

Privacy Guide for Personal Information Exchange Agreements

This guide and the “Privacy Checklist for Personal Information Exchange Agreements” were prepared by the Office of the Information and Privacy Commissioner of British Columbia for use by public bodies entering agreements to exchange personal information.

Information exchange or data sharing (including data matching) involves at least two parties - the source of the information and the recipient. In effect, the source in this arrangement **discloses** the information to the recipient, and the recipient **collects** the information from the source. All parties to a particular arrangement may be both sources and recipients.

When a public body is either the source or the recipient and the information shared is personal information, then “Part 3 - Protection of Privacy” of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 (the Act) applies to the transfer of information¹. In particular, the purposes for which and how the personal information is collected, the accuracy of the personal information, the right to request correction of personal information, how the personal information is protected, retention policies, and the information uses must all comply with Part 3 of the Act².

A data sharing agreement sets out the parameters of the data sharing arrangement. From a privacy perspective, the general idea is to ensure that the public are aware of the how their personal information is being used and to ensure that these uses and, in general, the entire arrangement does not contravene the Act. Therefore, the more information the agreement contains about the arrangement and the more specific this information is, the better informed the public will be and the less likely their personal information will be used incorrectly. From a privacy perspective, it is desirable to include in the agreement as much of this information as possible.

The following list contains many of the issues that should be considered when drafting or evaluating a data sharing agreement and is meant to serve as a checklist.

1. Statutory Authority for Data Matching

If a public body collects personal information pursuant to a data sharing arrangement, then the public body must comply with section 26 of the Act. If a public body discloses personal information, then the public body must comply with section 33. If a public body does both, then it must comply with both sections 26 and 33.

Wherever possible, the legislation that the public body is operating under should specifically authorize this type of arrangement and use of personal information (subsection 26(a)). Otherwise, the exchange of personal information must satisfy either

¹ The Act does not protect from collection and disclosure information that is not of a personal nature.

² See sections 26-36.

subsection 26 (b) or 26 (c). Whatever the situation, the public body's legal basis for the disclosure, collection, or both should be clearly identified in the agreement.

Clearly identifying the legal authorization for the public body's involvement in the arrangement helps ensure that this use of personal information is authorized by law. It also serves as notice to the public of the authorization.

2. Purpose and Reason for Data Sharing

Identify Purpose and Reason

Clearly identifying in the agreement the purpose and reason for the data sharing arrangement helps the public body to turn its mind to the necessity for the arrangement. This also helps notify the public and contribute to their understanding of why the data sharing is necessary in that situation.

Cost-Benefit Analysis

The public body should consider the costs and the benefits of the data sharing arrangement when it considers whether the arrangement is necessary. If the costs outweigh the benefits, or if there is a better way to achieve the same objective, then it is likely the arrangement is not necessary and should not be instigated.

It may be acceptable in the situation for the public body to address the cost-benefit analysis internally and not include this in the agreement (e.g., the public body internally circulates a background note with the justification for the data sharing). This internal analysis should include why the agreement is necessary and what benefits the public body hopes to achieve from it. It should also mention what effects this will have on personal privacy, whether these effects are outweighed by the benefits, and why.

Research Using Personal Information

Any research using personal information contemplated by the public body or the other parties in the arrangement should also be addressed in the agreement.

3. Elements of Personal Information Shared

The agreement should specify the information that will be shared, the frequency of the sharing, and the method to be used. Again, this helps ensure the public body turns its mind to these issues and that the privacy implications are considered. It also serves as a form of public notice on this issue.

4. Use of Information

The agreement should clearly identify how the personal information shared under the arrangement is to be used. As well, secondary use should be limited, if not prohibited. In addition, the parties to the agreement should be limited to the uses listed. This helps ensure the public body considers how the personal information is to be used and its privacy implications.

5. Notice

Notice to each individual may not be required where there is a general exchange of information. However,

a general notice may be required, for example, when the individual originally provides the information. There is a stronger argument for notifying the individual where the exchange is limited to a certain individual or group.

6. Accuracy and Completeness of Information

The parties should agree that they will verify the information received from a third party independently before they use it to make administrative decisions/action. This means, for example, that when a discrepancy between two sources of information is identified, the recipient will not act on this discrepancy without first checking to see that the information used is accurate and complete.

The agreement should also address what technical standards will be used to ensure data quality, integrity and security. As well, the agreement should identify what record controls will be used. Finally, the agreement should state that no new databanks will be created from the exchange of information.

7. Termination Date

The time period to which the agreement applies should be limited to avoid an exchange of information when it is no longer necessary. If the agreement is anticipated to be long term, the time period should still be limited. However, the agreement should contain a renewal clause if the arrangement is still necessary.

8. Signing Authority and Contact Names

Signing authority for the agreement may be best limited to the minister responsible for the ministry involved in the data sharing arrangement.

The agreement should also contain a contact name and number in case changes to the agreement become necessary. The public can also use this name and number to learn more about the data sharing arrangement.

9. Disclosure

The agreement should place restrictions on disclosure, but it should not be so restrictive as to stand in the way of disclosure required for law enforcement purposes. The objective is to ensure that a recipient who is not a public body covered by the Act is required to treat the personal information it receives with the same sensitivity as is required by public bodies under the Act.

10. Retention and Destruction

The agreement should specify how long the personal information shared is to be kept, and whether the information is to be returned to the source or if it is to be destroyed by the recipient.

Consideration should also be given to the *Document Disposal Act* to determine how it applies to the information collected and retained under the agreement, particularly to that information received and kept electronically.

11. Other Clauses

The other clauses must not require or permit an activity that contravenes the Act.

12. Consultation with OIPC

If OIPC has commented on the agreement to ensure the privacy issues are addressed, the Commissioner may want to consider offering the public body a letter to that effect.