Privacy Impact Assessment Policy

Purpose

The purpose of this policy is to ensure the development and maintenance of privacy impact assessments (PIAs) in a manner that is transparent and consistent with any orders, guidelines, fact sheets and best practices issued by privacy commissioners. CIHI is a prescribed entity under Ontario's Personal Health Information Protection Act (PHIPA) and conducting PIAs is an essential aspect of CIHI's Privacy Program.

PIAs are viewed as critically important by CIHI and its stakeholders. The application of this policy and the resulting PIAs demonstrate that privacy principles are being taken into account during the design, implementation and evolution of CIHI's programs and initiatives. Conducting a PIA includes developing measures intended to mitigate and, wherever possible, eliminate identified risks in keeping with CIHI's Privacy and Security Risk Management Framework and related policy.

At CIHI, the chief privacy officer (CPO) has been delegated day-to-day authority to manage the Privacy Program, and the chief information security officer (CISO) has been delegated day-to-day authority to manage the Information Security Program.

At CIHI, the director of a business area owns the PIA while the conducting of PIAs is a shared responsibility. Business area staff (or the project manager, as the case may be) and Privacy and Legal Services (PLS) staff collaborate to develop the PIA. The PIA report may be written by business area staff with assistance from PLS staff or vice versa. Use of external privacy consultants in the development of a PIA must be coordinated through PLS.

Scope

This policy addresses CIHI programs and initiatives involving the collection, use or disclosure of personal health information, health workforce personal information and employee personal information.

Definitions

“Privacy impact assessment (PIA)” means a process by which privacy, confidentiality and security issues associated with the collection, use or disclosure of personal information are assessed based on the 10 principles of the Canadian Standards Association’s Model Code for the Protection of Personal Information.

“Personal Information” means personal health information, health workforce personal information and employee personal information.

“Personal health information” means health information about an individual that identifies the specific individual, may be used or manipulated by a reasonably foreseeable method to identify the individual, or may be linked by a reasonably foreseeable method to other information that identifies the individual.

“Health workforce personal information” means information about a health service provider that identifies the specific individual, may be used or manipulated by a reasonably foreseeable method to identify the individual, or may be linked by a reasonably foreseeable method to other information that identifies the individual.

“Employee personal information” means personal information about an individual that is collected, used or disclosed for purposes of establishing, managing or terminating an employment relationship between CIHI and that individual. It includes but is not limited to information related to the hiring process, administration of compensation and benefit programs, performance appraisals, disciplinary proceedings and promotion planning.

Policy

1. Circumstances in which PIAs are required

PIAs are required to be conducted in the following circumstances:

- For existing and proposed data holdings involving the collection, use or disclosure of Personal Information;
- Whenever a substantive change to an existing data holding involving Personal Information is contemplated; and
- For any other programs and initiatives with privacy implications, as recommended by the CPO in consultation with the program area.

1.1 Process for identifying when PIAs are to be completed

- For proposed data collections, the determination of whether a privacy impact assessment or a data management plan will be put in place is made by the Executive Committee as set out in Section 1.4 of *Privacy Policy Procedures*.
- For existing data holdings, see process under Section 3 below.

2. Circumstances in which PIAs are not required

Where applicable, the rationale for undertaking a data management plan instead of conducting a privacy impact assessment, based on the minimum level of risk involved, must be documented.

A data management plan may be used in certain limited circumstances where a full PIA is not required given the minimal level of risk involved. An example would be where a small set of Personal Information is brought into CIHI to conduct a proof of concept. In this circumstance, an initial data management plan is to be prepared to ensure that the required processes for the collection, use, disclosure and retention or disposal of the Personal Information are followed. A full PIA would be undertaken at such time that it was determined that broader collection would occur.

Use of a data management plan must form part of the approval process for new collections of Personal Information under section 1 of CIHI's *Privacy Policy Procedures*.

The director of the applicable business area owns the data management plan. Development of the data management plan is a shared responsibility between program area staff and PLS.

Data management plans will be undertaken in accordance with this policy, with the exception of the following:

- Data management plans will be approved by the responsible director; and
- Data management plans will not be published.

3. Timing for conducting and reviewing PIAs

PIAs will be undertaken beginning at the conceptual design stage of the new or updated program or initiative and will be reviewed and amended, if necessary, during the detailed design and implementation stage.

The CPO is responsible for ensuring that a timetable is developed to ensure existing PIAs are conducted and reviewed. At a minimum, PIAs are to be reviewed annually by the responsible director[i] to ensure that they continue to be accurate and to be consistent with the information practices of CIHI. Such reviews will ensure that PIAs are updated when

- Substantive changes occur to the functionality, purposes, data collection, uses, disclosures, relevant agreements or authorities for a program or initiative that are not reflected in its PIA;
- Discrepancies exist between the content of existing PIAs and actual practices or processes; or
- Other changes occur that may potentially affect the privacy and security of those programs and initiatives.

At any other time, the CPO may determine that an update of a PIA or a new PIA is required and recommend same.

4. Required content of PIAs

The required content of PIAs include

- The data holding, program or initiative at issue;
- The nature and type of Personal Information collected, used or disclosed or that is proposed to be collected, used or disclosed;
- The sources of the Personal Information;
- The purposes for which the Personal Information is collected, used or disclosed or is proposed to be collected, used or disclosed;
- The reason that the Personal Information is required for the purposes identified;
- The flows of the Personal Information;
- The limitations imposed on the collection, use and disclosure of the Personal Information;
- Whether or not the Personal Information is or will be linked to other information;
- Whether or not the Personal Information will be de-identified and/or aggregated and the specific purposes for which and circumstances in which the de-identified and/or aggregate information will be re-identified, if any, and the conditions or restrictions imposed;

i. The responsible director is the owner of the PIA and may be the data holding custodian, the director responsible for the initiative or process, or the project business owner.

