

Government-to-Government Personal Information Sharing Agreements *Guidelines for Best Practice*

CONTENTS

A) Introduction	3
A1. Purpose of the Guidelines	3
A2. Structure of the Guidelines	3
A3. Why the Guidelines are needed	3
A4. History of the Guidelines	3
A5. Who should use the Guidelines	4
A6. How to use the Guidelines	4
A7. Summary of Best Practice Steps	5
B) What are Personal Information Sharing Agreements (ISAs)?.....	8
B1. Is an ISA Mandatory?.....	8
B2. Benefits of an ISA.....	8
B3. Types of ISAs	8
B4. Provincial ISA Guidelines	9
B5. Sample ISA	9
B6. Private Sector Contractors	9
C. Six Best Practice Steps	11
Best Practice One: Identify Need and Determine Risk Factors	12
1.1 What is personal information?	12
1.2 Do you have the legal authority?	12
1.2.1 Legal authority	12
1.2.2 Consent and notice.....	13
1.2.3 Mandatory provision of information.....	13
1.3 When sharing is needed	13
1.4 Justification of Information Sharing Agreement	14
1.5 Preliminary assessment of the risks.....	14
1.5.1 High risk scenarios	15
1.5.2 Potential Information Sharing Arrangements with Greater Sensitivity	15
1.5.3 International transfer	15
1.5.4 Security measures	16
1.5.5 Pushing information	16

Best Practice 2: Explore Alternative Strategies 17

2.1 Summary reporting.....	17
2.2 De-identified information	17
2.3 Aggregated data.....	17

Best Practice 3: Conduct Risk Assessment 18

3.1 Conduct a Privacy Impact Assessment (PIA)	18
3.2 Public reporting and communications.....	18
3.3 Consult departmental privacy, security and legal experts.....	18
3.4 Consult your jurisdiction’s privacy advisor	18

Best Practice 4: Document 19

4. Document your decision	19
---------------------------------	----

Best Practice 5: Create an ISA..... 20

5.1 How to use the template.....	20
5.2 Oversight body.....	20
5.3 ISA approval/sign-off	20
5.4 Ten principles	20
5.5 Plain language	20
5.6 Personal Information Sharing Agreement Template	21

Best Practice 6: Monitor and Follow Up 27

6. Monitor and Follow Up.....	27
-------------------------------	----

APPENDICES 28

APPENDIX A: Privacy laws that apply to personal information under the control of the Public Sector in Canada	28
Appendix B: International Context.....	30
Appendix C: PIA Templates and References	31
Appendix D: Privacy Officials in Canada.....	32
Appendix E: Potential Privacy Risks	33

A) Introduction

A1. Purpose of the Guidelines

Governments have a responsibility to protect the privacy of personal information within their custody and for which they are responsible.

The purpose of these guidelines is to provide a model of privacy best practices for personal information sharing agreements between governments within Canada.

A2. Structure of the Guidelines

The guidelines present six major privacy “best practice” steps, which form the lifecycle of the decision-making process, starting with identifying needs and concluding with the monitoring of agreements.

A3. Why the Guidelines are needed

Today, the Canadian economy, like most world economies, is increasingly dependent upon the transfer of information across borders, known as “transborder data flow”. Much of the transferred data is personal information. This information can be vulnerable to privacy and security breaches in the event appropriate protective measures are not taken.

Such breaches could be in violation of Canadian law. In addition, the consequences for government departments can be severe – including the loss of public trust; complaints and subsequent investigations; and in some cases, the loss of continued program or service funding.

In a recent major audit of transborder data flows conducted on the Canada Border Services Agency by the Federal Privacy Commissioner, Jennifer Stoddart concluded that much can be done to better manage privacy risks and to achieve greater transparency, control and accountability.

To read the full report, visit

http://www.privcom.gc.ca/information/pub/ar-vr/cbsa_060620_e.asp - 001.

These guidelines provide strategies to minimize or eliminate privacy and security risks within personal information sharing agreements.

They also serve to standardize these agreements so that governments in Canada at all levels can avoid duplication of effort and process agreements in a timely and efficient manner.

A4. History of the Guidelines

Privacy and information officials in Canada have long recognized the risks of transborder data flow especially outside of Canada where foreign laws can take precedence.

The comments from David Loukidelis, Information and Privacy Commissioner of British Columbia, generally reflect those of the government privacy community:

"The territorial limits on jurisdiction are very real and therefore threaten the ability of data protection authorities to do their work in the context of international data flows."

(Taken from "Transborder Data Flows and Privacy – An Update on Work in Progress, February, 2006)

In March, 2005, an EKOS Research Associates survey commissioned by the Office of the Privacy Commissioner of Canada, found that 85 per cent of Canadians surveyed reported a moderate or high level of concern about Canadian government agencies transferring personal information to foreign governments.

See the survey findings:

http://www.privcom.gc.ca/information/survey/ekos_e.asp

That same year, at the annual Lac Carling conference, there was agreement on the need for advice and standards on transborder data flows. In response, the Public Sector CIO Council – comprised of federal, provincial, territorial and municipal representation – approved funding to develop such guidance for use by all governments in Canada.

These resulting guidelines were developed under the Council's Privacy Subcommittee.

A5. Who should use the Guidelines

Anyone responsible for consultation, development or management as it relates to a government program or service in which personal information could be, or is being, shared with another jurisdiction should consult these guidelines. Included are CIO offices, privacy advisors and program and service managers.

A6. How to use the Guidelines

These guidelines contain best practices for government to government sharing of personal information but should not be used in isolation.

It is important that you always consult with your privacy and legal advisors to identify, review and consider all laws and policies that may have an impact on privacy and security issues, prior to initiating any agreements. All agreements should also be reviewed and approved by the appropriate privacy and legal experts.

