Personal Information Privacy Policy

Purpose

The Canadian Institute for Health Information (CIHI) is committed to processing Personal Information in accordance with its policies and practices and with relevant Privacy Laws. Privacy compliance is a team effort that requires the full cooperation of all Staff and involves using appropriate processes and technologies to ensure the appropriate handling and protection of Personal Information throughout the information life cycle, in accordance with CIHI's policies and procedures.

Scope

This policy applies to the collection, use, retention, access, disclosure, storage, or other processing or handling (collectively, "**processing**") of Personal Information in the custody or control of CIHI, including Personal Information that has been transferred to a service provider for processing on behalf of CIHI.

For the avoidance of doubt, this policy does not apply to the processing of employee personal information, which is covered by CIHI's *Employee Privacy Policy*. This policy also does not apply to the processing of Personal Health Information (**PHI**) nor to the processing of health workforce information (**HWFI**), which are covered by CIHI's *Privacy Policy* and *Health Workforce Privacy Policy*, respectively.

Definitions

Privacy Commissioner means any of the following Canadian privacy and information commissioners: the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner of Alberta or the Office of the Information and Privacy Commissioner of British Columbia.

Chief Privacy Officer or **CPO** means CIHI's Chief Privacy Officer and General Counsel (CPO/GC).

Individual means a CIHI customer, prospect, applicant, website visitor or other similar individual who interacts with CIHI.

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).

Privacy Laws means applicable laws and regulations relating to the processing and protection of Personal Information.

Sensitive Personal Information means Personal Information that, due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, entails a high level of reasonable expectation of privacy.

Service Provider means any third-party service provider, contractor or consultant retained by CIHI to provide services who requires and is authorized to access CIHI data or information systems as defined in CIHI's *Acceptable Use Policy*.

Staff means all full-time, part-time and contract employees of CIHI, individuals working at CIHI on secondments, students and temporary workers.

Website Privacy Notices means CIHI's Website Privacy Notice and Cookie Notice published on its external website, which describe how CIHI collects, uses and discloses Personal Information collected through its website, as well as the rights that website visitors have with respect to their Personal Information.

Policy

Consent

1. Consent is the legal authority that dictates how and for what purposes CIHI can collect, use and disclose an Individual's Personal Information.
2. Consent may be express (i.e., opt-in) or implied (i.e., Website Privacy Notices and subscription forms). Specifically, consent must be obtained expressly when the processing involves Sensitive Personal Information. Staff should contact Privacy and Legal Services (PLS) if they need consent or are unsure about the type or validity of consent required for processing Personal Information.
3. Unless otherwise permitted or required by law, CIHI must ensure it has obtained valid consent from Individuals prior to collecting, using and disclosing their Personal Information for legitimate purposes.

Collection, use and disclosure of Personal Information

Collection: General

4. CIHI collects the minimal amount of Personal Information required for the purpose(s).
5. CIHI collects only the Personal Information reasonably required in support of the following:
    a. To provide and deliver products and services, such as when an Individual registers to receive emails, newsletters, upcoming releases or career alerts from CIHI; signs up for a CIHI event; creates a profile on our website; or makes a purchase from CIHI's online store;
    b. To manage CIHI's business operations, including to respond to inquiries or requests about CIHI's products and services; to facilitate the use of CIHI's website (including through cookies and similar technologies); to ensure the security of the website; and to protect CIHI's properties, Individuals and the public against fraud or other types of harm;
    c. To verify an Individual's identity, including to allow access to appropriate/authorized areas of CIHI's website;
    d. To develop relationships with, understand the interests of and obtain opinions from Individuals about CIHI's products or services, including through the use of client relationship management (CRM) tools;
    e. To provide Individuals with personalized content and services, for instance by tailoring our products and services and our digital customer experience and offerings;
    f. To communicate with Individuals about CIHI's programs, products, services or events that may be of interest to them in compliance with the *CRM General Policies*.
    g. To establish, manage or terminate a relationship with a Service Provider; and
    h. To comply with applicable legal or contractual requirements.

Use and disclosure

6. CIHI must use and disclose Personal Information only in accordance with this policy.
7. More specifically, CIHI does not use or disclose Personal Information for purposes other than those for which it was collected as specified in Section 5, except with the consent of the Individual, or as authorized or required by law.

Use: General

8. CIHI uses Personal Information for the purposes set out in Section 5, in compliance with this policy.
9. CIHI allows only authorized Staff to access and use Personal Information on a need-to-know basis.

10. CIHI may allow Service Providers who are retained to process Personal Information on CIHI's behalf to access and use Personal Information on a need-to-know basis and subject to the following:
    a. CIHI must conduct a privacy and security assessment prior to providing access to Personal Information to the Service Provider to ensure that the Personal Information will be accurately protected. Privacy and security risks identified during an assessment must be assessed, treated and monitored as set out in CIHI's *Privacy and Security Risk Management Policy*;
    b. The Service Provider must enter into an information protection agreement or other legally binding instrument(s) with CIHI and meet the mandatory educational requirements in the areas of privacy and security as required under CIHI's *Privacy and Security Training Policy*;
    c. The Service Provider must comply with relevant privacy, security and confidentiality obligations as detailed in the information protection agreement or other legally binding instrument(s) with CIHI; and
    d. CIHI may impose any other requirement(s) as needed on a case-by-case basis to maintain the confidentiality of the Personal Information.
11. It is the responsibility of the procuring manager or delegate to consult with PLS and Information Security (InfoSec), as appropriate, to ensure that Personal Information is and will remain adequately protected prior to engaging a Service Provider as required under CIHI's *Supplier Management Framework*.
12. CIHI remains accountable for Personal Information provided to Staff and Service Providers, and ensures that Personal Information is used, disclosed, retained and disposed of by Staff and Service Providers in accordance with this policy.
13. Consistent with its mandate and core functions, CIHI does not use Personal Information to make decisions about an Individual.