- The statutory authority for each collection, use and disclosure of Personal Information identified;
- The retention period for the records of Personal Information;
- The secure manner in which the records of Personal Information are or will be retained, transferred and disposed of;
- The functionality for logging access, use, modification and disclosure of the Personal Information and the functionality to audit logs for unauthorized use or disclosure;
- The risks to the privacy of individuals whose Personal Information is or will be part of the data holding, program or initiative and an assessment of the risks;
- Recommendations to address and eliminate or reduce the privacy risks identified; and
- The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the Personal Information.

5. Statements of purpose

Statements of purpose are included in PIAs in Section 3.4, Principle 2: Identifying purposes for personal health information. PIAs are posted on CIHI's external website and will be provided on request to health information custodians or other persons or organizations from whom the Personal Information in the data holding is collected.

Statements of purpose must

- Set out the purposes for which the Personal Information is collected, used or disclosed or is proposed to be collected, used or disclosed;
- Describe the nature and type of Personal Information collected, used or disclosed or that is proposed to be collected, used or disclosed;
- Identify the sources of the Personal Information;
- Explain the reasons that the Personal Information is required for the purposes identified; and
- Explain why de-identified and/or aggregated information will not serve the identified purpose.

6. Privacy and security risk management assessments for PIAs

The privacy, confidentiality and security risks associated with the data holding, program or initiative for which the PIA is being undertaken must be identified and assessed using CIHI's *Privacy and Security Risk Management Framework*.

Privacy and security risk management (PSRM) assessments must be undertaken for all new data holdings, programs or initiatives.

For existing data holdings, programs or initiatives, substantive changes to the functionality, purposes, data collection, uses, disclosures, relevant agreements or authorities for a data holding, program or initiative may require the conducting of a PSRM assessment as recommended by the CPO in consultation with the program area.

Privacy and security risks associated with the PIA process are to be assessed, treated and monitored as set out in CIHI's *Policy on Privacy and Security Risk Management* and its PSRM methodology.

7. PIA findings and recommendations

PLS maintains a log of all privacy-related recommendations, including recommendations resulting from PIAs and their associated PSRM assessment. The log identifies

- The staff responsible for addressing, monitoring and ensuring the implementation of the recommendations;
- The date that each recommendation was or is expected to be addressed;
- The manner in which each recommendation was or is expected to be addressed; and
- The evaluation of the residual risk remaining after implementation of the mitigations and recommendations.

PLS feeds this information into CIHI's Master Log of Action Plans, where it will be monitored and reported on at the corporate level. The owner of the individual action plan (vice president or director) is responsible for documenting the recommendations and the actions taken (or planned) to address these. Furthermore, each owner of the action plan is required to provide regular updates/presentations to the Senior Management Committee. Regular updates will continue to be provided until such time as the recommendations are fully implemented.

8. PIA log

PLS maintains a log of PIAs that have been completed, that have been undertaken but that have not been completed, and that have been identified but have not been undertaken. The log contains

- The name of the program, data holding or initiative involving Personal Information that is at issue;
- The date that the PIA was completed or is expected to be completed;
- The name(s) of the staff responsible for completing or ensuring the completion of the PIA; and
- If the PIA will not be undertaken, the log will state the reason, the name of the staff responsible for making this determination, and the date the determination was made.

9. PIA approval process

PIAs require final sign-off before publication or external dissemination; this sign-off must be from both the vice president/executive director of the relevant program area and the CPO.

Approval process documentation must include a final version of the PIA and the associated PSRM assessment (if applicable). Where the PSRM assessment forms part of the approval documentation, it will not be included in the published version of the PIA.

10. Publication

Once the PIA has been approved, pursuant to Section 9 above, the CPO makes it or a summary of it publicly available, including posting it on CIHI's website where and when it is appropriate to do so.

11. Compliance, audit and enforcement

- *CIHI's Code of Business Conduct* describes the ethical and professional behaviour related to work relationships, information — including personal health information — and the workplace. The code requires all staff to comply with the code and all of CIHI's policies, procedures and practices.
- Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*, which requires staff to immediately report incidents and breaches to incident@cihi.ca, including non-compliance with this policy.
- The chief privacy officer is responsible for ensuring compliance with privacy policies, procedures and practices. The chief information security officer is responsible for ensuring compliance with information security policies, procedures and practices.
- Violations of the code — including violation of privacy and security policies, procedures and practices — are referred to People, Culture and Learning, as appropriate, and may result in disciplinary action up to and including dismissal, in accordance with the CIHI *Employee Discipline Guidelines*.
- Compliance is monitored through either CIHI's *Privacy Audit Policy* or CIHI's Information Security Audit Program as applicable.

Roles and responsibilities

The chief privacy officer is responsible for the development, implementation and oversight of this policy.

Related policies and procedures/ supporting documents

CIHI's Code of Business Conduct

Policy on Privacy and Security Risk Management

Privacy and Security Risk Management Framework

For more information, please contact

privacy@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Privacy Impact Assessment Policy*. Ottawa, ON: CIHI; 2025.