Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data

2010

Updated July 2019

1994 • 2019

Canadian Institute for Health Information

Institut canadien d'information sur la santé

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860
Fax: 613-241-8120
cihi.ca
copyright@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*. Ottawa, ON: CIHI; 2019.

Cette publication est aussi disponible en français sous le titre *Politique de respect de la vie privée relative à la collecte, à l'utilisation, à la divulgation et à la conservation des renseignements personnels sur la santé et des données dépersonnalisées, 2010*.

Table of contents

Part I: Introduction

Background

In the early 1990s, there were considerable gaps in information about Canada's health systems and the health of Canadians. Canadians wanted to know how well our health systems worked, how we could improve them and how healthy we were as a nation. But answers were difficult to find. To respond to these questions, the provinces, territories and the federal government created an independent, not-for-profit institute to help the public and those running Canada's health systems get a clearer picture of what's being spent on health care, what kind of care is being delivered, who's delivering it and the factors influencing the health of Canadians. Since then, government bodies, hospitals, health authorities, health professional colleges and associations, the media, the public and others have come to depend on the Canadian Institute for Health Information (CIHI) as an essential source of relevant, timely and dependable health information to assess the effectiveness of different parts of Canada's health systems and to plan for the future.

Mandate

CIHI's mandate is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care.

Flowing from its mandate, and in accordance with all applicable legislation, CIHI's core functions include

- Identifying health information needs and priorities;
- Coordinating and promoting standards and data quality;
- Developing comparable measures of health system performance;
- Conducting analyses in the areas of population health and health services;
- Developing national health indicators; and
- Building capacity and conducting education sessions.

Commitment to privacy and security

The Canadian Institute for Health Information is committed to protecting the privacy of individuals and ensuring the security of their personal health information. CIHI is a prescribed entity under Section 45 of the Ontario *Personal Health Information Protection Act* (PHIPA) and is authorized to collect personal health information for the purpose of analysis or compiling statistical information with respect to the management, evaluation or monitoring of the allocation of resources to or planning for all or part of Canada's health systems. As a prescribed entity, CIHI is subject to independent oversight by the Ontario Information and Privacy Commissioner and must have its information practices reviewed and approved by the Commissioner every 3 years. This review process provides the Canadian public with the assurance that CIHI's information management practices comply with PHIPA and with privacy and security standards of practice expected from the Commissioner. As a result, CIHI adheres to this and any other applicable privacy legislation.

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. The Privacy program includes the following key activities:

- Fostering a culture of privacy at CIHI;
- Analyzing and applying privacy-related policies;
- Administering a privacy audit program;
- Conducting an education and outreach program; and
- Collaborating with CIHI's information technology and security department.

CIHI is committed to safeguarding its IT ecosystem, to securing its data holdings and to protecting health information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information. These safeguards protect CIHI's data holdings against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

To this end, CIHI has in place a Privacy and Security Framework ("Framework") that provides a coherent and comprehensive approach to enterprise privacy and security management. The Framework is designed to enable the effective integration and coordination of CIHI's privacy and security policies, and to provide CIHI's decision-makers, privacy and security officers and the entire governance structure with a holistic view of the organization's information management practices. It is intended to be a living document, updated as CIHI's privacy and security programs evolve over time.

The Framework has been informed by best practices for privacy and information management across the public, private and health sectors. The Framework is modular, thus offering CIHI the flexibility to share accountability across lines of business and to identify areas for improvement and develop action plans specific to particular components of the Framework.

CIHI is committed to the principle of openness about the management of personal health information and de-identified data. As such, CIHI makes its Framework and its Privacy Policy publicly available.

Policy objective

The purpose of this policy is to protect the privacy of Canadians and ensure that personal health information and de-identified data resulting from personal health information are collected, used, disclosed, retained and disposed of in a manner consistent with this policy and in accordance with applicable laws and agreements.

Effective date

This Privacy Policy is in effect as of March 2010.

