

## Fact sheet

### **New Guidelines Provide Recommended Process for Developing Government-to-Government Personal Information Sharing Agreements**

To protect personal information, a number of laws and policies require that certain government organizations have agreements in place when sharing personal information with other government parties.

Such agreements, known as information sharing agreements (ISAs), are an effective risk management tool, and even if not mandatory, are regarded as a best practice to ensure compliance with privacy laws.

ISAs make clear the purpose(s) of sharing personal information, the legal authority to disclose and collect such information and the commitment that the information will be kept private and secure.

While a number of provinces have ISA templates containing appropriate clauses, there has not existed a comprehensive guide on the process involved in developing an ISA. That is, until now.

The guidance provided in the best practices document on government to government information sharing agreements was created by the Privacy Subcommittee of the Public Sector CIO (Chief Information Officer) Council. The PSCIOC is comprised of federal, provincial, territorial and municipal CIOs.

The guidelines meet the need for an easy-to-follow, organized approach to the consideration and development of ISAs on the part of officials at all levels of government.

### **Step by Step Outline**

The guidelines contain a step-by-step outline that takes the reader through six essential "best practice" milestones forming the lifecycle of the decision-making process.

The six best practices are as follows.

*1. Identify Need and Determine Risk Factors:* This initial step provides a definition of personal information; helps answer key questions about whether information should be disclosed, if there is legal authority and when an ISA is appropriate; then guides the reader through a preliminary assessment of risks that include high risk scenarios.

*2. Alternate Strategies:* Disclosing personal information is a last resort to accomplish the objectives of a government program or service. Step two therefore looks at alternative methods.

*3. Conduct Risk Assessment:* If, after exploring alternatives, it is decided that the sharing of personal information is still needed, step 3 provides guidance on conducting a risk assessment to ensure any and all privacy vulnerabilities are identified and addressed.

*4. Document:* This step recommends documenting the decision to proceed with information sharing under an ISA for transparency, accountability and auditing purposes.

*5. Create an ISA:* Here are recommendations for an effective ISA and suggested clauses as contained in an easy-to-use, comprehensive template.

*6. Monitor and Follow-up:* The final step is monitoring the effectiveness of an ISA and following up as required.

## **Reference Lists**

In addition to the six best practice steps, the guidelines include handy reference lists as appendices. They include: a listing of privacy laws applicable to the public sector along with corresponding web links; guidance on international agreements; a list of Privacy Impact Assessment templates and guidance documents for step 3 of the recommended best practices; a list of privacy oversight officials in Canada; and additional detail on potential privacy risks.

## **Not meant to be used in Isolation**

The guidelines, while providing a recommended approach to developing ISAs, are not meant to be used in isolation. Readers are asked to always consult with their 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 — and to ensure the appropriate authorities review, approve and sign off the agreements.

## **Accessing the Guidelines**

The guidelines are available at <http://www.iccs-isac.org/>