Privacy Audit Policy

Purpose

The purpose of this policy is to set out the requirements of privacy audits conducted by the Canadian Institute for Health Information (CIHI).

Scope

This policy addresses CIHI programs, initiatives, processes and systems involving the collection, use or disclosure of personal health information or health workforce personal information, as well as de-identified data derived from personal health information or health workforce personal information.

Definitions

“Confidential information” means any information that is sensitive in nature and that must be secured against loss or theft, as well as unauthorized access, disclosure, copying, use or modification throughout its life cycle. Confidential information includes, but is not limited to, health-related information (personal health information, de-identified data, confidential aggregate data, health workforce personal information) and confidential or restricted business records, which include technical information and employee personal information.

“De-identified data” means personal health information or health workforce personal information that has been modified using appropriate de-identification processes so that the identity of the individual cannot be determined by a reasonably foreseeable method.

“Health workforce personal information” means information about a health service provider that identifies the 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.

“IT services organization,” for the purposes of this policy, means the third-party organization, as defined under the applicable agreement with CIHI, that is accessing confidential CIHI information for the purpose of storing and managing this information on behalf of the principal organization.

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

"Personal health information" means health information about an individual that identifies the 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.

"Principal organization," for the purposes of this policy, means the third-party organization ultimately accountable for data protection and security of confidential CIHI information, and for the actions of authorized persons, in compliance with the obligations outlined in the applicable agreement with CIHI.

"Staff" means any worker at CIHI, including all full-time or part-time employees, employees on secondment to CIHI, temporary workers, students and contract employees, including external consultants or other third-party service providers whose role includes access to CIHI data or information systems as defined in CIHI's internal *Acceptable Use Policy*.

Policy

1.0 Privacy audits

1.1 The chief privacy officer is delegated day-to-day authority to manage CIHI's Privacy Program. Privacy audits will be conducted under this program in accordance with the audit schedule presented in CIHI's Annual Privacy Audit Plan.

1.2 The chief privacy officer is responsible for developing and maintaining CIHI's Annual Privacy Audit Plan and for ensuring the plan is approved annually by the Governance and Privacy Committee of CIHI's Board of Directors.

1.3 CIHI will conduct internal privacy audits to assess compliance with CIHI's privacy and security policies, procedures and practices. Audits ensuring CIHI staff are permitted to access and use personal health information pursuant to CIHI's privacy and security policies, procedures and practices are carried out under CIHI's Information Security Management System (ISMS), including related audits. At a minimum, audits of agents granted approval to access and use personal health information under Section 10 of CIHI's *Privacy Policy Procedures* must be conducted on an annual basis.

1.4 CIHI will conduct third-party privacy audits of external recipients of personal health information, health workforce personal information and de-identified data derived from personal health information or health workforce personal information to assess compliance with the terms of the disclosure agreement governing the use of CIHI data and make recommendations to address any issues identified.

2.0 Requirements of privacy audits

2.1 The nature and scope of privacy audits will be described in CIHI's Annual Privacy Audit Plan. Privacy audits may include in-person visits (including remote site visits), inspections, document reviews and interviews, as CIHI sees fit.

2.2 The scope of third-party privacy audits will include the principal organization and the IT services organization(s), as applicable.

2.3 Privacy audits will be conducted by CIHI's Privacy and Legal Services branch staff or by staff contracted to perform the privacy audit, in collaboration with CIHI's Information Security department as required.

2.4 Privacy audits will be conducted in accordance with the audit schedule presented in CIHI's Annual Privacy Audit Plan or on an ad hoc basis in response to emergent privacy and security risks (e.g., incident and breach response processes), or in response to external factors such as an investigation, recommendation or order from a privacy commissioner/ombudsperson.

3.0 Privacy audit process

3.1 Criteria considered in selecting the subject matter of internal privacy audits include assessment information arising from compliance with CIHI's *Privacy Impact Assessment Policy*, *Policy on Privacy and Security Risk Management* and *Privacy and Security Incident Management Protocol*, or from external factors such as an investigation, recommendation or order from a privacy commissioner/ombudsperson. Criteria considered in selecting the subject matter of third-party privacy audits will be described in CIHI's Annual Privacy Audit Plan and will include, for example, proposed changes in the use of data disclosed to a third party, the complexity of project data management, disclosure of personal health information, and CIHI's assessment of sources of current and emergent privacy and security risks associated with the disclosure of CIHI data to third-party organizations.

3.2 Notification of a privacy audit, in the format required by the chief privacy officer, will be provided for both internal and third-party privacy audits. The chief privacy officer (or designate) will issue notification for internal privacy audits and third-party privacy audits.

3.3 Notification of a privacy audit will be issued in writing, in accordance with the associated agreement where applicable, and will include the policy or contractual basis for conducting the audit, the contact information of the CIHI staff conducting the audit, the nature and scope of the audit, potential participants to be included in any audit-related interviews or inspections, and the proposed timing for the audit.