Definitions

aggregate data

Data that has been compiled from record-level data to a level of aggregation that ensures that the identity of individuals cannot be determined by reasonably foreseeable methods. Aggregate data with units of observation less than 5 may constitute either de-identified data or personal health information.

collect

Collect, in relation to personal health information, means to gather, acquire, receive or obtain the information by any means from any source and “collection” has a corresponding meaning.

data linkage

The bringing together of 2 or more records of personal health information or de-identified data to form a composite record for a specific individual.

data provider

An organization, health care provider or other individual that discloses health information to CIHI, which may include ministries of health, regional health authorities and similar bodies, hospitals, other health care facilities and professional colleges.

de-identification processes

Such processes include but are not limited to

- Removal of name and address, if present; and
- Removal or encryption of identifying numbers, such as personal health number and chart number;

and may also involve

- Truncating postal code to the first 3 digits (forward sortation area);
- Converting date of birth to month and year of birth, age or age group; or
- Converting date of admission and date of discharge to month and year only;

and then

- Reviewing the remaining data elements to ensure that they do not permit identification of the individual by a reasonably foreseeable method.

Methodologies, standards and best practices, in addition to those listed above, may evolve and be developed from time to time and followed, as appropriate, to de-identify personal health information.

de-identified data

Personal health 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.

disclose

To release or make available personal health information or de-identified data other than to the original data provider or the individual the information concerns.

health information

A broad term including but not limited to financial information about health and health care, personal health information, de-identified data and aggregate data.

health system use

Health system use of data is the use of health information for clinical program management, health system management, surveillance, and research, all of which lead to improved patient care and health outcomes.

personal health information (PHI)

Health information about an individual that

- Identifies the specific individual; or
- 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.

Personal health information does not include health workforce information, or health facility information as defined in CIHI's *Policy on Health Facility Identifiable Information, July 2015*.

residual disclosure

The combination of publicly released health information with other available information that reveals previously unknown information about an individual.

record-level data

Data in which each record is related to a single individual (also referred to as "micro data").

use

Use, in relation to personal health information in the custody or control of CIHI, means to handle or deal with the information or to apply the information for a purpose, and includes reproducing the information but does not include disclosing the information.

Part II: Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data

Minimal collection and purpose

1. CIHI only collects from data providers, personal health information and de-identified data that is reasonably required for health system uses, including statistical analysis and reporting.
2. CIHI only collects personal health information and de-identified data reasonably required in support of the management, evaluation or monitoring of the allocation of resources to, or planning for, the health care system in Canada, including support for the improvement of the overall health of Canadians.

Use, disclosure and retention

3. CIHI does not use personal health information if other information will serve the purpose and does not use more personal health information than is reasonably necessary to meet the purpose. CIHI de-identifies personal health information using the appropriate methodologies for de-identification (see definition of “de-identified data”). These and other methodologies as deemed appropriate and/or necessary enable CIHI to reduce the risks of re-identification and residual disclosure.
4. In general, names and addresses of patients are not collected and therefore are not held in CIHI data holdings. The only exceptions are in the case of the Canadian Joint Replacement Registry and the Canadian Organ Replacement Register which collect the names of individuals.
5. More specifically, CIHI does not use or disclose personal health information for purposes other than those for which it was collected as specified in sections 1 and 2, except with the consent of the individual, or as authorized or required by law.
6. Consistent with its mandate and core functions, CIHI may retain personal health information and de-identified data recorded in any way regardless of format or media, for as long as necessary to meet the identified purposes, with the exception of ad hoc linked data, which will be destroyed in a manner consistent with Section 29.

Use — General

7. CIHI uses personal health information and de-identified data in a manner consistent with its mandate and core functions as described in sections 1 and 2, and in compliance with all applicable legislation, including privacy legislation.
8. If CIHI were to use personal health information or de-identified data for a new purpose, it would document this purpose in a manner consistent with its *Privacy Impact Assessment Policy* and in compliance with all applicable legislation, including privacy legislation, prior to any such use.
9. In instances where CIHI collects direct identifiers such as health card number and name, these are generally removed from analytical files and used solely for the purposes of processing data.
10. CIHI allows only authorized staff and, in some circumstances, external consultants or other third-party service providers, to access and use specific data on a "need-to-know" basis, that is, when required to perform their duties and/or services, and only after they have met the mandatory educational requirements in the areas of privacy and security.
11. CIHI remains accountable for personal health information and de-identified data provided to staff and third-party service providers, and ensures that data is used, disclosed, retained and disposed of by staff and third-party service providers in accordance with this Privacy Policy, the relevant Confidentiality Agreements and in compliance with all applicable legislation.
12. CIHI may require certain external consultants or other third-party service providers to meet the mandatory education requirements under CIHI's *Privacy and Security Training Policy*.
13. Consistent with its mandate and core functions, CIHI does not use personal health information to make decisions about an individual's entitlement to health services and benefits or for any other administrative purpose related to the individual.

