April 2002

Privacy and Confidentiality of Health Information at CIHI

Principles and Policies for the Protection of Personal Health Information and Policies for Institution-Identifiable Information

3rd edition

Canadian Institute for Health Information

Institut canadien d'information sur la santé

Privacy and Confidentiality of Health Information at CIHI

Principles and Policies for the Protection of
Personal Health Information
and
Policies for Institution-Identifiable Information

April 2002
3rd edition

For further information, please contact the Canadian Institute for Health Information at:

377 Dalhousie Street
Suite 200
Ottawa, Ontario
K1N 9N8

Telephone: (613) 241-7860
Fax: (613) 241-8120
www.cihi.ca

Cette publication est aussi disponible en français. «*Le respect de la vie privée et confidentialité de l'information sur la santé à l'ICIS : Principes et politiques pour la protection des renseignements personnels sur la santé et Politiques pour l'information sur l'établissement*»

ISBN 1-55392-038-4

© 2002 Canadian Institute for Health Information

Privacy and Confidentiality of Health Information at CIHI
April 2002
3rd edition

Table of Contents

Executive Summary

The Canadian Institute for Health Information (CIHI) is an independent, national, not-for-profit organization with a mandate agreed to by the Federal/Provincial/Territorial Ministers of Health. CIHI's mandate is:

- To coordinate the development and maintenance of an integrated approach to Canada's health information system; and
- To provide and coordinate the provision of accurate and timely information required for:
  - Establishing sound health policy;
  - Effectively managing the Canadian health system; and
  - Generating public awareness about factors affecting good health.

Respecting personal privacy, safeguarding confidential information and ensuring security are critical to this mandate. To this end, CIHI has in place an active privacy program to:

- Keep CIHI's privacy principles, policies, procedures and practices current and in harmony with existing legislation and public opinion;
- Monitor developments in privacy legislation, privacy enhancing technologies and public opinion;
- Enhance CIHI's data protection tools and activities;
- Foster transparency and increase awareness of CIHI's privacy principles, policies and procedures;
- Support staff in applying CIHI's privacy principles, policies and procedures; and
- Support controlled access to and responsible use of health information under CIHI's management.

A key component of CIHI's privacy program is its statement of privacy principles and policies. The principles and policies guide CIHI's operations and inform others of CIHI's practices. CIHI has self-regulated on the basis of its stated principles since its inception and, in concert with current privacy legislation, it continues to do so. The principles and policies are reviewed regularly.

The latest review was completed after consultation with ministries of health and privacy officials across the country. CIHI has chosen to align its principles and policies with Schedule 1 of the federal *Personal Information Protection and Electronic Documents Act,* with modifications related to the context within which CIHI functions. Although the federal Act applies to commercial uses of personal information by the private sector, Schedule 1 of the Act sets a national standard for addressing personal information protection. It is for this reason that CIHI has chosen to align its Principles with Schedule 1 of the Act.

As indicated, the principles have been modified to reflect the context within which CIHI operates. For example:

- CIHI works in partnership with ministries of health and others to identify health information needs, purposes and transfer arrangements;
- CIHI receives personal health information from organizations that have the authority to disclose the information to CIHI for the purposes of carrying out its mandate. CIHI relies on these organizations to comply with the requirements and laws in place in their jurisdictions for the collection, use and disclosure of personal health information;
- CIHI receives summaries of coded personal health information that represent a fraction of the information in the original records of individuals concerned;
- Most of CIHI's records include a unique identifier to facilitate statistical analysis and research. This number is usually a personal health number. However, CIHI cannot identify individuals with the number because CIHI does not have access to the registration databases of health plans. Therefore the data CIHI receives are not readily identifiable. Nonetheless, CIHI protects the data to the same degree as readily identifiable personal health information;
- CIHI uses health information for analysis and reporting to improve the health of Canadians and the health care system. Given its mandate, CIHI does not use personal health information to make administrative decisions about the individuals concerned, such as their entitlement to services or benefits; and
- CIHI supports access to de-identified personal health information in a responsible, secure manner for purposes of analysis and research, consistent with CIHI's mandate.

Scope

The principles and policies in this document apply to CIHI's data holdings of:

- Personal health information, which includes:
  - information about recipients of health services;
  - registration and practice information about health professionals; and
- Institution-identifiable Information.

Separate policies are under development for personal information about clients and employees of CIHI used in the administration of CIHI's activities.

I Introduction

Mandate

The Canadian Institute for Health Information (CIHI) is an independent, national, not-for-profit organization with a mandate agreed to by the Federal/Provincial/Territorial Ministers of Health. CIHI's mandate is:

- To coordinate the development and maintenance of an integrated approach to Canada's health information system; and
- To provide and coordinate the provision of accurate and timely information required for:
  - Establishing sound health policy;
  - Effectively managing the Canadian health system; and
  - Generating public awareness about factors affecting good health.

