Canadian Institute for Health Information

Privacy Audit Policy

Policy: Privacy Audit Policy

Version number: 1.1

Policy owner: Chief Privacy Officer

Department/branch/division: Privacy and Legal Services

Effective date: September 2021

Approval authority: Executive Committee

Next revision date: March 2025

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, health workforce personal information, as well as de-identified data derived from personal health information or health workforce personal information.

Definitions

“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.

"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 Multi-Year Privacy Audit Plan.

1.2 The chief privacy officer is responsible for developing and maintaining CIHI's Multi-Year 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 and procedures. Audits ensuring CIHI staff are permitted to access and use personal health information pursuant to CIHI's privacy and security policies and procedures are carried out under CIHI's Information Security Management System (ISMS) Audit Program. At a minimum, audits of agents granted approval to access and use personal health information (PHI) under the Policy and Procedures for Limiting Agent Access to and Use of PHI 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 determined in accordance with CIHI's Multi-Year 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 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 Multi-Year 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 Multi-Year 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 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 department.

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 Addressing recommendations arising from privacy audits

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

4.2 Staff conducting an internal privacy audit will obtain acceptance of the audit report and recommendations from an individual in a position of director or above. Once the recommendations are accepted, the Privacy and Legal Services department is responsible for ensuring all recommendations are entered into the Privacy Recommendation Log, and then into CIHI's Master Log of Action Plans. Internal owners of a recommendation are responsible for providing regular updates/presentations to CIHI's Senior Management Committee. These updates will be provided until the recommendations are fully implemented.

4.3 Staff conducting a third-party privacy audit will obtain acceptance of the audit report 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 each recommendation until the organization has confirmed that appropriate corrective action to implement the recommendation 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, audit findings and observations, audit recommendations and opportunities for improvement.

6.0 Communication of privacy audit findings and recommendations

6.1 The chief privacy officer (or designate) is responsible for determining the manner, circumstances and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of their implementation, are communicated to internal and external audiences. This includes the mechanism and format for communicating the findings of the privacy audit, including the level of detail for communicating the findings. The findings of a privacy audit will be communicated at the earliest appropriate opportunity following the conclusion of the audit.

6.2 Recommendations resulting from internal privacy audits will be communicated to the department that underwent the audit, other CIHI departments directly impacted by the audit findings or more generally at CIHI through privacy and security awareness activities. Recommendations may be communicated by email or published on CIHI’s intranet.

6.3 Recommendations arising from third-party privacy audits will be communicated to the auditee. Where findings may result in improvements to CIHI’s internal operations, communications may also be directed to impacted CIHI departments. Summary information derived from recommendations arising from third-party privacy audits will be communicated to third-party recipients of CIHI data, as well as organizations that are considering requesting CIHI data.

6.4 The chief privacy officer will report regularly on all auditing activities, including findings 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.

7.0 Log of privacy audits

7.1 The chief privacy officer (or designate) will establish and maintain a log of privacy audits. At a minimum, the log will capture the recommendations arising from internal privacy audits, the individual(s) responsible for addressing each recommendation, the date each recommendation was or is expected to be addressed and the manner in which each recommendation was or is expected to be addressed.

7.2 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 department.

8.0 Incident and breach response

8.1 Staff conducting a privacy audit will respond to suspected or actual privacy or security incidents, or privacy or security breaches, in compliance with CIHI's *Privacy and Security Incident Management Protocol*.

Related procedures/supporting documents

Acceptable Use Policy

Information Security Management System Audit Manual

Multi-Year Privacy Audit Plan

Policy on Privacy and Security Risk Management

Privacy and Security Incident Management Protocol

Privacy Impact Assessment Policy

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

For more information, please contact us at privacy@cihi.ca.

Revision history

Date	Version	Description of revisions	Approval authority
September 2021	1.0	New policy	Senior Management Committee
March 2022	1.1	Minor revisions to address requirements of IPC/ON revised manual	Executive Committee