Use for data linkage — General

14. When carrying out data linkage, CIHI will generally do so without using names or personal health numbers; and where possible, CIHI will do so using the client linkage index or other comparable methodologies as may be developed from time to time.
15. The Chief Privacy Officer may consult with privacy commissioners or their equivalent and/or other government officials or bodies responsible for privacy protection (such as ethics review committees) prior to undertaking linkages of personal health information that are unusual, exceptional or precedent-setting in terms of their scope, scale, methods of linkage or other factors.
16. Results from the consultations referred to in Section 15 will be brought to the attention of the President and Chief Executive Officer for approval.
17. The linked data remain subject to the use and disclosure provisions in this Privacy Policy.

Use — Data linkage for CIHI purposes

18. Data linkage within a single data holding for CIHI's own purposes is generally permitted.
19. Data linkage across data holdings for CIHI's own purposes will be submitted to the Privacy, Confidentiality and Security Committee for approval when the requisite criteria set out in sections 22 to 27 are met.

Use — Data linkage by or on behalf of third parties

20. All third-party requests for data linkage will be submitted to the Privacy, Confidentiality and Security Committee for approval when the requisite criteria set out in sections 22 to 27 are met.
21. Requests for data linkage referred to in sections 19 and 20 may include linkages with CIHI data holding(s) and cohort files from the requesting third-party.

Use — Approval requirements for data linkage

22. Criteria for approval pursuant to sections 19 to 21 are as follows:
23. The individuals whose personal health information is used for data linkage have consented to the data linkage.

    OR

24. All of the following criteria are met:
    a. The purpose of the data linkage is consistent with CIHI's mandate;
    b. The public benefits of the linkage significantly offset any risks to the privacy of individuals (see Section 26);
    c. The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns (see Section 27);
    d. The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or
    e. The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and
    f. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

25. Any request for data linkage that is unusual, sensitive or precedent-setting shall be referred by the Privacy, Confidentiality and Security Committee to the President and CEO for approval.
26. For greater clarity, “public benefits” means the results of the linkage are expected to contribute to
    a. The identification, prevention or treatment of illness, disease or injury;
    b. Scientific understanding relating to health;
    c. The promotion and protection of the health of individuals and communities; or
    d. Improvements in health system policy, management and resource allocation.
27. For greater clarity, “detrimental” means the purpose of a data linkage is not to make decisions about an individual that would result in harm to the individual, such as being denied access to appropriate health services and/or benefits to which the individual is entitled.

Destruction of data, including linked data

28. CIHI destroys personal health information and de-identified data in a secure manner, using destruction methodologies appropriate to the format, media or device, such that reconstruction is not reasonably foreseeable.
29. For linked data resulting from time-limited specific projects, secure destruction will occur within 1 year after publication of the resulting report or analysis, or 3 years after linkage, whichever is sooner, in a manner consistent with CIHI’s Information Destruction Standard, as amended from time to time. For linked data resulting from a CIHI ongoing program of work, secure destruction will occur when the linked data are no longer required to meet the identified purposes, in a manner consistent with CIHI’s Information Destruction Standard, as may be amended from time to time.
30. On an exceptional basis, requests may be granted for a retention period for linked data longer than that specified in Section 29, based on approval by the Privacy, Confidentiality and Security Committee.
31. In all cases, destruction of personal health information and de-identified data will be in accordance with any applicable privacy legislation.

Public use

32. CIHI makes statistical information publicly available only in a manner designed to minimize any risk of identifiability and residual disclosure of information about individuals.
33. In general, CIHI makes publicly available aggregate data with units of observation no less than 5.

Return of own data to original data provider

34. CIHI may return personal health information or de-identified data to a data provider that originally provided the personal health information to CIHI or the relevant ministry of health for data quality purposes and for purposes consistent with their mandate, for example, for health services and population health management, including planning, evaluation and resource allocation.

