Privacy Impact Assessment - Key Elements

PIPA requires an organization to collect, use or disclose personal information in accordance with the act, and to protect personal information in its custody or control by making reasonable security arrangements. Although Privacy Impact Assessments (PIAs) are not required under PIPA, they assist organizations to comply with PIPA obligations and identify and address potential privacy risks. An organization can ask the Office of the Information and Privacy Commissioner for B.C. to review a draft or final PIA and provide non-binding guidance.

The final PIA should be signed by the head of the organization or an authorized representative.

Characterize the Initiative

This section provides an outline of the project, including the following elements:

- Title of initiative
- Name of organization and name/contact information for person completing the PIA
- Overview of the Initiative, including the:
    - purpose of the project
    - relationship between this purpose and the public body's mandate
    - description of the project
    - description of the parties/stakeholders involved and how they are involved
    - description of the data-linking initiative or common/integrated program or activity (if applicable)
- Expected implementation date

Analyze the Personal Information

This section analyzes the type of personal information and the privacy implications involved including:

- Describe the personal information that will be collected, used, and/or disclosed as part of the initiative.
- Describe how the personal information will be collected, used and disclosed.
    - Prepare a personal information flow diagram that indicates how the personal information will be transmitted or exchanged within and outside the organization.
    - Prepare a table indicating the legal authority for each collection, use and disclosure including the type of consent used (express, implied, opt-out) or the applicable exception to consent.
- Outline the contents of the collection notice.
- Determine the reasonableness of information being collected.

    - Personal information can only be collected for purposes that a reasonable person would consider appropriate in the circumstances.
- Assess the necessity for the collection, use or disclosure for providing the product or service.**Privacy Impact Assessment - Key Elements**
    - If consent is a condition of supplying a product or service, an individual cannot be required to consent to collection, use, or disclosure of personal information beyond what is necessary to provide that product or service.
    - Define the process for individuals to withdraw consent.
    - Individuals have the right to withdraw consent on giving reasonable notice to the organization and the organization must inform the individual of the likely consequence of withdrawing.

Assess the Privacy Risks

This section evaluates the privacy risks associated with the project including:

- Describe the privacy risks and the mitigation strategies in detail, including the:
    - risk of collecting or disclosing inaccurate personal information
    - risk of unauthorized access, possibly including a table describing role based access
    - risk of re-identification of anonymized data and
    - unnecessary retention of personal information (after it's no longer necessary for the purposes collected)
- Describe the proposed measures to mitigate those risks and include a table setting out the privacy risk mitigation measures.
    - Include residual privacy risks after taking into account the proposed mitigation measures.
    - Analyze whether the residual privacy risk is proportional to the benefits of the project for the individuals whose personal information is involved.
- Include a PIA post-implementation evaluation plan to monitor and review the initiative to determine whether the project is operating as envisioned in the PIA.
    - Revise and adapt the PIA as the program develops to reflect how the project is addressing privacy rights and privacy risks.

Privacy Management Program

This section outlines the organization's Privacy Management Program.

- Describe who is responsible for the program and their contact information.
- Describe privacy training and materials.
- Ensure Information security policies exist and the following measures are in place:
    - Physical security measures
    - Technical security measures (including where the data is stored and where it can be accessed from)

    - Organizational security measures**Privacy Impact Assessment - Key Elements**
    - Access controls and access logs
- Describe the plan to be implemented in the event of a privacy breach
- Describe the process for how information is kept accurate, how corrections can be requested
- Include information about how long information is retained (records management/retention schedules) and how it is disposed

See guidance document: Getting Accountability Right with a Privacy Management Program