

Question and Answer Document

The Public Sector CIO Council has released a new document entitled: "Government-to-Government Personal Information Sharing Agreements - Guidelines for Best Practice".

The guidelines cover the management of ISAs, information sharing agreements that outline the terms and conditions for the exchange of personal information between governments.

1. What are the guidelines all about?

The guidelines present an organized process from which to base decisions related to the development of ISAs. While a number of jurisdictions in Canada have ISA templates, what has been lacking is a step-by-step approach that helps government managers first decide if sharing personal information is warranted and if so, what measures need to be taken to frame and implement an ISA, and in following up.

2. Why is this important?

When personal information under the care of a government organization leaves the custody of that organization and is transferred to another party, there is always the risk that the privacy and security of the information could be breached. That can have serious consequences including a lack of public trust, complaints and in some cases, the withdrawal of government funding.

3. Why now?

The guidelines were produced to meet a growing need on the part of government Chief Information Officers and other program and service managers to better understand privacy and security measures and their application related to government to government sharing of personal information. This need is being fueled by a number of trends taking place simultaneously. More personal information is being exchanged across borders (known as transborder data flow) for a variety of reasons including increased government program integration and the need to verify information to prevent program abuse.

4. Who should use these 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.

5. How are the guidelines structured?

The guidelines comprise six best practice steps, which when followed in the order presented, will serve as a risk management tool for government managers considering the sharing of personal information. The guidelines recommend actions and ISA clauses designed to mitigate privacy risks as much as possible but should not be used in isolation. Readers are told they must consider the laws and policies governing their jurisdiction and seek guidance and approval from their own privacy and legal experts as applicable.

6. What are the six best practice steps?

1. Identifying need and legal authority
2. Exploring alternatives to sharing personal information
3. Conducting risk assessment
4. Documenting the decision to proceed with an ISA
5. Creating an effective ISA
6. Monitoring and following up

7. Are there varying degrees of sensitivity when it comes to personal information?

Yes, personal information in certain categories are regarded as more sensitive than others and in these cases, more stringent measures are recommended for privacy protection. Generally, information related to a person's medical, financial and if applicable, criminal records, are regarded as more sensitive because of the ramifications of such information being accessed by unauthorized parties.

8. Do the guidelines cover all governments in Canada?

Yes, the guidelines are designed to be used by public sector jurisdictions: municipal, provincial and territorial and federal. The basic principles of privacy and recommended best practices apply to all jurisdictions in Canada. However, there are some differences in laws and policies among jurisdictions. The guidelines therefore include reference materials such as a list of privacy laws for each jurisdiction to help the reader customize the best practices to their circumstances. In addition, the reader is instructed to consult their jurisdiction's legal and policy framework and privacy and legal advisors.