Personal Information Map Requirements

Purpose

This document provides the business reasons for completing personal information maps (PIM) as well as requirements for program managers completing a PIM. PIM should capture all personal information stored within a program, regardless of format.

It is recommended a PIM be completed in conjunction with completing a Privacy Impact Assessment (PIA).

Business Case

The PIM allows departments and citizens to understand what personal information is held; how many people have access to it; to whom it is routinely disclosed; and where it is held. The PIM is an inventory of the personal information holdings of departments and its programs.

Maintaining an inventory of personal information allows the government to:

- Proactively disclose to citizens the information the government has about them and inform them about how it is being used;
- Identify potential risks and vulnerabilities;
- To more quickly respond to an individual's request to access their personal information;
- Ensure personal information is managed appropriately throughout its lifecycle;
- Allow for faster responses in the event of a privacy breach;
- Identify personal information that is retained but is not necessary for business purposes (and therefore not required); and
- Enable programs to understand the types of personal information held, including: who has access; for what purpose; where the data is stored; and ensure proper controls are in place (information sharing or service-level agreements, for example).

Steps to complete a PIM

Step #1: Complete Categories of Personal Information Tool

Begin completing your inventory by accessing the *Categories of Personal Information Tool*, located on the ATIPP office's SharePoint site.

Briefly review the tool. If you are uncertain how to complete the tool, contact your departmental privacy officer or ATIPP office for assistance.

Note: Reviewing intake forms and fields within your program are good sources to reference when listing the types of personal information within your program.

Step #2: Complete the PIM tool: Accountability

Identify: (1) the name of program; (2) the information owner[1]; and (3) the name of the information system (if any).

Step #3: Complete the PIM tool: Personal Information Holdings

1. List the category of the information collected.
    a. Refer to the *Categories of Personal Information Tool* – located on the ATIPP office's SharePoint site.
2. List your authority to collect the information.
    a. Identify the legislative provisions that allow you to collect the personal information. For example, "29(c) of the ATIPP Act".
3. List your authority to use the information.
    a. For example, "35(1)(a) of the ATIPP Act".
4. # of employees that have access.
    a. List the number of employees who have access to the categories of information. Refer to the *Categories of Personal Information Tool* you completed in step #1.
    b. The number of employees is grouped by: 0-5 employees; 6-10 employees; 11-20 employees; or 20 + employees).
5. Audit Log
    a. Identify whether your system has audit capabilities.
6. Can audit log capture: User ID, date and time PI viewed?
    a. Identify whether an audit log can be created in the format above. This is to allow citizens and employers to monitor how personal information is being accessed and used.
7. Approved Records Retention and Disposition Schedule.
    a. Identify whether you have an approved Records Retention and Disposition Schedule for this information.
8. Routine disclosure outside of your department.
    a. List the program and name of the institution to which the information is routinely disclosed.
9. List your authority to disclose the information.
    a. Identify the legislative provisions that allow you to legally disclose the personal information. For example, "36(b) of the ATIPP Act".
10. List categories of information disclosed.

[1] The information owner is the individual who is accountable for a program's information holdings.

a. Refer to the *Categories of Personal Information Tool* – located on the ATIPP office's SharePoint site.

11. List agreements in place.
    a. If routine disclosures of information outside of your department or outside of your program, you may need to have an Information Sharing Agreement (ISA), Information Manager Agreement (IMA), or a Service Provider Agreement (SPA), for example. Note that the agreements vary depending on the risks associated with sharing/disclosing information. For example:
        i. Least-risk: Information shared within a department.
        ii. Medium-risk: Information shared with another department.
        iii. Higher-risk: Information shared with a custodian or an external agency or government.
    b. Note: you need only list the <u>type</u> of agreement in place, if any. For example, "ISA", "IMA" or "SPA".