Canadian Institute for Health Information

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. Through the publication of PIA reports, CIHI can demonstrate that privacy principles are being taken into account during the design, implementation and evolution of its programs, initiatives, processes and systems. Conducting a PIA includes developing measures intended to mitigate and, wherever possible, eliminate identified risks. An essential element of the PIA process is the implementation of any recommendations flowing from the assessment.

At CIHI, PIAs are a shared responsibility. Program 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 program 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").

Canadian Institute for Health Information
Institut canadien d'information sur la santé

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 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 to assess risks to privacy in the following circumstances:
    - On existing programs, initiatives, processes and systems when significant 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 chief privacy officer (CPO) in consultation with the program area or project management.

    Specifically, PIAs will be conducted at the conceptual design stage and will be reviewed and amended, if necessary, during the detailed design and implementation stage.

2. At a minimum, PIAs must describe
    - The data holding, information system, technology or program 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;
    - 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.

PIA Approval Process

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

Recommendation Implementation

4. PLS maintains a log of all privacy-related recommendations, including recommendations resulting from PIAs. The log contains the recommendations arising from the PIA; 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 prioritized action items, including 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.

Annual Review

5. Directors are responsible for reviewing annually any existing PIAs for discrepancies between their content and actual practices or processes, and for advising the CPO of any discrepancies. Together, they will determine whether an update or a new PIA is required.

PIA Updates/Renewals

6. PIAs are to be updated
    - When significant 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;
    - When other changes occur that may potentially affect the privacy and security of those programs, initiatives, processes and systems;
    - When the CPO determines that an update of a PIA or a new PIA is required and recommends same; or
    - Every 5 years at a minimum.

Publication

7. Once the PIA has been approved, pursuant to Section 3 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.

Monitoring

8. PLS shall maintain 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 shall contain
    - The name of the data holding, information system, technology or program 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.

Non-Compliance and Audit Monitoring

9. The *CIHI Code of Business Conduct* describes the ethical and professional behaviour related to work relationships, information (including personal health information) and the workplace. All employees are required to comply with the code and all of CIHI's policies, protocols and procedures. Compliance with CIHI's Privacy Program is monitored through CIHI's risk-based Privacy Audit Program, as set out in a multi-year audit plan.

10. Instances of non-compliance with privacy and security policies are managed through CIHI's *Privacy and Security Incident Management Protocol*.

Violations of the code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Related Policies/Procedures and Supporting Documents

CIHI Code of Business Conduct

Privacy and Security Incident Management Protocol

For More Information please contact:

privacy@cihi.ca