Privacy Management Guidelines

This document[1] establishes guidelines to assist programs develop policies and/or procedures relating to management of personal information.

Documenting policies and/or procedures on handling personal information can serve to significantly reduce risks associated with the management of personal information within your program; for example, a privacy breach.

Collection

When collecting personal information, programs should develop policies and procedures that identify:

- Their legal authority and purpose for collecting the information (as prescribed in section 29 of ATIPP Act).
- The means by which personal information is to be collected. For example, if there is a prescribed form, inform staff that this is the only means to collect personal information.
    - If there is not prescribed means to collect personal information (it is recommended you do), list the types of personal information needed.
- Whether personal information is to be only collected directly from individuals.
    - If your program foresees individuals having authorized representatives acting on their behalf, have procedures and forms in place to ensure compliance with section 62 of ATIPP Act. It is recommended you work with legal services branch to ensure compliance with ATIPP Act.
- Whether personal information will be collected indirectly from individuals. Ensure one of the following (as prescribed in section 30(1) of ATIPP Act):
    - Authorization has been received by the individual the information is about;
    - An Act authorizes the indirect collection; or
    - The Commissioner has authorized the indirect collection.
- The manner by which notice will be given to individuals at the point of collection. Collection notices can be located on intake forms, posters, brochures, or on program websites.
    - Notices must include the following:
        - The legal authority to collect the personal information;
        - The purpose for collecting the personal information; and
        - The business contact information of an employee who can answer any questions (as prescribed in section 30(2) of ATIPP Act).
- Steps taken to ensure the accuracy and completeness of the information.

[1] This document was adapted from material from the Office of the Privacy Commissioner of Canada.

Use

When using personal information, programs should develop policies and procedures that identify:

- The role(s) that are authorized to use which type of personal information and for what business purpose.
    - Program managers must ensure personal information is limited only to which is necessary to for staff perform assigned duties.
- An individual who is responsible for authorizing the use of personal information for secondary uses.
    - Program managers should also identify whether any foreseen secondary uses of the information and ensure these purposes are captured in the collection notice. For example, will the information be used for program evaluation, planning or research purposes?
- Acceptable use of: electronic communication, fax machines, information systems, remote access, removing information from the office, and information assets.
    - Note: there may exist corporate standards or guidelines on these topics your policy and/or procedure can reference.
- The prescribed form that staff must sign to acknowledge they have read and understood the department or program's policies and/or procedures.

Disclosure

If disclosing personal information, programs should develop policies and procedures that identify:

- How personal information should be disclosed to individuals or their authorized representative. For example, you could make a procedure that encourages clients to pick-up their personal information in person (depending on the sensitivity of the information) or state that registered mail must be used.
- How personal information can be transmitted. For example, you can state that encryption is required when transmitting personal information electronically or personal information must not be faxed or emailed to individuals.
- The consent requirements for personal information being disclosed. The requirements include
    - It must be in writing; and
    - Identify who the personal information can be disclosed to and for what purpose (as per ATIPP Act regulation 2(1));
- How disclosures will be logged. If there is a prescribed form when disclosing information, include this in the procedures or policy.
- An individual who is responsible for authorizing the disclosure of personal information for secondary uses or disclosing personal information without consent.
    - Program managers should also identify whether any foreseen secondary uses or disclosures of the information. If there are foreseen disclosures of information (law enforcement, for example), the program manager should develop a standardized form for staff to use.

Safeguards

- Departments and/or programs need to ensure physical, technical and administrative safeguards are in place that are appropriate to the information.
    - For more information on safeguards, read *Guidance for Safeguarding Information Assets* (on the internal ATIPP site).
- The following factors should be considered when determining appropriate safeguards: sensitivity of the information; amount of the information; extent of distribution; format of the information; and type of storage.
- Make sure employees are aware of the importance of maintaining the security of confidentiality of personal information.

Accuracy

- Programs need to consider the sensitivity of the information and how the information used will impact the individual. For example, the greater the impact, the greater the weight to ensuring the information is accurate and complete.
    - Collecting information directly from individuals is the best means to ensure accuracy.
    - Programs can also build information systems which track and record any changes made to personal information.

Access

Programs should develop policies and procedures to enable individual's access to their personal information and should include:

- A timeline that individuals can expect a response by.
    - Responses should be made as quickly as possible.
    - Information must be given at no charge.
- An individual who is responsible to respond to requests for access or correction to personal information.
- The procedures around determining the release of the information.
    - Be sure not to disclose a third party's personal information unless you have received consent in the prescribed form (as per ATIPP Act regulation 2(1)).
    - Include rationale, in writing, for any information that was refused.
- Notifying individuals of their right to file a formal access to information request or request for correction (as per section 6 of ATIPP Act).

Accountability

- Departments and/or programs should communicate the title of any individual who is responsible for privacy for either the program or the department.
    - This information should be made publicly available or easily accessible (for example, posted on a website, publications, brochures etc …).
- Department and/or program staff should confirm in writing they have read and understood any policies or procedures that apply to them.

Openness

- Ensure the following information and procedures are available to the public:
    - Title and contact information of the person who is accountable for your department's privacy policies and procedures.
    - Title and contact information of the person to who requests for information should be sent, including the contact information to the ATIPP office (for formal ATIPP requests).
    - How an individual can gain access to their personal information.
    - How an individual can complain to your organization.

Challenging Compliance

Departments and/or programs should develop policies and procedures that identify:

- How a complaint is to be received.
    - The date a complaint is received, the contact information of the complainant and the nature of the complaint must be recorded.
- How many days and in what format the acknowledgement of the complaint is to be sent to the complainant.
    - Include the title and contact information of the individual who is responsible to resolve the complaint.
        - Note: appoint individuals who will be impartial.
    - Include timelines for how long it will take to resolve the complaint.
- How notification will occur. Notification should be in writing and include:
    - Notification of the outcome, including any steps taken to resolve the issue (if taken).
    - Notification of the individual's right to request information or a correction of personal information through the ATIPP office.
    - Notification of the individual's right to complain to the Office of the Information and Privacy Commissioner.