35. Personal health information returned to an original data provider shall not contain additional identifying information to that originally provided.

36. For clarity, additional identifying information excludes other CIHI value-added data, such as derived variables, that CIHI routinely returns to data providers.

Disclosure — General

37. CIHI discloses health information and analyses on Canada's health systems and the health of Canadians in a manner consistent with its mandate and core functions. These disclosures typically fall into 1 of 4 categories:

    a. Disclosures to parties with responsibility for the planning and management of the health care system to enable them to fulfill those functions;

    b. Disclosures to parties with a decision-making role regarding health care system policy to facilitate their work;

    c. Disclosures to parties with responsibility for population health research and/or analysis; and

    d. Disclosures to third-party data requesters to facilitate health or health services research and/or analysis.

38. Prior to disclosure, CIHI reviews the requests to ensure that the disclosures are consistent with Section 37 and meet the requirements of applicable legislation.

39. For clarity, statistical information made available to the public, or return of own data to the original data provider for data quality or other purposes, is not considered a disclosure for purposes of this Privacy Policy.

Disclosure of personal health information

40. CIHI will not disclose personal health information if other information will serve the purpose of the disclosure and will not disclose more personal information than is reasonably necessary to meet the purpose. CIHI does not disclose personal health information except under the following limited circumstances and where the recipients have entered into a data protection agreement or other legally binding instrument(s) with CIHI:

    a. The recipient has obtained the consent of the individuals concerned; or

    b. The recipient is a prescribed entity under Section 45 of Ontario's *Personal Health Information Protection Act, 2004* (PHIPA) for the purpose of analysis or compiling statistical information with respect to the management, evaluation or monitoring of the allocation of resources to or planning for all or part of the health system, including the delivery of services, provided the requirements of PHIPA and CIHI's internal requirements are met; or

    c. The recipient is a prescribed person under Subsection 13(1) O.Reg.329/04 of Ontario's PHIPA for the purposes of facilitating or improving the provision of health care, provided the requirements of PHIPA and CIHI's internal requirements are met; or

    d. The disclosure is otherwise authorized by law; or

    e. The disclosure is required by law.

Requirements for disclosure of personal health information

41. For greater certainty, where the recipient has obtained the consent of the individuals concerned pursuant to paragraph 40a, prior to disclosure, the recipient must sign a data protection agreement or other legally binding instrument(s) that, at a minimum, contains the following requirements:

    a. Prohibits linking the personal health information, unless authorized to do so in accordance with the consent obtained;

    b. Limits the purposes for which the personal health information may be used, disclosed or published in accordance with the consent obtained;

    c. Requires that the personal health information be safeguarded;

    d. Permits CIHI to conduct on-site privacy audits pursuant to its privacy audit program;

    e. Requires the destruction of data, as specified; and

    f. Requires the recipient to comply with any other provision that CIHI deems necessary to further safeguard the data.

42. Where the disclosure is pursuant to paragraphs 40b, c or d, prior to disclosure, the recipient must sign a data protection agreement or other legally binding instrument that, at a minimum, contains the following requirements:
    a. Prohibits contacting the individuals;
    b. Prohibits linking the personal health information unless expressly authorized in writing by CIHI;
    c. Limits the purposes for which the personal health information may be used;
    d. Requires that the personal health information be safeguarded;
    e. Limits publication or disclosure to data that do not allow identification of any individual;
    f. Requires the destruction of data, as specified;
    g. Permits CIHI to conduct on-site privacy audits pursuant to its privacy audit program; and
    h. Requires the recipient to comply with any other provision that CIHI deems necessary to further safeguard the data.
43. Prior to the disclosure of personal health information for research purposes, the requester will provide CIHI with evidence of the requisite Research Ethics Board approval.
44. CIHI reserves the right to impose any other requirement(s) as needed on a case-by-case basis in order to maintain the confidentiality of personal health information.

Disclosure of de-identified data

45. CIHI data disclosures are made at the highest degree of anonymity possible while still meeting the research and/or analytical purposes. This means that, whenever possible, data are aggregated.
46. Where aggregate data are not sufficiently detailed for the research and/or analytical purposes, data that has been de-identified using various de-identification processes may be disclosed to the recipient on a case-by-case basis and where the recipient has entered into a data protection agreement or other legally binding instrument with CIHI.
47. Only those data elements necessary to meet the identified research or analytical purposes may be disclosed.

