Government to Government) Best Practice Guidelines.* The Guidelines present the same six best practice steps noted above.

Other Information and Privacy Commissioner's across Canada also recognize the need for best practices and recommend similar practices in their jurisdictions. For example, previous British

Columbia Information and Privacy Commissioner, Paul Fraser, Q.C stated the following in his Investigation Report F10-02:

> [118] To be FIPPA compliant, public bodies must use information-sharing agreements to govern the disclosure of personal information from one entity to another. An information-sharing agreement sets out the terms and conditions for how the personal information will be collected, used, and disclosed by the entity receiving the data. Information-sharing agreements also enhance the transparency and accountability of public bodies with respect to data flows of personal information and how the privacy of individuals is being protected. Government recently recognized their fundamental importance in a statutory requirement for information-sharing agreements with respect to disclosures from health information banks [E-Health Act, s. 19].
>
> …
>
> [120] We conclude that there are information-sharing agreements in place for most external disclosures **but that they do not always impose specific or detailed standards for the protection of the privacy and security of personal health information. The agreements should not merely reference broad legislative standards, but specifically state the obligations of the recipients of the data to protect it.** Given the particular sensitivity of personal health information, all information-sharing agreements should specify high standards for privacy and security, including encryption, secure storage, retention schedules, and requirements for secure disposal of personal information.
>
> **Recommendation 8**
>
> **VCH should ensure that all information-sharing agreements require recipients of personal health information outside VCH to maintain specific reasonable standards of privacy and security protection**
>
> [emphasis added]

Further, the British Columbia Information and Privacy Commissioner's office released a resource titled, *Managing Contracts and Information Sharing Agreements (ISAs).* In that resource it states:

> ISAs usually:
>
> 1. Define what personal health information means.
> 2. Describe the purpose for data sharing.
> 3. Reference all applicable legislation that provides the legal authority for collection, use, and disclosure of personal information.
> 4. Establish an understanding of who has custody and control.

5. Identify the type of information that each party will share with each other.
6. Identify the uses for the information and limitations on the uses to the specified purpose.
7. Describe who will have access and under what conditions.
8. Describe how the information will be exchanged.
9. Describe the process for ensuring accuracy.
10. Describe the process for managing privacy breaches, complaints, and incidents.
11. Identify retention periods.
12. Identify secure destruction methods when retention expires.
13. Describe the security safeguards in place to protect information.
14. Describe termination of the agreement procedures.

Consistent with other jurisdictions, we expect Saskatchewan government institutions and local authorities to establish similar best practices when they enter into information sharing agreements.

CONTACT INFORMATION

If you have any questions or concerns regarding information sharing agreements, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

webmaster@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC