Privacy Policy on the Collection, Use, Disclosure and Retention of Health Workforce Personal Information and De-identified Data, 2011

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

Who We Are

Established in 1994, CIHI is an independent, not-for-profit corporation that provides essential information on Canada's health system and the health of Canadians. Funded by federal, provincial and territorial governments, we are guided by a Board of Directors made up of health leaders across the country.

Our Vision

To help improve Canada's health system and the well-being of Canadians by being a leading source of unbiased, credible and comparable information that will enable health leaders to make better-informed decisions.

Privacy Policy on the Collection, Use, Disclosure and Retention of Health Workforce Personal Information and De-identified Data, 2011 ("Health Workforce Privacy Policy")

Table of Contents

Introduction

Commitment to Privacy and Security

The Canadian Institute for Health Information (CIHI) is committed to safeguarding its IT environment, 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 (the "Framework"). The Framework provides a coherent and comprehensive approach to enterprise privacy and security management for the CIHI. 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 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. As outlined in the Framework, CIHI's privacy code is based on the 10 fair information principles set out in the Canadian Standards Association's Model Privacy Code.

About This Policy

Before 2009, CIHI had a single privacy policy and procedures document that guided the management of all of the different types of health information collected by CIHI across its many data holdings (for instance, about patients, facilities, and health service providers). Over time, for reasons of clarity, precision and efficiency, CIHI recognized the need to differentiate distinct but related privacy policies that focus specifically on CIHI's management of personal health information, health facility identifiable information and health workforce information.

The following *Health Workforce Privacy Policy* now forms part of CIHI's suite of privacy and security policies. It governs CIHI's collection, retention, use and disclosure of health workforce personal information. While it is separate and distinct from the *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010* (which focuses on personal health information) and the *Policy on Health Facility Identifiable Information* (which focuses on health facility information), the following *Health Workforce Privacy Policy* is intended to be complementary to these other policies, and to embody the same core privacy principles. For clarity, whenever CIHI activities involve personal health information, CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010* will be followed.

Policy Objective

The objective of this *Health Workforce Privacy Policy* is to establish a framework within which CIHI can collect, retain, use and disclose health workforce information in a manner that ensures that health workforce personal information and resulting de-identified data 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 Policy is in effect as of February 2011.

Definitions

Aggregate data

Data that have 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 five may constitute either de-identified data or health workforce personal information.

Collect

Collect, in relation to health workforce personal 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 two or more records of health workforce personal information or de-identified data to form a composite record for a specific individual.

Data provider

Means an organization, health care provider or other individual that discloses health information to CIHI, which includes, but are not be limited to, ministries of health, regional health authorities and similar bodies, local health integration networks, hospitals, clinics within hospitals, other health care facilities, regulatory bodies, professional societies/associations and physicians.

De-identified data

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.

De-identification processes

Such processes include but are not limited to:

- Removal of name and address, if present; and
- Removal or encryption of health service provider identifying numbers (for example registration or license numbers) assigned by a data provider or other organization;

and may also involve:

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

and then:

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

In addition to the above measures, further methodologies, standards, and best practices may be developed and implemented from time to time in order to de-identify health workforce personal information.

Disclose

To release or make available health workforce personal 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

The use of data for purposes of health human resource management, health surveillance, health system planning and performance management, research and evaluation.

Health workforce

Health workforce refers to health service providers collectively who have trained/educated and/or are employed in health occupations.

Health workforce personal information

Information about a health service provider 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.

Health workforce personal information does not include personal health information as defined in the *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010* , or health facility information as defined in the *Policy on Health Facility Identifiable Information*.

Residual disclosure

The combination of publicly released 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 health workforce personal 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.

Privacy Policy for Health Workforce Personal Information

Minimal Collection and Purpose

1. CIHI only collects health workforce personal information, de-identified data and aggregate data from data providers where those data are reasonably required for health system uses, including statistical analysis and reporting.

2. CIHI only collects health workforce personal information, de-identified data and aggregate 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, and to support negotiations between employers and health professionals by providing comparable pan-Canadian data, where feasible.

Use, Disclosure and Retention

3. CIHI does not use health workforce personal information if other information will serve the purpose, and does not use more health workforce personal information than is reasonably necessary to meet the purpose. CIHI de-identifies health workforce personal 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, the names and addresses of individuals comprising the health workforce are not collected and therefore are not held in CIHI data holdings. The only exception is the Scotts Medical Database.

5. More specifically, CIHI does not use or disclose health workforce personal 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 health workforce personal 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 health workforce personal 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 health workforce personal 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 name and health service provider identifying numbers, 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 health workforce personal 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 *Health Workforce 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 the *CIHI Privacy and Security Training Policy*.

13. Consistent with its mandate and core functions, CIHI does not use health workforce personal information for any administrative purpose related to the individual (e.g. license or registration) or for market research.

Use for Data Linkage—General

14. When carrying out data linkage, CIHI may use names or provider identifying numbers.

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 health workforce personal 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 *Health Workforce 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 & Security Team 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 & Security Team 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.

Approval Requirements for Data Linkage

22. Criteria for approval pursuant to sections 19 to 21 are as follows:

23. The individuals whose health workforce personal 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 health workforce personal 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; and
    (e) 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 & Security Team 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 health service provider.

Destruction of Data, Including Linked Data

28. CIHI destroys health workforce personal 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, secure destruction will occur within one year after publication of the resulting report or analysis, or three years after linkage, whichever is sooner, in a manner consistent with CIHI's Data Destruction Standard, as 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 & Security Team.

31. In all cases, destruction of health workforce personal 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 five. CIHI may make publicly available aggregate data with units of observation of less than five, where:
    (a) The information is already publicly available; and
    (b) Making the information available will not reveal any additional personal information not already publicly available.

Return of Own Data to Original Data Provider

34. CIHI may return health workforce personal information or de-identified data to a data provider that originally provided the information to CIHI, or the relevant ministry of health where appropriate, for data quality purposes and for purposes consistent with their mandate, for example, for health services management, including planning, evaluation and health human resource allocation, and to support negotiations between employers and health professionals by providing comparable pan-Canadian data, where feasible.

35. Health workforce personal 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 system and the health of Canadians in a manner consistent with its mandate and core functions. These disclosures typically fall into one of four 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 *Health Workforce Privacy Policy*.

Disclosure of Health Workforce Personal Information

40. CIHI does not disclose health workforce personal 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 personal information is already publicly available, and making the information available will not reveal any additional personal information not already publicly available;
    (b) The recipient has obtained the consent of the individuals concerned;
    (c) The disclosure is authorized by law; or
    (d) The disclosure is required by law.

Requirements for Disclosure of Health Workforce Personal Information

41. For greater certainty, where the recipient has obtained the consent of the individuals concerned pursuant to paragraph 40 (b), 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 health workforce personal information, unless authorized to do so in accordance with the consent obtained;
    (b) Limits the purposes for which the health workforce personal information may be used, disclosed or published in accordance with the consent obtained;
    (c) Requires that the health workforce personal 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 paragraph 40 (c), 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 health workforce personal information unless expressly authorized in writing by CIHI;

(c) Limits the purposes for which the health workforce personal information may be used;

(d) Requires that the health workforce personal 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 health workforce personal 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 health workforce personal 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 have 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 health workforce personal information and will be governed by section 40.

Disclosure Outside of Canada

53. CIHI does not disclose health workforce personal 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 *Health Workforce 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 health workforce personal 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 & Security Team 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 & Security Team.

Recourse Against Third Parties

58. If CIHI receives a concern or complaint that a third-party recipient of health workforce personal information or de-identified data has made false or misleading statements in the request for data or has violated one 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) Notify the applicable ethics review body(s) and, if applicable, file a complaint to a governmental authority, as applicable;
    (e) Refusal of future access to data; or
    (f) Legal action.

Individuals' Access to and Amendment of Own Health Workforce Personal 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 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 health workforce personal information.

63. When a data provider notifies CIHI that the individual has successfully demonstrated the inaccuracy or incompleteness of health workforce personal information, CIHI amends the information as required.

Questions About Privacy or Privacy Complaints

64. Questions, concerns or complaints about CIHI's handling of the health workforce personal 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 CPO may direct an inquiry or complaint to the Privacy Commissioner of the appropriate jurisdiction.

66. For other information on CIHI's data holdings, privacy policies, procedures and practices visit www.cihi.ca.

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

Phone: 613-241-7860
Fax: 613-241-8120
www.cihi.ca
copyright@cihi.ca

Talk to Us

CIHI Ottawa
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860

CIHI Toronto
4110 Yonge Street, Suite 300
Toronto, Ontario M2P 2B7
Phone: 416-481-2002

CIHI Victoria
880 Douglas Street, Suite 600
Victoria, British Columbia V8W 2B7
Phone: 250-220-4100

CIHI Montréal
1010 Sherbrooke Street West, Suite 300
Montréal, Quebec H3A 2R7
Phone: 514-842-2226

CIHI St. John's
140 Water Street, Suite 701
St. John's, Newfoundland and Labrador A1C 6H6
Phone: 709-576-7006

June 2011

www.cihi.ca

Canadian Institute for Health Information

Institut canadien d'information sur la santé