A7. Summary of Best Practice Steps

Here is a brief summary of the six best practice steps outlined in the guidelines.

Steps 1 to 3: The first three steps contain best practices recommended **before** proceeding with an Information Sharing Agreement (ISA).

Step One: Identify Need and Determine Risk Factors

Essential requirements: Sharing personal information under your care should only be considered when both of 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.

(Section 1.5 looks at examples of high risk scenarios and Appendix E lists common potential privacy risks)

Step Two: Explore Alternatives

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. **(Appendix "C" contains a list of PIA guidelines).**
- Communications planning that includes public reporting.
- Consultation with you departmental privacy, security and legal experts and the privacy official for your jurisdiction (such as a Privacy Commissioner or Ombudsman).

Steps 4 to 6: These steps contain best practices *after* deciding to proceed with an ISA.

Step Four: Document your Decision

It is a 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 the 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
- Provision for accuracy of the information
- Indemnification
- Compliance monitoring

(For details, use the template under Section 5.6 filling in text applicable to your circumstances).

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.

B) What are Personal Information Sharing Agreements (ISAs)?

A government-to-government personal information sharing agreement, hereafter referred to simply as an ISA, is an agreement that covers the terms and conditions for the collection, use and disclosure of personal information between government parties.

Three priorities

If you agree to disclose personal information to another government party, an ISA identifies three priority requirements.

- The purpose or purposes for which the collecting party will use the information.
- The legal authority to disclose and collect.
- A commitment that the information will be kept private and secure and that the disclosing party will be notified in advance if the collecting party intends to disclose the information outside the terms of the agreement.

B1. Is an ISA Mandatory?

There may be a legal or policy requirement to develop an ISA. But even if not, an ISA is strongly recommended as a practical and effective risk management tool.

Failure to use an ISA could be viewed by privacy commissioners or the public as an indication of lack of concern about protecting privacy.

B2. Benefits of an ISA

An ISA has a number of benefits that support its use as a best practice. These benefits include:

- Clarification of rights and obligations of the parties
- Compliance with applicable legislation and policies
- Establishment of custody and control
- Limitations on the type, amount and purposes of sharing
- Protocols that cover procedures if anything should go wrong

Details on the creation of an ISA, complete with privacy protection clauses, are contained in Best Practice 5, Create an ISA.

B3. Types of ISAs

Repeated Transfers: An ISA that covers repeated transfers of personal information over a period of time is the most common because it avoids the need for separate agreements for each incidence of transfer.

Case by Case: If information is expected to be transferred only once, a single case ISA can be used.

One-Way Flow: In this agreement, information is flowing from one government body to another. One party is disclosing personal information while the other is collecting.

Two-Way Flow: Two-way agreements provide for the reciprocal sharing of personal information. One government party discloses personal information to another government party for certain purposes. The other government party reciprocates by disclosing personal information it may have about the same, or other, individuals.

Cautionary Note: As a general rule, ISA's should be bilateral, covering both the party disclosing the information and the other party receiving the information. One of the functions of the ISA will be to identify a party's lawful authority to collect or disclose the information in question, what precise purposes the information will be used for, what precise information is required, and what precise security measures will be applied to that information. In a multilateral ISA, there is a risk that unnecessarily vague or broad terms will be used to deal with these issues, in an attempt to make the clauses broadly applicable to all parties.

B4. Provincial ISA Guidelines

Some provinces have produced ISA guidelines relevant to their own circumstances.

British Columbia: [Privacy Guide for Personal Information Exchange Agreements](#)

Alberta: [Guide for Developing Personal Information Sharing Agreements](#)

Ontario: [Model Data Sharing Agreement \(1995\)](#)

You may wish to consult with your own access and privacy office to determine if your jurisdiction has similar guidelines or templates.

B5. Sample ISA

An ISA is in place for the exchange of personal information to carry out the Canada-Alberta Agreement on Labour Market Development. It serves as a sample ISA:

<http://www.hrsdc.gc.ca/en/epb/lmd/lmda/alberta/pdlmdaalberta31.shtml>

B6. Private Sector Contractors

If a private contractor is used to process personal information shared between governments, this should be referenced in the ISA. However, the specific terms under which a private firm carries out this task should be covered in a separate legal contract between the firm and government organization involved.

It is very important that any contract between a government and a third party, where the third party is hired to process personal information in some way, contain specific clauses that detail the responsibilities of the third party. In particular, such contracts should deal with limits on how the third party may use the information, who within the third party is authorized to deal with the information, rules relating to retention and security of the information, and in particular, what right of access to the information the government agency will have and how an individual's right of access to their own information will be administered.

The contract should specify whether the third party is required to comply with the privacy statute that binds the government agency in addition to other laws applicable to the

contractor. As a general principle, government agencies cannot contract out of their privacy obligations.

Your jurisdiction may have procurement laws, policies and guidelines that govern private sector contracts which must be followed if any private firms are used in the sharing of personal information. Consequently, you should check with your own access and privacy office for appropriate guidance on this issue. Relevant web links are as follows:

Treasury Board of Canada Secretariat Guidance Document: Taking Privacy into Account Before Making Contracting Decisions:

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/gd-do/gd-do_e.asp

Alberta Public Sector Outsourcing and Risks to Privacy:

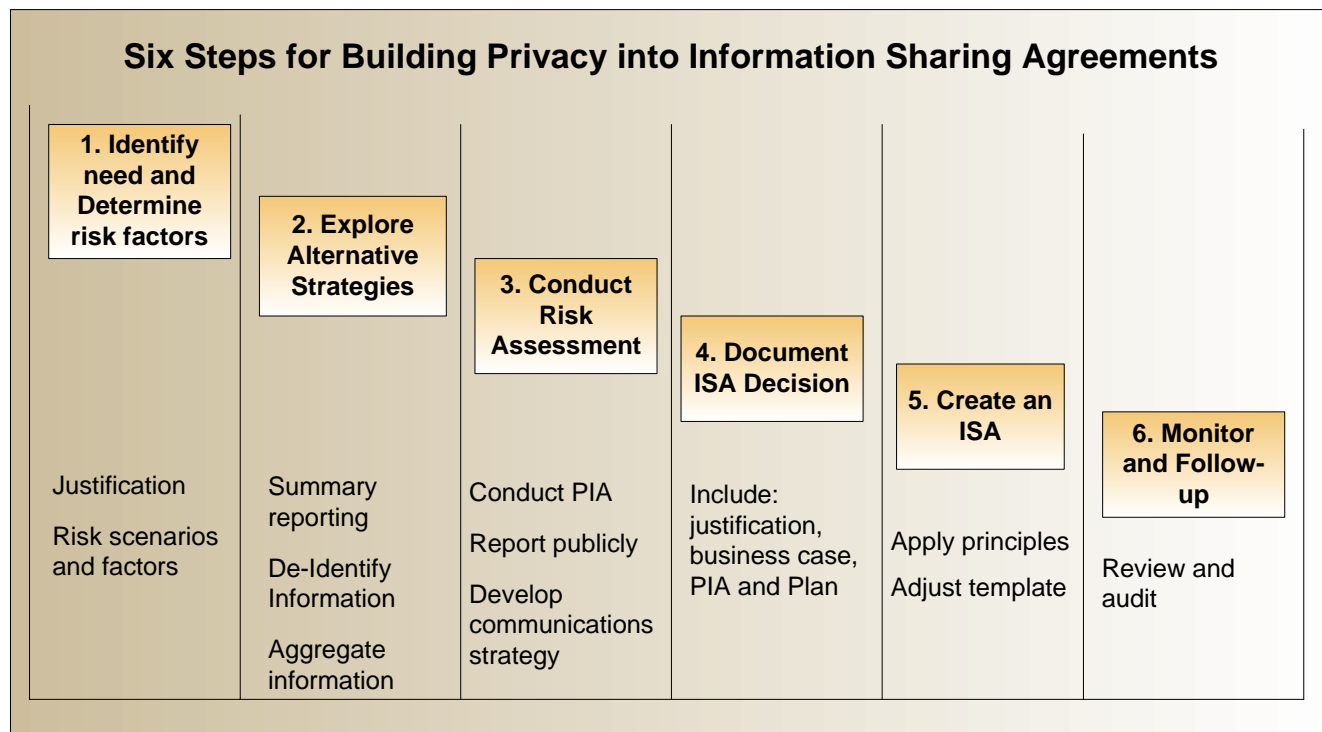
<http://www.gov.ab.ca/acn/200602/19490.pdf>

Discussion Draft on Managing Contracts under the Alberta FOIP Act (Sept 2005)

http://www3.gov.ab.ca/foip/other_resources/publications_videos/pdf/contract_managers_guide.pdf

C. Six Best Practice Steps

The following six best practices cover the lifecycle of decision-making.



Best Practice One: Identify Need and Determine Risk Factors

1.1 What is personal information?

The first step is to determine if the information that could be shared falls within the definition of “personal information”.

Most legislation in Canada uses a definition similar to the following:

Generally, personal information is any information, whether factual or subjective, recorded or not, about an identifiable individual. This includes information in any form, such as:

- Age, name, date of birth, identification numbers, income, ethnic origin, or blood type
- Opinions, evaluations, comments, social status, or disciplinary actions
- Employee files, credit records, loan records, medical records and transaction records

It is recommended that you consult your jurisdiction’s legislation for the definition that applies to your circumstances.

Identifiable

If the information being shared can be used to identify a person, for example through a personal identifying number, it is considered “personal information”. It is not necessary that the person’s name be present for the information to be personal information.

1.2 Do you have the legal authority?

Due to the inherent privacy risks, sharing personal information should be the last resort for meeting a specific objective. Alternatives should always be explored first (*see Best Practice 2*).

Personal information should be shared only when both of the following circumstances exist:

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

(The second circumstance of justifiable need is explored in the next section, 1.3).

1.2.1 Legal authority

Legislation specific to a program or service may or may not make reference to collection or disclosure of personal information. However, the authority to collect the information in question may be implied from the authority to operate the program or service. Authority to disclose the information would normally be found in the individual’s consent or as authorized by a jurisdiction’s privacy statute. If the authority is not clear, officials should consult their legal experts within their jurisdiction.

1.2.2 Consent and notice

The law or legal agreement under which your program or service operates may allow sharing of personal information without consent under certain circumstances.

For example, almost all privacy laws permit the use and disclosure of personal information without consent where that use or disclosure is consistent with the original purpose of collecting the information, where the use or disclosure is required by a law, where the use or disclosure is required for legal proceedings or is required for archival purposes. In certain circumstances, privacy laws permit use and disclosure of personal information for the purposes of lawful investigations, agreements with other governments, research or use or disclosure where there is a clear public benefit.

However, even if a proposed use or disclosure is permitted by law and consent of the affected individuals not required, it is considered a best practice for government agencies to obtain consent in the interest of greater transparency and accountability.

This can be done by ensuring that at the time of the original collection of the personal information, the individual is given notice in clear language how the information will be used and that the individual's participation in a voluntary government program is conditional on consent to those uses and disclosures of the information.