Disclosure: General

14. CIHI discloses Personal Information in compliance with all applicable consents and Privacy Laws.
15. CIHI does not disclose Personal Information except under the following limited circumstances:
    a. The request is from a Privacy Commissioner regarding CIHI's processing of Personal Information;
    b. The request is from law enforcement or a governmental authority seeking to obtain access to Personal Information under the custody or control of CIHI;
    c. The recipient has obtained the valid consent of the Individual concerned;
    d. The disclosure is otherwise authorized by law; or
    e. The disclosure is otherwise required by law.

16. CIHI will not disclose Personal Information if other information will serve the purpose of the disclosure, and CIHI will not disclose more Personal Information than is reasonably necessary to meet the purpose.
17. CIHI must conduct a privacy and security assessment prior to disclosing any Personal Information to ensure that the Personal Information will be accurately protected. Privacy and security risks identified during an assessment are to be assessed, treated and monitored as set out in CIHI's *Privacy and Security Risk Management Policy*.
18. Staff must immediately inform PLS, which is under the direction of the CPO, if they receive any inquiry or request for disclosure of Personal Information.
19. The CPO is responsible for handling and responding to such inquiry, request or communication; consulting as appropriate with Staff or other stakeholders; and keeping records of the inquiry, request or communication received.

Accuracy, retention and destruction of Personal Information

Accuracy

20. CIHI must use Personal Information that is accurate, complete and up to date as is necessary for the purpose(s) for which the information is to be used and taking into account the interests of the Individual to whom the information relates.

Retention

21. CIHI retains Personal Information only for as long as necessary to fulfill the purpose(s) for which this information was originally collected, unless further retention is required for legitimate legal or business purposes.

Destruction

22. When Personal Information is no longer required to be retained, CIHI must securely destroy the information in accordance with CIHI's *Secure Destruction Standard*. Staff are responsible for complying with these requirements, including by using secure destruction methods when performing authorized destruction of Personal Information.

Individuals' access to and correction of Personal Information, information about processing and withdrawal of consent

Access, correction and request for information: General

23. CIHI respects Individuals' right to access and request the correction of their Personal Information and to obtain information about CIHI's processing of their Personal Information.
24. CIHI responds to Individuals' requests promptly and not later than 30 days from receipt of the request and at minimal or no cost to the Individual.
25. Individuals must direct their request to the CPO by submitting a written request to privacy@cihi.ca.
26. Staff receiving these requests must immediately forward the request to the CPO, who is responsible for responding to these requests in accordance with relevant legal and contractual obligations.

Request for information pertaining to decisions about the Individual, if applicable

27. Under a request for information pertaining to decisions about the Individual, CIHI must inform the Individual concerned of the following information:
    a. The Personal Information used to render a decision about the Individual, if applicable;
    b. The reasons and the principal factors and parameters that led to the decision; and
    c. The right of the Individual to have the Personal Information used to render the decision corrected.

Withdrawal of consent

28. Individuals have a right to withdraw their consent pertaining to CIHI's collection, use and disclosure of their Personal Information.
29. If CIHI receives a request to withdraw consent, CIHI must cease collecting, using and disclosing that Individual's Personal Information and must securely destroy the Personal Information.

Questions and complaints about privacy at CIHI

30. Questions, concerns or complaints about CIHI's handling of the Personal Information it holds should be addressed to CIHI's CPO as follows:

    Chief Privacy Officer
    Canadian Institute for Health Information
    495 Richmond Road, Suite 600
    Ottawa, Ontario K2A 4H6

    Phone: 613-694-6294
    Email: privacy@cihi.ca

31. The CPO is responsible for investigating any relevant and credible complaints pertaining to this policy, and for diligently responding to such complaints in a manner that respects CIHI's policies and procedures as well as legal and contractual requirements.
32. The CPO may direct an inquiry or complaint to the Privacy Commissioner of the jurisdiction of the Individual making the inquiry or complaint.
33. For other information on CIHI's privacy policies, procedures and practices, visit cihi.ca.
34. There will be no retaliation against any Individual for reporting violations or suspected violations of this policy, so long as the report is made in good faith.

Compliance, audit and enforcement

35. CIHI's *Code of Business Conduct* describes the ethical and professional behaviour related to work relationships, information — including Personal Information — and the workplace. The code requires all Staff to comply with the code and all of CIHI's policies, protocols and procedures.
36. 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

37. 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.

Roles and responsibilities

President and CEO

CIHI's President and CEO is ultimately accountable for CIHI's Privacy Program and has delegated specific responsibilities, including the day-to-day responsibility for compliance and administration of the Privacy Program, to the Chief Privacy Officer.

Chief Privacy Officer

CIHI has designated a Chief Privacy Officer as the person responsible for ensuring compliance with applicable Privacy Laws. The CPO may delegate these responsibilities, in whole or in part, to any other person. Any such delegation of responsibility must be in writing and reflected in CIHI's policies and procedures, including this policy, as appropriate.

The CPO works closely with the Chief Information Security Officer (CISO) to ensure that CIHI has policies, procedures and other practices in place that accurately reflect CIHI's activities and operations regarding information security and privacy.

For more information

cihilegal@cihi.ca

privacy@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Personal Information Privacy Policy*. Ottawa, ON: CIHI; 2023.