Requirements for disclosure of de-identified data

48. Prior to disclosure, the recipient must sign a data protection agreement or other legally binding instrument that, at a minimum, contains the following requirements:
    a. Prohibits re-identifying or contacting the individuals;
    b. Prohibits linking the de-identified data unless expressly authorized in writing by CIHI;
    c. Limits the purposes for which the de-identified data may be used;
    d. Requires that the de-identified data be safeguarded;
    e. Limits publication or disclosure to data that do not allow identification of any individual;
    f. Requires the destruction of data, as specified;
    g. Permits CIHI to conduct on-site privacy audits pursuant to its privacy audit program; and
    h. Requires the recipient to comply with any other provision that CIHI deems necessary to further safeguard the data.
49. Prior to the disclosure of de-identified data for research purposes, the requester will provide CIHI with evidence of Research Ethics Board approval.
50. CIHI reserves the right to impose any other requirement(s) as needed on a case-by-case basis in order to maintain the confidentiality of de-identified data.
51. Prior to disclosure, program areas will evaluate the de-identified data to assess and subsequently minimize privacy risks of re-identification and residual disclosure, and to implement the necessary mitigating measures to manage residual risks.
52. CIHI will not disclose de-identified data if it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual and that, where it is reasonably foreseeable that it could be used to identify an individual, the information will be treated as personal health information and will be governed by Section 40.

Disclosure outside of Canada

53. CIHI does not disclose personal health information to recipients located or in transit outside of Canada without the consent of the individuals concerned, or except where authorized or required by law.
54. CIHI may disclose de-identified data as defined in this Privacy Policy to recipients located outside of Canada except where prohibited by law or by agreement. Data will be de-identified using various de-identification processes.

55. Prior to disclosure, program areas will evaluate the de-identified data to assess and subsequently minimize privacy risks of re-identification and residual disclosure, and to implement the necessary mitigating measures to manage residual risks.
56. CIHI will not disclose de-identified data if it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual and that, where it is reasonably foreseeable that it could be used to identify an individual, the information will be treated as personal health information and will be governed by Section 40.

Approval requirements for disclosure outside of Canada

57. All disclosures pursuant to sections 53 and 54 must be reviewed by the Privacy, Confidentiality and Security Committee to ensure that the request meets the criteria set out in sections 40 to 50, and approved by CIHI's President and CEO on the recommendation of the Privacy, Confidentiality and Security Committee.

Recourse against third parties

58. If CIHI receives a concern or complaint that a third-party recipient of personal health information or de-identified data has made false or misleading statements in the request for data or has violated 1 or more conditions in the signed agreement, CIHI may investigate.
59. Where the concern or complaint is substantiated, CIHI will impose sanctions on the third-party recipient, which may include
    a. A written complaint to the recipient organization;
    b. Recovery of data disclosed by CIHI;
    c. A complaint to the Information and Privacy Commissioner of the relevant jurisdiction;
    d. A report to the relevant research ethics review committee, funding body, data provider and ministry of health, as applicable;
    e. Refusal of future access to data; or
    f. Legal action.

Individuals' access to and amendment of own personal health information

60. CIHI responds to an individual's request within a reasonable time and at minimal or no cost to the individual.
61. Upon request, CIHI also indicates the source of the original health information and refers the individual to the original data provider.
62. CIHI will also refer the individual to the original data provider when an individual requests amendment of his or her personal health information.
63. When a data provider notifies CIHI that the individual has successfully demonstrated the inaccuracy or incompleteness of personal health information, CIHI amends the personal health information as required.

Questions about privacy at CIHI

64. Questions, concerns or complaints about CIHI's handling of the personal health information or de-identified data it holds should be addressed to CIHI's Chief Privacy Officer at the following coordinates:

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

    Phone: 613-694-6294
    Fax: 613-241-8120
    Email: privacy@cihi.ca

65. The Chief Privacy Officer may direct an inquiry or complaint to the Privacy Commissioner of the jurisdiction of the person making the inquiry or complaint.
66. For other information on CIHI's privacy policies, procedures and practices, and its data holdings, visit www.cihi.ca.

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

20678-0919