Disclosure of Personal Information Policy

1. About this document

This policy defines the requirements for departments when disclosing personal information, and should be referred to by program managers when establishing new programs.

2. Definitions

"ATIPP Act" is the *Access to Information and Protection of Privacy Act.*

"Disclose" means making information available or releasing it outside of the original department that collected the information. For example, telling or giving someone, another department, agency or organization information that was originally supplied to your department means you are disclosing the information.

"Individual" is the person the personal information is about or their authorized representative.

"Personal Information" is as defined in section 3 of the ATIPP Act.

"Personal Information Directory" is the published list of completed Personal Information Maps. This list can found on the publicly facing ATIPP website.

"Personal Information Map" (PIM) shows what personal information is held and where it is held by government programs. Overall, the PIM is an inventory of the personal information holdings of departments and its programs. PIM must be completed using the approved template created by the ATIPP Office.

"Purpose" means the purpose for which the information was originally collected by the department or program.

3. Application

This policy applies to any programs or activities to which the *Access to Information and Protection of Privacy Act* applies and the department is listed in GAM 2.1.

4. Authority

This policy is issued under GAM 2.27 and was approved by the DM of HPW on March 13, 2017 .

5. Policy

General

- Departments must only disclose personal information in accordance with sections 36 (disclosure of personal information), 38 (disclosure for research and statistical purposes) and 39 (disclosure for archival or historical purposes) of the ATIPP Act.
- Departments must limit the disclosure of personal information to the minimum amount necessary to accomplish the purpose for which it is to be disclosed.
- Departments must not disclose personal information if the purposes of the disclosure can be achieved using other information (non-identifiable information, for example).
- Departments must update Personal Information Maps when any new routine disclosure of personal information occurs, if a Personal Information Map was completed previously.
- Completed Personal Information Maps must be submitted to the ATIPP Office for entry into the Personal Information Directory.

Written Consent

Consent to disclose personal information must be in writing and specify to whom the personal information may be disclosed and how it may be used (as per regulation 2(1), O.I.C. 1996/053).

- It is recommended the written consent be verified by the signature or mark of the individual. Departments should take the sensitivity[1] of the personal information into consideration when determining whether a signature or mark is necessary.

When obtaining consent, departments should be satisfied that:

- Reasonable steps have been taken to verify the individual's identity.
- It is voluntary and not obtained through misrepresentation.
- The consequences (if any) of refusing to consent have been communicated.

[1] For more information on determining the sensitivity of personal information, see the "Personal Information Classification Guidelines" on the ATIPP office's SharePoint site.

- An individual who has given consent may withdraw it by notifying the department. A withdrawal does not have a retroactive effect.
- Departments cannot penalize individuals for refusing to give consent for additional disclosures by denying them any benefit or service provided in connection with the original collection.

Care or Treatment of a Patient (ATIPP Act, Regulation 2(2), O.I.C. 1996/053)

- Consent is not required if the disclosure is necessary for the care or treatment of a patient of the department.
- Departments must record in the patient's file the personal information disclosed, the date and time of the disclosure and to whom the personal information was disclosed.
- When such a disclosure occurs, the patient must be notified, when practicable, to whom the personal information was disclosed, the purpose for the disclosure and what information was disclosed.

Non-Routine Disclosures

- When disclosing personal information in a specific instance, departments must document in the individual's file:
    - The type of the information disclosed.
    - The name of individual and the department, public body, person or organization receiving the information.
    - The purpose of the request.
    - The recipient's legal authority to collect the personal information;
    - The legal authority under which the personal information was disclosed.
    - The name and position of the employee who authorized the disclosure.
- The information above must be retained for a minimum of one year.
- A disclosure is considered "non-routine" when the disclosure is limited to one specific instance. For example, disclosing personal information to law enforcement in order to comply with a warrant.

Agreements

- Should a department need to routinely disclose personal information, it must enter into a written agreement with the person or institution to which the personal information will be disclosed.

    - A disclosure is considered "routine" when the disclosure is built into the program's regular business process and requests for access are not required for each instance the personal information is disclosed.
- Departments must complete a Personal Information Map and submit it to the ATIPP Office for entry into the Personal Information Directory.
- Agreements must establish, at minimum, the following:
    - Ownership over the personal information.
    - The names, titles and signatures of the individuals who are responsible for the agreement, the date of the agreement and the period for which it is in effect.
    - The authority for disclosing, using and collecting the information.
    - Limitations on the collection, use, subsequent disclosure and retention of personal information for the purposes of the agreement.
    - The purposes for which the personal information is to be disclosed, including a restriction on subsequent uses.
    - Obligations to report any suspected or confirmed privacy breach.
    - A statement that failure to meet the conditions of the agreement may result in cancellation of the agreement.
    - A statement that the department must be consulted prior any disclosure of the information supplied (for example, a disclosure to a law enforcement agency or for research purposes).
    - Identification of the types of personal information to be disclosed.
    - Administrative, technical and physical safeguards to protect the information.
- Departments must consider the sensitivity and amount of the personal information being disclosed when establishing agreements.
- Departments should use the agreement templates created by the ATIPP Office or another template that has been approved by the government's legal services branch.

Research Agreements

- Research agreements must comply with section 38 of the ATIPP Act.
- Departments must consult with the Bureau of Statistics prior to negotiating research agreements that include personal information.
- Departments must report all completed research agreements for entry into the Personal Information Directory.
- Research agreements must establish, at minimum, the following:
    - Personal information disclosed may be used only for the research purpose set out in the agreement.

- The names of those persons who will be given access to the personal information.
- The security requirements for the personal and research information.
- How and when identifiers will be removed or destroyed.
- That contact with the individuals to whom the information relates is prohibited without prior written authorization from the department.
- No use or disclosure can be made of the information in a form that identifies individuals without prior written authorization from the department.
- Information cannot be used for an administrative purpose directly affecting an individual.
- Notification of the department is required if any conditions of the agreement are breached.
- Failure to meet the conditions may result in cancellation of the agreement.

Transmission

- Departments will adopt appropriate safeguards to ensure personal information is protected while it is being transmitted. Such safeguards will be commensurate to the sensitivity of the personal information[2].
    - For example, using the government's approved secure file transfer application.

[2] For more information on determining the sensitivity of personal information, see the "Personal Information Classification Guidelines" on the ATIPP office's SharePoint site.