For a table of all privacy laws in Canada relevant to ISAs covered in these guidelines, please see Appendix A.

1.2.3 Mandatory provision of information

There are particular circumstances, such as a health epidemic, when the provision of personal information to another jurisdiction is mandatory. The *Quarantine Act* (2005) is an example of federal legislation that requires personal health information to be disclosed to provincial health authorities.

1.3 When sharing is needed

Your government organization may receive requests from other jurisdictions to gain access to the personal information under your care. There may also be cases where you are the party making the request, or when your organization is among several that identify a common requirement.

In all cases, sharing personal information should be considered only when there is a clearly identified need in the current period of time. It is not sufficient to share personal information based on desire or "in case it's needed in the future" or "this information could be useful".

Disclosure of personal information from one government body to another is only "needed" when that information is required to administer a lawful government program or service, and even then, the disclosure must be limited to the minimum amount of information necessary for the specified purpose.

The collection, use and disclosure of personal information should be carried out in the most limited manner, on a need-to-know basis and with the highest degree of anonymity possible.

Here are some examples of need.

Accountability: It may be necessary to share personal information to determine or verify the accuracy of information about individuals or assess eligibility for a program or service.

Joint Programs and Agreements: If your department is engaged in a joint program or agreement with another government, sharing personal information may be necessary to fulfill program or service delivery.

Client Request: For convenience, clients may request their personal information be shared with other jurisdictions to avoid giving the same information more than once.

1.4 Justification of Information Sharing Agreement

Conducting a cost benefit analysis or a business case is a good business practice for justifying the need to share personal information.

- Outline the potential risks or consequences of not conducting the information sharing activity.
- Clarify why personal information must be shared at this time.
- Specify exactly what information is to be shared, and exactly how the recipient will use the disclosed information.
- Clarify why the information needs to include personal identifiers.
- Identify why the personal information must be collected indirectly (if applicable) and the advantages of sharing the data against alternative methods of achieving the same objectives.
(See *Best Practice 2, Explore Alternative Strategies.*)
- Provide the legal authority by which the information will be disclosed by one party and collected by the other party.

If your objective is related to cost reduction:

- Identify any funds that could be recouped or savings realized through disclosing or collecting personal information under the agreement. For example, there may be savings due to termination of ineligible benefits that would not have been possible without information sharing.
- Weigh the financial advantages against identified privacy risks.

1.5 Preliminary assessment of the risks

Once you have determined that the information fits the definition of “personal information,” that you have permission to share the information, and that there is a clear need to share, you must assess the privacy risks before initiating an ISA.

1.5.1 High risk scenarios

Jurisdictions may wish to take into account an invasion of privacy test that considers three interrelated factors:

- The sensitivity of the personal information, including whether the information is detailed or highly personal (e.g., health information) and the context in which the information was collected.
- Whether it would be reasonable for the individual who provided the information to expect that it would be used in the proposed manner.
- The potential injury if personal information is wrongfully disclosed or misused, including the potential for identity theft or access by foreign governments.

1.5.2 Potential Information Sharing Arrangements with Greater Sensitivity

Personal Health Information (medical records): Medical records can contain information not directly related to a person's physical health. For example, they may contain information about family history, substance abuse, suicidal tendencies, sexual behaviour or private conversations made with medical experts. A person's health record can determine their eligibility for certain medical coverage and affect their educational and employment opportunities.

NOTE: Alberta, Saskatchewan, Manitoba and Ontario have separate legislation covering health information. (*See Appendix A for applicable web addresses.*)

Lawful investigations (criminal records): Governments may need to share personal information for the purpose of conducting a criminal investigation. Information may be required to charge, prosecute or deport people from other jurisdictions. Such information is considered highly sensitive since it is often deeply personal and at the stage of unproven allegation.

Financial Records: Tax, credit, insurance and other financial-related information may be considered sensitive due to the ramifications of such information being accessed by unauthorized persons.

Any personal information which, if accessed under circumstances outside of the intended use, could result in harm to the individuals affected, would be considered "high risk."

1.5.3 International transfer

If your government wishes to share personal information with a government outside of Canada, privacy risks are elevated. This is because laws in a foreign jurisdiction can take precedence over Canadian law. Many countries around the globe are enacting anti-terrorism legislation that may over-ride the privacy of individuals. This means that personal information about Canadians in a foreign country may be accessed without the knowledge or permission of Canadians.

Risks are also elevated because there is no convenient or easy way to enforce a contract, or to regain access and control over information from an unwilling party in another jurisdiction.

Sharing personal information should be done only with countries that have made a commitment to protect personal information. Even then, it is no simple task to understand all of the intricacies of another country's privacy laws and exceptions.

It is recommended that assurances from the party wishing to collect personal information be independently verified.

For more information on addressing international circumstances, see Appendix B.

1.5.4 Security measures

A major consideration for privacy risks are the security measures taken to safeguard the information. This includes the location of databases, storage methods, methods of transfer, use of technology and personnel assigned.

You should consult your security policy and security officials to identify security measures and procedures applicable to your jurisdiction and specific circumstances.

For instance, the Government of Canada requires that departments must use encryption or other safeguards endorsed or approved by the Communications Security Establishment (CSE) to protect the electronic communication of classified and Protected C information. Departments should encrypt Protected A and B information, when use of encryption is supported by a Threat and Risk Assessment. However, departments must encrypt Protected B information prior to transmitting it across the Internet or a wireless network.

Security can go beyond technical and physical measures. Administrative safeguards include limiting access to individuals who have the necessary authorization, allowing access only to those who have signed a written commitment to the privacy and security of the information and limiting access to staff and management who have received training in security awareness, practices and procedures.

Since good privacy is dependent upon responsible security safeguards, it is essential this factor is addressed by the ISA.

1.5.5 Pushing information

Information provided by you to other parties should be pushed not pulled. Where it is concluded that the information or data should be shared, and the necessary authorities are in place, the collecting party should not be given access to the database in which personal information under your care is stored or held. Rather, you should transfer the information or data to the other jurisdiction in the manner, and at the times and dates, provided for in the agreement.

Best Practice 2: Explore Alternative Strategies

Avoiding the sharing of personal information is a priority to dramatically reduce or eliminate privacy risks.

Tom Wright, a former Ontario Information and Privacy Commissioner, pointed out in his paper on a 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).”

The following methods are alternatives to sharing personal information.

2.1 Summary reporting

Summarizing information contained in a database or directory may be sufficient to meet the project objectives. Rather than identifying people, the summary reports on results such as the number of people located in a specific geographical area.

2.2 De-identified information

Personal information that has been modified so that the identity of the subject individual cannot be determined by a reasonably foreseeable method is referred to as de-identification. This is typically accomplished by removing identifiers such as a person's name, age and other information that can be linked to make an identity. The modification of data must be such that re-identification, using information to make an identity, is impossible or cannot be done in any reasonable way.

(Definition source: Canadian Institute of Health Information, Privacy and Confidentiality of Health Information at CIHI,
http://www.icic.ca/cihiweb/en/downloads/privacy_policy_priv2002_e.pdf)

2.3 Aggregated data

Information that has been generalized in such a way that it cannot be linked to an individual, such as using a range of ages rather than specific ages of individuals, is known as aggregated data. This is a very good way to eliminate privacy risks. Always ask whether the specific objective can be achieved using aggregated data, before concluding that disclosing personal information is appropriate.

Best Practice 3: Conduct Risk Assessment

Assessing privacy risks should be conducted in a systematic and thorough manner through completion of a Privacy Impact Assessment (PIA) and a Threat Risk Assessment (TRA).

The following tools and procedures have proven to be effective in ensuring this is achieved.

3.1 Conduct a Privacy Impact Assessment (PIA)

One of the most effective ways to assess the level of risk is to conduct a Privacy Impact Assessment (PIA). A PIA uses a comprehensive checklist to identify potential privacy risks.

A PIA is a risk assessment tool that measures compliance not just against established legal standards, which represents minimum acceptable practice, but also against universal privacy principles.

In some Canadian jurisdictions, conducting a PIA is mandatory under certain circumstances such as the introduction or revision of a government program or service.

A list of PIA templates, documents and references is provided under Appendix C. A list of examples of common privacy risks is found in Appendix E.

3.2 Public reporting and communications

The authority under which you are sharing personal information may require you to report publicly on the information sharing agreement.

Even if not required, it is a best practice to develop a communications plan for any ISA. The plan should recognize the public's sensitivity to information sharing and the need for transparency.

3.3 Consult departmental privacy, security and legal experts

Your government organization may have its own privacy, security and legal experts who should always be consulted before any government-to-government information sharing agreement is planned or created.

3.4 Consult your jurisdiction's privacy advisor

Depending upon your jurisdiction and circumstances, you may be required under legislation or policy to consult your jurisdiction's Privacy Commissioner or Ombudsman.

Even if not required, it is a best practice to engage in consultation with the official representative for your jurisdiction in the area of privacy advice and research, especially if your ISA has a high level of risk.

For the federal government, this is the Office of the Privacy Commissioner and for a number of jurisdictions, this is the Office of the Information and Privacy Commissioner. In some jurisdictions the title and authority varies. *A link to the Privacy officials across Canada is provided in Appendix D.*

Best Practice 4: Document

4. Document your decision

If after exploring alternatives (Best Practice 2) and conducting a risk assessment (Best Practice 3) you have concluded that personal information must be shared, it is good practice to document this decision.

Documentation justifies the decision to share personal information and outlines a plan to mitigate risk. It should include, but not be limited to a justification, a cost benefit analysis, a Privacy Impact Assessment and a risk mitigation plan to address all risks.

Your documentation should also include what steps will be followed in the event of a security breach.

A critical best practice is to implement effective information management practices throughout the life cycle of the ISA (framing, design, implementation, follow-up) to facilitate informed decision-making. It is also important to keep in mind that without sound information management practices in place that ensure all aspects of agreements are appropriately documented, it becomes difficult to follow-up or effectively monitor agreements. This leads to inadequate reporting on the extent of personal information sharing and by extension, whether your organization can determine if the information sharing activity is appropriately managed and is in compliance.

Best Practice 5: Create an ISA

This section provides a template for creating an ISA. Your jurisdiction may have its own template applicable to your circumstances.

5.1 How to use the template

Insert the appropriate clauses where indicated and change text as required to fit your specific circumstances. While the template is comprehensive, it does not necessarily cover all circumstances applicable to your agreement.

5.2 Oversight body

It is a best practice to have an oversight body for the development of an ISA. This is a group or committee within your organization familiar with privacy and security issues who can provide guidance and advice.

5.3 ISA approval/sign-off

Always ensure that your privacy and legal advisors review and approve each ISA. It is also important to ensure that an ISA is signed-off or approved by the proper signing authority for both parties.

5.4 Ten principles

Content in the ISA template reflects the 10 privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information, recognized as a standard in Canada. The principles are:

1. Accountability
2. Identifying Purposes
3. Consent and Authority
4. Limiting Collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Security Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

5.5 Plain language

Each ISA should be written in plain language so it is easily understood. Explain all terms and acronyms to avoid confusion.

5.6 Personal Information Sharing Agreement Template

Note: Most information sharing agreements between governments in Canada are by way of Memorandum of Understanding (M.O.U.) and not by contract, because it is not intended that governments will go to court to enforce disputes between each other.

Where there is a broader federal-provincial agreement that creates an interjurisdictional program or service, that agreement should contain general clauses providing for the sharing of information, subject to the conclusion of a more specific Information Sharing Agreement between the parties.

1.0 Title of agreement

[Insert title]

2.0 Agreement Parties

This agreement is between [name of party] and [name of party].

3.0 Roles and Responsibilities

Each party of this agreement agrees to be responsible for the actions of its employees, agents and contractors with respect to the use, disclosure and disposition of the personal information that is subject to this agreement.

3.1 Disclosing party: The party that is disclosing personal information under this agreement is: [name the party and provide contact information].

3.2 Collecting Party: The party that is collecting (receiving) personal information from the disclosing party is: [name the party and provide contact information].

(In the case of reciprocal agreements, both parties may be disclosing and collecting and the above wording would therefore reflect this).

3.3 Private Contractors: *(If applicable)* The following private firm or firms have been contracted in the transfer of data covered in this agreement:

[Identify the party which has contracted each firm, the names of firms, contract numbers and privacy legislation that applies to the information when it is in the custody of the firm or firms. Note that the privacy law that applies to the government agency may also apply when the government contracts with a supplier. The government party cannot contract out of its legal obligations].

3.4 Resolution Mechanism and/or Parties: If there are any questions, challenges or disagreements related to any issue connected to this agreement, the matter will be handled as follows: [Outline how disagreements will be handled such as referring disputes to senior officials of the two parties, with the possibility of the parties referring the matter to a neutral third party mediator.]

3.5 Responsibilities for Costs: Costs incurred by a party in the context of this agreement will be the responsibility of that party.

4.0 Purpose or Purposes

The purpose of this agreement is to provide for the disclosure of personal information by [name the disclosing party] to [name the collecting party] for the following purpose (or purposes): [specify the purpose or purposes], and to provide for the protection of that information.

(In the case of reciprocal agreements or those with multiple parties, repeat the above clause as required).

4.1 Identification of Personal Information: The personal information that will be disclosed and collected under this agreement is as follows. (Include both a description of the personal information to be shared and a list of the data fields to be shared. Don't forget to list each individual data field or client file for each purpose outlined in section 4.0).

Example data field listing:

Party A will disclose to Party B, the following data fields from each client file that is part of [name of program] for the purpose of [state purpose].

- Name
- Client Identifier
- Address
- Date of Birth
- Benefits Received

Party B will disclose to Party A, the following data fields from each client file that is part of [name of program] for the purpose of [state purpose].

- Name
- Client Identifier
- Address
- Date of Birth

(If the lists of data fields or client files are extensive, they can be provided in appendices).

4.2 Frequency and duration: The personal information covered in this agreement will be transferred only at a frequency, and for a period of time, as is necessary. The frequency is expected to be [insert time frame] and the duration [insert dates or specify for the duration of the program or service]. [If the arrangement is anticipated to be over a longer term, the time period should be limited but the agreement can have a clause allowing for renewal if the arrangement is still necessary.]

4.3 Secondary use: Secondary use of personal information is prohibited except with the consent of the individual concerned or as permitted by law.

4.4 Third Party use: The information received by the collecting party under this agreement will not be provided to a third party without the prior written consent of the party that provided the information [the disclosing party], subject to applicable legislation of each jurisdiction, including access and privacy laws and any other relevant law.

4.5 Agreement to consult: In the case of an access to information (ATI) request or a Freedom of Information (FOI) request under appropriate legislation both parties agree to consult.

5.0 Authority

[Name the disclosing party] confirms that it is authorized to disclose the personal information described in this agreement to [name the collecting party] for the stated purposes under Section 4 by authority of [name legislation and specific section or sections thereof].

[Name the collecting party] confirms that it is authorized to collect the personal information described in this agreement from [name the disclosing party] for the stated purposes under Section 4 by authority of [name legislation and specific section or sections thereof].

6.0 Method of Transfer

Personal information covered in this agreement will be securely transferred in the following ways: [State the technical and physical ways in which the personal information will be transferred such as computer tapes, encryption, password protection and other methods.]

7.0 Security of Personal Information

7.1 Confirmation to ensure personal information is secure: Both parties are responsible for the security and integrity of the personal information entrusted to them under this agreement and promise to safeguard the personal information against accidental or unauthorized access, disclosure, use, modification and deletion.

7.2 Administrative, Technical and Physical Safeguards: Personal information covered in this agreement will have the following administrative, technical and physical safeguards. [State all the administrative, technical and physical safeguards required to protect the confidentiality of the information, especially in regard to use and disclosure.]

7.3 Security laws and policies: Personal information covered under this agreement will be securely collected, disclosed, used, retained, destroyed and disposed of in accordance with the laws, security policies, guidelines and directives applicable to each party.

In the case of [name the disclosing party], these are: [name laws and policies covering privacy and security].

In the case of [name the collecting party], these are: [name laws and policies covering privacy and security].

Example: In the case of Canada, the main applicable laws and policies are: [statute authorizing the program or service], *Privacy Act*, *Access to Information Act*, *Library and Archives of Canada Act*, *Privacy and Data Protection Policy*, *Access to Information Policy*, *Government Security Policy* and the *Management of Government Information Policy*.

7.4 Prevention of recurrence: In the event of accidental or unauthorized access, disclosure, use, modification and deletion, the party responsible for the security of the

personal information will promptly take all reasonable steps to prevent a recurrence of the event and will promptly notify the other party of the occurrence.

7.5 Inspection of security measures: It is agreed that the disclosing party, at its discretion, has the right to inspect the security and confidentiality procedures of the collecting party, subject to reasonable protections for security and confidentiality processes.

7.6 Response to breach of privacy or security: It is agreed that the disclosing party, upon receiving notice of accidental or unauthorized access, disclosure, use, modification and deletion, may, at its discretion, terminate the agreement immediately and may request the return of personal information already disclosed. In the event of a privacy or security breach there needs to be a plan in place to notify the individuals whose information was disclosed.

7.7 Disposal on termination of agreement: Personal information covered in this agreement will be disposed of on the termination of the agreement in such a way that re-identification is not possible after disposal. Disposal will be in the form of [returning personal information to the disclosing party or destruction by the collecting party] in accordance with the laws and/or policies identified in Section 7.2.

7.8 Disposal for other reasons: Personal information can be recalled or disposed of for reasons other than termination of the agreement by written consent of the parties.

8.0 Limiting Collection, Use, Disclosure and Retention

8.1 Commitment to Limit: Personal information covered in this agreement shall not be collected (received), used, disclosed or retained for purposes other than those identified in this agreement except with the consent of the individual concerned or as permitted by law.

8.2 Notification of identification and re-identification: No attempt is to be made to re-identify individuals whose identities have been removed from the data unless permitted by law. If a collecting party to this agreement is permitted under its own laws to identify or re-identify an individual, it shall first notify the disclosing party and seek agreement to proceed.

9.0 Openness, Individual Access and Challenging Compliance

Each party agrees, with respect to personal information that is under the control of that party, to respond to requests from individuals to receive their personal information and to request correction of their personal information in accordance with [name legislation]. Each party agrees to notify the other party of the request and the corrected information. In addition, each party also agrees to respect each other's revisions to the information.

10.0 Accuracy

Each party will use reasonable efforts to ensure the completeness, accuracy and timeliness of the information covered under this agreement. Although, it is understood and agreed that the parties cannot guarantee accuracy and will therefore not be held responsible for any damage to the other party resulting from the disclosure or use of any information that is inaccurate, incomplete or out-of-date, each party will endeavor to correct any inaccuracies and ensure that the rights of an individual to access and correct personal information is upheld (see 9.0).

11.0 Indemnification

[Party A] agrees to indemnify and save harmless [Party B] and all of its representatives and employees from and against any damages, costs, losses or expenses or any claim, action, suit or other proceeding which they or any of them may at any time incur or suffer as a result of or arising out of any injury or loss which may be or be alleged to be caused by or suffered as a result of the acts or omissions of [Party A] and its representatives and employees relating to, attributable to or in connection with the performance of this Agreement.

[Party B] agrees to indemnify and save harmless [Party A] and all of its representatives and employees from and against any damages, costs, losses, or expenses or any claim, action, suit or other proceeding which they or any of them may at any time incur or suffer as a result of or arising out of any injury or loss which may be or be alleged to be caused by or suffered as a result of the acts or omissions of [Party B] and its representatives and employees relating to, attributable to or in connection with the performance of this Agreement.

Each party agrees to give notice to the other party of any claim, action, suit or proceeding relating to or in connection with the management of the information that is the subject of this Agreement. Each party must, at its own expense and to the extent reasonably requested by the other party, participate in or conduct the defense of any such claim, action, suit or proceeding and any negotiations for the settlement of the same, but one party will not be liable to indemnify the other party or any other indemnified persons for payment of settlement of claim, action, suit or proceeding unless the other party has given prior written consent to the settlement.

12.0 Compliance Monitoring

The parties will, separately or jointly, on a periodic basis, review the practices and procedures outlined in this agreement to ensure compliance with the provisions of legislation referred to in this agreement. [Note: Specify if physical inspection will take place as part of any review]. Each party will provide the results of such reviews to the other party upon written request.

The parties will also ensure that they take appropriate measures to ensure that information about the agreement is kept up-to-date and that a record is kept of any discrete disclosures with respect to the personal information collected as part of the agreement.

The parties also recognize the agreement is subject to compliance audits, investigations and reviews conducted by the appropriate federal/provincial/territorial Commissioner, other authorized official, or third party.

13.0 Amendments

This agreement can be modified with the written consent of designated officials of each party.

14.0 Other General Provisions

(Insert other clauses as required that do not contravene the legal authority for each party. These may include clauses for special consideration such as international data flows).

15.0 Signatures, Signing Dates and Appropriate Appendices

(This includes identifying the names, titles and signatures of the appropriate officials for both the disclosing and collecting parties and the date of the agreement. Ensure that sign-off is by a level appropriate to each party.)

Best Practice 6: Monitor and Follow Up

6. Monitor and Follow Up

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

You would not normally engage in auditing of activities and responsibilities of the other party, relying instead on their commitment in the agreement to adhere to their legal and policy structure. Alternatively, this can be achieved through the use of providing assurances that the obligations are being met by means of self-assessments and written certificates of compliance exchanged periodically throughout the term of the agreement. However, your ISA should include the right to investigate matters related to the other party in the event you deem it necessary and provide for termination if not satisfactory.

It should be noted that monitoring itself could represent a privacy risk depending upon how it is conducted. Ensure that your oversight team has the proper credentials and authority to conduct monitoring and that the same safeguards used to protect personal information are used for agreement monitoring.

Finally, do not forget to review your ISA files, on a regular basis, to ensure that each ISA is supported by complete, accurate and up-to-date records, and that you have followed sound information management practices (e.g., documenting all disclosures).

APPENDICES

APPENDIX A: Privacy laws that apply to personal information under the control of the Public Sector in Canada

Jurisdiction	Public Sector	Health	Municipal
Alberta	Freedom of Information and Protection of Privacy Act	Health Information Act	
British Columbia	Freedom of Information and Protection of Privacy Act		
Manitoba	Freedom of Information and Protection of Privacy Act	Personal Health Information Act	
New Brunswick	Protection of Personal Information Act		
Newfoundland	Access to Information and Protection of Privacy Act		
Northwest Territories	Access to Information and Protection of Privacy Act		
Nova Scotia	Freedom of Information and Protection of Privacy		
Nunavut	See N.W.T.		
Ontario	Freedom of Information and Protection of Privacy Act	Personal Health Information Protection Act	Municipal Freedom of Information and Protection of Privacy Act
Prince Edward Island	Freedom of Information and Protection of Privacy Act		

Jurisdiction	Public Sector	Health	Municipal
Quebec	<u>Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information</u>		
Saskatchewan	<u>Freedom of Information and Protection of Privacy Act</u>	<u>The Health Information Act</u>	<u>Local Authority Freedom of Information and Protection of Privacy Act</u>
Yukon Territory	<u>Access to Information and Protection of Privacy Act</u>		
Government of Canada	<u>Privacy Act</u>		

Appendix B: International Context

If your government wishes to share personal information with a government outside of Canada, privacy risks are generally considered more severe. This is because laws in a foreign jurisdiction can take precedence over Canadian law.

Countries around the globe are enacting anti-terrorism legislation that may over-ride the privacy of individuals. This means that personal information about Canadians in a foreign country may be accessed without the knowledge or permission of Canadians.

Risks are also elevated because there is no convenient or easy way to enforce an agreement, or to regain access and control over information from an unwilling party in another jurisdiction.

Does the country share Canadian values and principles?

Sharing personal information should be done only with countries that have made a commitment to protect personal information. Even then, it is no simple task to understand all of the intricacies of another country's privacy laws and exceptions.

It is recommended that assurances from the party wishing to collect personal information be independently verified.

The processes and issues identified in this document can also be used for international agreements involving personal information. It is important that your legal and privacy experts are consulted throughout the framing of an agreement.

International Protective Clauses

While the use of a clause that forbids access to personal information by a foreign government for purposes outside the terms of an agreement may be over-ridden by foreign legislation, its inclusion should still be considered as a protective measure.

This may involve a statement similar to the following:

"Access to the personal information identified in this agreement by any party or purpose not identified in this agreement is strictly forbidden."

Provincial legislation impacting international transfer: Your jurisdiction may have legislation restricting the geographical scope of personal information transfer.

For example, the *Freedom of Information and Protection of Privacy Act* in British Columbia under Section 30 limits the storage and access of personal information to within Canada except under certain circumstances.

See http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm#section30

Cautionary Note: No template wording for international data flow is included in these guidelines because of the complex nature of such transfers. Consult your jurisdiction's privacy laws and legal and privacy experts in the consideration of any international agreements.

Appendix C: PIA Templates and References

Government of Canada	British Columbia	Alberta	Saskatchewan	Manitoba	Ontario
<p>Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks</p> <p>PIA Template</p> <p>PIA Learning Tool</p>	<p>Privacy Impact Assessment Process</p> <p>NOTE: PIA is required under Section 69 of the FOIP</p>	<p>Privacy Impact Assessments</p>	<p>Privacy Impact Assessments (PDF)</p>	<p>The Privacy Compliance Tool</p>	<p>Privacy Impact Assessment Guidelines</p> <p>Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act (PDF)</p>

Appendix D: Privacy Officials in Canada

Please refer to the Federal Privacy Commissioner's Web site for a centralized reference to both Provincial / Territorial Oversight Offices and Government Organizations:

http://www.privcom.gc.ca/information/comms_e.asp

For the **Government of Canada**, there are three government institutions involved:

- Treasury Board of Canada Secretariat with respect to the *Privacy Act* and policy directives. Refer to the following TBS Web site for implementation reports and notices http://www.tbs-sct.gc.ca/qos-sog/atip-airp/index_e.asp and for policies <http://www.tbs-sct.gc.ca> ;
- Industry Canada with respect to the federal privacy legislation for the private sector (*the Personal Information Protection and Electronic Documents Act*). http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_qv00003e.html ; and
- Justice Canada <http://canada.justice.gc.ca/>.

The Federal Privacy Commissioner is a federal agent of Parliament that plays an oversight role for both pieces of federal privacy legislation: <http://www.privcom.gc.ca/>

Appendix E: Potential Privacy Risks

The following are some of the common privacy risks that are associated with Information Sharing Agreements.

Lack or Doubtful Legal Authority: Failure to identify clear program authority to collect, use or disclose personal information raises fundamental concerns.

Data profiling/data matching: Combining unrelated personal information obtained from a variety of sources to create new information about an individual or using information about an individual's preferences and habits to build a profile on the individual.

Transaction Monitoring: Observing or tracking the history of an individual's interaction with one or more programs or services. This usually results in creation of new personal information describing an individual's overall experience with one or more programs.

Identification of Individuals: Government service delivery generally requires identification of an individual and authentication of their identity as a way of managing security risks. Surveillance risks exist where the use of common identifiers or identification systems facilitate data sharing, profiling or transaction monitoring. The type and number of data elements required to establish identity must be calibrated to the level of confidence needed to perform the transaction.

Inadequate security measures: Failure to comply with standards about electronic and physical security controls or standards relating to transmission security such as encryption. Studies have shown that up to 70 to 80% of database intrusions are committed by persons who have network authorization, knowledge of database access codes and an appreciation of the value of the data they wish to exploit

Use or Disclosure of Information for secondary purposes: The objectives of the ISA and the use or disclosure of information goes beyond the original purpose of the collection.