Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

GUIDANCE DOCUMENT

INFORMATION SHARING AGREEMENTS

SEPTEMBER 2017

CONTENTS

What is information sharing? 1
What are ISAs? 2
When do I need an ISA? 2
What should be included in an ISA? 3

PURPOSE OF THIS GUIDANCE DOCUMENT

This guide is for public bodies and organizations that are interested in sharing personal information. It describes information sharing and explains the role and value of information sharing agreements (ISAs) to ensure compliance with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). This guide also recommends provisions that should be included in an ISA.

WHAT IS INFORMATION SHARING?

Information sharing is the disclosure of personal information from a public body or organization to another party, which then collects and uses that information. This can be a one-way transfer or a reciprocal exchange, a single event or a series of regular transactions.

Public bodies and organizations share information for numerous reasons, such as administrative efficiencies, evaluating and improving programs and services, and creating new opportunities for collaboration.

While there may be benefits to information sharing, Canada's information and privacy commissioners caution that it can raise privacy concerns. Potential issues include a lack of transparency with affected individuals, inaccuracy of personal information, use of information for secondary purposes, security breaches, and the potential for surveillance and discrimination.[1]

For these reasons, public bodies and organizations should carefully consider whether the purposes for sharing are fair and ethical. Public bodies should be open about the nature of their information sharing initiatives, while organizations that share personal information should be prepared to demonstrate compliance with PIPA.

[1] *Protecting and Promoting Canadians' Privacy and Access Rights in Information Sharing Initiatives*. A joint resolution of Canada's Information and Privacy Commissioners and Ombudspersons, January 2016. Retrieved from https://www.oipc.bc.ca/media/16825/2016-01-25-information-sharing-resolution-eng.pdf

	Remember, whether you represent a public body or an organization, your information sharing program must comply with privacy legislation.

WHAT ARE ISAs?

ISAs are formal agreements that describe the terms and conditions for sharing personal information. Examples of ISAs include agreements with service providers, researchers, or other public bodies or organizations.

These agreements document the roles and responsibilities of the parties involved and are an important measure of accountability. They guide the actions and decision-making of public bodies or organizations so parties to ISAs know when and how that sharing can occur.

ISAs can also impose further restrictions on using shared information than required by law. For example, the disclosing party may seek assurance that the shared information will not be used or disclosed beyond the stated purposes of the ISA.

ADVICE FROM THE COMMISSIONER	If you are considering disclosing personal information, you must ensure that you have the legal authority to do so. For public bodies, these authorities are detailed in sections 33.1, 33.2, 33.3, 35 and 36 of FIPPA. For organizations, they are found in sections 17 to 22 of PIPA.
	Once your public body or organization has determined it has authority to share information, it must do so responsibly. You must make reasonable security arrangements to protect the data (pursuant to s. 30 of FIPPA and s. 34 of PIPA) and to adhere to other legislated requirements.

WHEN DO I NEED AN ISA?

ISAs are usually prepared when a public body or organization plans to share personal information on a recurring basis.

However, ISAs can also be prepared for one-time transfers or exchanges of personal information. In these cases, the need for an ISA or similar record will depend on the purpose of the sharing and the volume and sensitivity of the information.

ADVICE FROM THE COMMISSIONER	If your public body or organization is contemplating the disclosure of a large amount of personal information, we recommend that you document the purpose and authority for the disclosure and explain any additional expectations or requirements on the subsequent use of that information.

WHAT SHOULD BE INCLUDED IN AN ISA?

In a few instances, the contents of ISAs are prescribed by legislation.[2] FIPPA requires ministries to prepare these agreements in accordance with the directions of the minister responsible for the Act.[3] As of the date of this publication, the directions to ministries have not been issued.

In general, ISAs should include or address the following provisions:

1. A statement of the purpose for the disclosure.
2. The legal authority to disclose the data for that purpose and the legal authority for the collection by the public body or organization to which the data is being disclosed.
3. A description of the data that will be disclosed that is as specific and comprehensive as possible (i.e.: the nature and type of data elements, as well as the quantity of data).
4. A description of how the data will be disclosed (such as direct access to a database or a specific data flow versus indirect access via email from the originating party, and in response to a request or at regular intervals).
5. Where possible, a description of who within a public body or organization will have access to the data and any other disclosure restrictions. This could enable the disclosing public body or organization to limit further disclosure of the shared data.
6. A description of the authorized use of the data and limits on further use of the data.
7. A clear statement about who has custody and control of the data. This may be needed because parties to the agreement will likely have custody of the shared data, while one party could maintain control over managing that information.
8. An undertaking to protect the data in a certain manner (i.e.: particular administrative, technical, and physical safeguards to protect the data adequately given its sensitivity).
9. A description of any restrictions on the storage and access of personal information outside of Canada (FIPPA includes a requirement to keep personal data in Canada).
10. A description of the process to ensure accuracy of the data, including the process to update and correct personal information if needed.

[2] For example, s. 19 of the *E-Health Act* and s. 67 of the *Coroners Act*, prescribe the content for ISAs entered into under those statutes.
[3] Section 69(5.7)

11. A specific retention period and directions on secure destruction when the retention period expires.
12. A description of the process for managing privacy breaches, complaints, and incidents.
13. Methods for monitoring compliance with the ISA and consequences for non-compliance.
14. Term of the ISA and process for amendment and renewal.

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867
info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy