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 one 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, initiatives, processes and systems. 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 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 conduct 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, initiatives, processes and systems involving the collection, access, use or disclosure of personal health information, health workforce personal information and employee personal information (collectively known as "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 any factual or subjective information, regardless of its format, that can be used, either alone or in combination with other information, to identify an individual, including photographs and videos. Personal Information does not include information that relates to an individual's business position or function (e.g., position or title, business address, business telephone number or email address).

"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. PIAs will be conducted in the following circumstances:
    - On existing programs, initiatives, processes and systems when substantive changes relating to the collection, use or disclosure of personal information are being implemented;
    - In the design of new programs, initiatives, processes and systems that involve the collection, use or disclosure of personal information or otherwise raise privacy issues. PIAs will be reviewed and amended as necessary during the design and implementation stage; and
    - On any other programs, initiatives, processes and systems with privacy implications, as recommended by the CPO in consultation with the business area or project management.

Specifically, PIAs will be undertaken beginning at the conceptual design stage of the new or updated program, initiative, process or system and continuing through the detailed design and implementation stage.

2. At a minimum, PIAs must describe
    - The program, initiative, process or system 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 the personal information is required for the purposes identified;
    - The flows of the personal information;
    - The statutory authority for each collection, use and disclosure of personal information identified;
    - 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 PHI 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, as well as the conditions or restrictions imposed in that regard;
    - 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 used to log the access, use, modification and disclosure of the personal information and the functionality used 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, information system, technology or program, 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.

Statements of purpose for data holdings

3. Each of CIHI's data holdings requires a PIA and a corresponding statement of purpose.
4. The CPO has been delegated day-to-day authority to manage the Privacy Program in respect of the statements of purpose.
5. Statements of purpose are included in the PIAs. These documents 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 health information in the data holding is collected.
6. The CPO is responsible for ensuring that a timetable is developed to ensure PIAs are conducted.

Data management plan

7. A data management plan may be used in certain limited circumstances where a full PIA is not required. An example would be where a small set of personal health information is brought into CIHI (after approval under Section 1 of CIHI's Privacy Policy Procedures) 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 health 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 will be considered as part of the approval process for new collections of personal health information under Section 1 of CIHI's Privacy Policy Procedures.

   Data management plans will be undertaken in accordance with the PIA 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.

Privacy and security risk management

8. Privacy and security risks identified during a PIA process are to be assessed, treated and monitored as set out in CIHI's *Policy on Privacy and Security Risk Management*.

PIA approval process

9. PIAs require final sign-off before publication or external dissemination from both the vice president/executive director of the relevant business area and the CPO.

Recommendation implementation

10. PLS maintains a log of all privacy-related recommendations, including recommendations resulting from PIAs and privacy and security risk management assessments. The log identifies the employee(s) responsible for addressing, monitoring and ensuring the implementation of the recommendations; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed. 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.

PIA updates/renewals

11. The responsible director[i] is to ensure that PIAs are to be updated when
    - Substantive changes occur to the functionality, purposes, data collection, uses, disclosures, relevant agreements or authorities for a program, initiative, process or system that are not reflected in its PIA;
    - Discrepancies exist between the content of existing PIAs and actual practices or processes; and
    - Other changes occur that may potentially affect the privacy and security of those programs, initiatives, processes and systems.

At minimum, PIAs are to be renewed every 5 years, as set out in the schedule in the PIA log.

The CPO may determine that an update of a PIA or a new PIA is required and recommend same.

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

Annual review

12. In order to ensure the continued accuracy of PIAs and in order to ensure that the personal health information collected for purposes of the data holding is still necessary for the identified purposes, responsible directors are to review annually any existing PIAs and statements of purpose for discrepancies between their content and actual practices or processes, and to advise the CPO of any discrepancies. Together, they will determine whether an update is required.
13. Any updates to PIAs, including updates to statements of purpose, require sign-off before publication or external dissemination from both the vice president/executive director of the relevant program area and the CPO.
14. Updates to PIAs, including updates to statements of purpose, are included in the PIAs. These documents 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 health information in the data holding is collected.

Publication

15. Once the PIA has been approved, pursuant to Section 4 above, the CPO makes it or a summary of it publicly available, including by posting it on CIHI's website where and when appropriate to do so.

PIA log

16. PLS maintains a log of PIAs that have been completed, that have been undertaken but that have not been completed and that have not been undertaken. The log contains
    - The name of the program, initiative, process or system involving personal information that is at issue;
    - The date that the PIA was completed or is expected to be completed; and
    - The name(s) of the employee(s) responsible for completing or ensuring the completion of the PIA.

Compliance, audit and enforcement

17. *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 employees to comply with the code and all of CIHI's policies, protocols and procedures. Compliance is monitored through CIHI's Privacy Audit Policy. Violations of the code — including violation of privacy and security policies, procedures and protocols — are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Notification of breach

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.

Related policies/procedures and supporting documents

CIHI's Code of Business Conduct

Privacy and Security Incident Management Protocol

Policy on Privacy and Security Risk Management

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; 2023.