3.4 Documentation will be created, received and maintained in the format required by the chief privacy officer as evidence of the administration and operations of CIHI's privacy audits and/or to support legal obligations. Such documentation will include lists of audit participants present for meetings, records of site visits and inspections, audit assessment questionnaires developed and utilized for the purpose of conducting the audit, documentation submitted or collected for the purpose of conducting the audit, written confirmations of acceptance and internal approval, the final audit report, and findings, mitigations and recommendations arising from the audit.

3.5 CIHI staff conducting a privacy audit are responsible for completing privacy audit documentation as required. Privacy audit documentation is maintained by CIHI's Privacy and Legal Services branch.

3.6 Upon completion of a privacy audit, an audit report in the format required by the chief privacy officer will be provided to the auditee. For internal privacy audits, an audit report will be provided to CIHI staff in the accountable area who are in a position of director or above. For third-party privacy audits, an audit report will be provided to an individual able to bind the principal organization and/or IT services organization(s).

4.0 Reviewing findings and addressing mitigations and recommendations[i] arising from privacy audits

4.1 Staff conducting a privacy audit will identify the primary contact of the auditee who is responsible for reviewing the findings of the privacy audit and for addressing mitigations and recommendations arising from the privacy audit, determine the associated timelines for addressing the mitigations and recommendations and obtain confirmation in writing from the auditee of acceptance of the audit report, including findings, mitigations and recommendations.

4.2 Staff conducting an internal privacy audit will obtain approval of the audit report from the relevant director or senior executive. Once the audit report has been approved, Privacy and Legal Services is responsible for ensuring all recommendations are entered into the Privacy Recommendation Log, and then into CIHI's Master Log of Action Plans. Subsequently, internal owners of a recommendation are responsible for providing regular updates to CIHI's Senior Management Committee. Monitoring by the Senior Management Committee will continue until such time as the recommendations are fully implemented. Internal owners are also responsible for evaluation of any residual risks remaining after the implementation of the mitigations and recommendations.

i. Mitigations not implemented prior to the finalization of the privacy audit report are considered to be recommendations.

4.3 Staff conducting a third-party privacy audit will obtain acceptance of the audit report, including findings, mitigations and recommendations, from an individual able to bind the principal organization and/or IT services organization(s).

4.4 For third-party privacy audits, Privacy and Legal Services staff are responsible for following up on mitigations and recommendations until the organization has confirmed that appropriate corrective action to address the mitigations and recommendations has been taken.

5.0 Privacy audit report

5.1 Staff conducting a privacy audit will prepare an audit report in the format required by the chief privacy officer and are responsible for delivering the audit report to the chief privacy officer upon conclusion of a privacy audit.

5.2 The format of a privacy audit report will typically include background information, a description of the audit scope and methodology, and audit findings, mitigations and recommendations.

5.3 The chief privacy officer (or designate) is responsible for communicating the findings, mitigations and recommendations of privacy audits, as well as determining the mechanism, manner, circumstances and format in which these will be communicated to internal and external audiences. This includes the level of detail for communicating the findings, mitigations and relevant recommendations, as well as the status of their implementation. Communication will occur at the earliest opportunity following the conclusion of the audit.

5.4 Findings, mitigations and recommendations arising from third-party privacy audits will be communicated to the auditee, and where findings may result in CIHI internal operational improvements, communication may also be directed to CIHI internal areas. Summary information derived from mitigations and recommendations arising from third-party audits will be communicated to the external audience of third-party organizations already in receipt of CIHI data, as well as organizations that are considering requesting CIHI data.

5.5 The chief privacy officer will report regularly on all auditing activities, including findings, mitigations and recommendations, to CIHI's Senior Management Committee and the Governance and Privacy Committee of CIHI's Board of Directors, which includes CIHI's president and chief executive officer.

6.0 Log of privacy audits

6.1 The chief privacy officer (or designate) will establish and maintain a log of privacy audits. At a minimum, the log will capture the following information about a privacy audit: the nature and type conducted; the date completed; the agent(s) responsible for completing it; the findings, mitigations and recommendations arising from it; the agent(s) responsible for addressing each mitigation and recommendation; the date each mitigation and recommendation was or is expected to be addressed; and the manner in which each mitigation and recommendation was or is expected to be addressed.

6.2 The chief privacy officer (or designate) is responsible for ensuring that the documentation relating to a privacy audit is maintained within the records of the Privacy and Legal Services branch.

7.0 Compliance, audit and enforcement

7.1 Staff conducting privacy audits will immediately notify CIHI at incident@cihi.ca of a privacy breach or suspected privacy breach, or of an information security breach or information security incident, in accordance with CIHI's *Privacy and Security Incident Management Protocol*.

8.0 Roles and responsibilities

8.1 The chief privacy officer is responsible for the development, implementation and oversight of this policy. The Governance and Strategy department is responsible for monitoring CIHI's Master Log of Action Plans. The Governance and Privacy Committee is responsible for approving CIHI's Annual Privacy Audit Plan on an annual basis.

Related procedures/supporting documents

Annual Privacy Audit Plan

Privacy and Security Incident Management Protocol

Requesting CIHI Data? What You Need to Know About CIHI's Privacy Audit Program

For more information, please contact

privacy@cihi.ca

How to cite this document:

Canadian Institute for Health Information. *Privacy Audit Policy*. Ottawa, ON: CIHI; 2025.