A Board of Directors, representing governments across Canada and the health delivery system, governs CIHI. The Board consists of:

- One government and one non-government representative from each of five regions across Canada;
- Two members-at-large;
- A representative from each of Health Canada and Statistics Canada; and
- The Chair.

More information on the Board is available on the CIHI Web site at www.cihi.ca.

Under its mandate, CIHI's core functions are to:

- Identify health information needs and priorities;
- Collect, process and maintain data for specified data holdings;
- Set national standards for collecting and reporting financial, statistical and clinical data, as well as standards for health informatics/telematics; and
- Produce and disseminate value-added analysis.

CIHI's data holdings include:

- Canadian Joint Replacement Registry (CJRR)
- Canadian MIS Database (CMDB)
- Canadian Organ Replacement Register (CORR)
- Continuing Care Reporting System (CCRS)
- Discharge Abstract Database (DAD)
- Health Personnel Database (HPDB)
- Hospital Mental Health Database (HMHDB)
- Hospital Morbidity Database (HMDB)
- National Ambulatory Care Reporting System (NACRS)
- National Health Expenditures Database (NHEX)
- National Physician Database (NPDB)
- National Rehabilitation Reporting System (NRS)

- National Trauma Registry (NTR)
- OECD Health Database (Canadian segment)
- Ontario Chronic Care Patient System (OCCPS)
- Ontario Trauma Registry (OTR)
- Registered Nurses Database (RNDB)
- Southam Medical Database (SMDB)
- Therapeutic Abortion Database (TADB)

Appendix C provides an overview Information Flow Diagram. More information on the purposes, data elements, data sources and reports for each data holding is available on the CIHI Web site at www.cihi.ca.

These health information data holdings are the foundation for analysis and reports that help health planners, policy makers and providers make the health system more efficient and effective. CIHI's reports also help individual Canadians to make more informed health decisions and to live healthier lives. For example, CIHI's data holdings are used to:

- Analyse and compare lengths of hospital stays for patients with a specific health condition or having a specific procedure;
- Monitor survival rates for kidney transplants;
- Track the supply and distribution of nurses and doctors;
- Understand the costs of health care; and
- Make comparisons among health regions to identify best practices.

Reliable, accurate and timely data are critical to providing dependable information to support these activities, to assess the current situation and to evaluate options. To assist health policy makers, health system managers, researchers and the public, CIHI's core functions include gathering coded extracts of personal health information from a variety of sources, such as hospitals, governments and professional registration bodies.

CIHI works in partnership with ministries of health to identify health information needs and to ensure that CIHI's personal health information protection practices comply with relevant legislation. CIHI also works with researchers to facilitate secure, responsible access to data in support of bona fide research. When researchers request CIHI data, CIHI undertakes a detailed review of the requests in relation to its privacy and confidentiality policies and also requires recipients to sign agreements covering their obligations to keep the data confidential and secure.

CIHI's Privacy Program

Respecting personal privacy, safeguarding confidential information and ensuring security are critical for carrying out CIHI's mandate successfully.

The privacy program includes:

- A Privacy Secretariat, headed by the Chief Privacy Officer who reports directly to the President and Chief Executive Officer;

- An active Privacy, Confidentiality and Security Team that includes the Vice President of Operations, directors and managers who represent all areas of the organization (information systems, databases, registries, standards, research and analysis, management, client relations and human resources); and
- A Chief Privacy Advisor, who is a former provincial information and privacy commissioner.

Key activities of the Privacy Program include:

- Policy analysis and application:
  - monitoring privacy and data protection legislation;
  - ongoing review of CIHI's privacy and confidentiality principles and policies;
  - identifying the privacy elements for CIHI's Bilateral Agreements with provinces/territories;
  - conducting privacy impact assessments of CIHI's data holdings;
  - reviewing and resolving privacy and confidentiality issues; and
  - second-level review of requests for data.
- Fostering a culture of privacy at CIHI by:
  - supporting development activities to ensure that privacy and data protection issues are addressed;
  - working with Information Systems and other areas of the organization to enhance CIHI's data protection practices and tools;
  - conducting staff training and communicating with staff on privacy and confidentiality policies and procedures;
  - ensuring staff sign a confidentiality pledge that indicates that breaches may lead to discipline, including termination and legal action; and
  - managing the CIHI Privacy, Confidentiality and Security Team.
- Communications/Outreach:
  - developing user-friendly and accessible information about CIHI's privacy program;
  - addressing organizations to explain privacy and data protection at CIHI;
  - liaising with the privacy officials in ministries of health and Privacy Commissioners' offices;
  - liaising with the privacy office of Statistics Canada to leverage its work and experience in privacy and data protection;
  - acting as the contact point for individuals wishing to access their own personal health information and for privacy related complaints;
  - participating on working groups such as the federal/provincial/territorial Protection of Personal Health Information Working Group of the Advisory Committee on Health Infostructure at Health Canada; and
  - supporting researchers through work internal to CIHI as well as through the Canadian Institutes of Health Research Group on Privacy.

Background

Shortly after its establishment, CIHI implemented guidelines for the protection of health information on April 1, 1996. The guidelines were based on:

- CIHI's national mandate in health information;
- Privacy legislation in place at the time;
- The Canadian Standards Association's *Model Code for the Protection of Personal Information,* which remains the basis for CIHI's self-regulatory efforts;
- Input from ministry of health and privacy officials across Canada; and
- The related policies of the predecessor organizations (Hospital Medical Records Institute, The MIS Group and parts of both Statistics Canada and Health Canada).

Based on the experience gained with the first edition of the guidelines and also the standards in emerging privacy-related legislation across Canada, CIHI reviewed and refined its guidelines. In April 1999, CIHI implemented revised guidelines (*Privacy and Confidentiality of Health Information at CIHI: Principles and policies for the protection of health information, 2nd edition.*)

2002 Edition

Consistent with CIHI's ongoing commitment to the protection of privacy, CIHI initiated a further review in the year 2000. This broad review included:

- Examination of existing and proposed legislation for the protection of personal health information; and
- Consultation with the federal/provincial/territorial ministries of health and Information and Privacy Commissioners/Ombudsmen.

This document, which has been approved by the CIHI Board of Directors, reflects the outcome of the above activities. The document has been revised to follow closely the 10 standards contained in Schedule 1 of the federal *Personal Information Protection and Electronic Documents Act*, with modifications to reflect CIHI's mandate and core functions. CIHI is also closely monitoring developments related to Ontario's privacy legislation. It is expected that this legislation will have a direct impact on CIHI's operations.

In order to ensure the continuing appropriateness of CIHI's privacy principles and policies, this document will continue to be reviewed and updated on a regular basis.

Scope and Structure

The principles and policies in this document apply to CIHI's data holdings of:

- Personal health information, which includes:
  - information about recipients of health services; and
  - registration and practice information about health professionals;
- Institution-identifiable information.

The document is organized as follows:

- Section I describes CIHI's Mandate, Privacy Program and Background;
- Section II explains the Legislative Framework within which CIHI functions;
- Section III sets out CIHI's privacy principles for personal health information with corresponding policies and procedures; and
- Section IV provides CIHI's policies for institution-identifiable information.

Separate policies are under development for personal information about clients and employees of CIHI used in the administration of CIHI's activities.

Acknowledgements

This 3rd edition of *Privacy and Confidentiality of Health Information at CIHI* was developed by CIHI's Privacy Secretariat. The revision process benefited from the valuable comments and suggestions of many individuals and organizations, who reviewed drafts of the document.

In particular, CIHI acknowledges the contributions made by:

- Federal/Provincial/Territorial ministries of health;
- Federal/Provincial/Territorial Information and Privacy Commissioners and Ombudsmen, and their staff;
- Federal/Provincial/Territorial Protection of Personal Health Information Working Group; and
- Representatives of hospitals and the health research community.

In addition, key input was provided internally by CIHI's:

- Chief Privacy Advisor;
- Privacy, Confidentiality and Security Team;
- Operations Management Committee; and
- Managers and staff in the program areas.

II Legislative Framework

A complex framework of privacy, health program and data protection laws at the federal/provincial/territorial levels governs the broad range of activity that takes place in the health sector. Within this framework, ministries of health, health service providers, patients and data users provide care, obtain treatment, process payments and conduct studies to analyze and evaluate health services and systems.

It is also within this framework that CIHI has established agreements with many organizations to carry out agreed upon functions in relation to health information in Canada. Such health data are disclosed to CIHI under a variety of authorities. Work is underway to strengthen references in the agreements to the authorities that govern the collection, use and disclosure of personal health information.

Policies

- CIHI works with provincial and territorial ministries of health to establish agreements that set out the terms for the transfer of health data to CIHI.
- CIHI abides by the agreements that have been established with provincial and territorial ministries of health.
- The organizations that provide personal health information to CIHI have the primary obligation of establishing the authorities for transfer of personal health information to CIHI and for otherwise complying with their governing legislation.
- CIHI prepares privacy impact assessments for its data holdings, both existing and proposed.

Related Documents

- Bilateral Agreements

III Principles and Policies for the Protection of Personal Health Information

Principle 1: Accountability for Personal Health Information

CIHI is responsible for personal health information under its control and has designated an individual who is accountable for CIHI's compliance with the following principles.

Policies	Related Procedures
Policy 1.1 Accountability for CIHI's compliance with the principles rests with CIHI's President and Chief Executive Officer, even though other individuals within CIHI are responsible for the day-to-day collection and processing of personal health information. In addition, other individuals within CIHI are delegated to act on behalf of the President and Chief Executive Officer. As the President and Chief Executive Officer is accountable for CIHI's compliance, he or she has decision-making authority regarding the interpretation and application of the principles and policies, subject to the Complaints section.	**Procedure 1.1** a) The Chief Privacy Officer, or designate, drafts a privacy delegation chart that: • Lists the specific accountabilities of the President and Chief Executive Officer for compliance with *Privacy and Confidentiality of Health Information at CIHI*; and • Indicates the CIHI staff with delegated authority to act on behalf of the President and Chief Executive Officer for each accountability. b) Following consultation with Senior Management, the Privacy, Confidentiality and Security Team and others as appropriate, the Chief Privacy Officer, or designate, revises the draft privacy delegation chart and recommends its approval to the President and Chief Executive Officer. c) The President and Chief Executive Officer: • Reviews the recommended delegation chart; • Modifies the delegation chart as she or he deems appropriate; and • Approves the privacy delegation chart for release by the Vice-President, Operations to all staff. d) The Chief Privacy Officer: • Reviews the delegation chart as required and at least every five years; and • Follows steps a) to c) above to prepare and issue a revised delegation chart.

Policies	Related Procedures
Policy 1.2 Reporting to the President and Chief Executive Officer, CIHI's Privacy Secretariat is responsible for providing leadership on privacy matters throughout the organization.	**Procedure 1.2** No related procedure.
Policy 1.3 CIHI is responsible for personal health information in its possession or custody, including personal health information that has been transferred to a third party for processing. CIHI uses contractual or other means to provide a comparable level of protection while the personal health information is being processed by a third party.	**Procedure 1.3** a) In cases where temporary staff may have access to personal health information, the appropriate manager ensures that temporary staff sign a confidentiality pledge. b) The Manager, Human Resources and Administration, or designate, ensures that standard contract wording includes provisions that specify the contractor's obligations to protect personal health information. c) When preparing contracts that involve contractor access to personal health information for processing or other purposes, the appropriate manager, or designate: • May consult with the Privacy Secretariat regarding the specific terms and conditions in the contract related to the contractor's protection of personal health information; • As required, adds additional provisions to the standard contract wording to specify the contractor's obligations to protect the personal health information to a level comparable with *Privacy and Confidentiality of Health Information at CIHI*, which may include non-disclosure agreements and/or confidentiality pledges; and • Ensures that the contract is executed prior to the third party gaining access to personal health information. d) This procedure applies to all new contracts. Existing contracts will be reviewed by December 2003 and amended as required.

Policies	Related Procedures
Policy 1.4 CIHI has procedures to give effect to the principles of: • Protecting personal health information (Principle 7: Safeguards); • Receiving and responding to complaints and inquiries (Principle 10: Complaints); • Staff training and a mechanism for communicating information about CIHI's policies and procedures to staff (Principle 7: Safeguards); and • Providing information and explaining CIHI's policies and procedures (Principle 8: Openness).	**Procedure 1.4** Protecting personal health information. • See Principle 7 and related procedures. Receiving and responding to complaints and inquiries. • See Principle 10 and related procedures. Staff training and a mechanism for communicating information about CIHI's policies and procedures to staff. • See Principle 7 and related procedures. Providing information and explaining CIHI's policies and procedures. • See Principle 8 and related procedures.

Related documents

- Privacy Delegation Chart
- CIHI Privacy Brochure
- CIHI Web site (www.cihi.ca)
  - Privacy and Data Protection
  - Program description
  - Frequently asked questions

Principle 2: Identifying Purposes for Personal Health Information

CIHI identifies the purposes for which it collects personal health information prior to the time the information is collected.

Policies	Related Procedures
Policy 2.1 Identifying the purposes for which it collects personal health information prior to the time of collection allows CIHI to determine the information it needs to fulfil these purposes. **Policy 2.2** CIHI only collects personal health information once the purposes have been identified in consultation with appropriate stakeholders. CIHI supports data providers informing individuals about the purposes at or before the time of collecting personal health information. **Policy 2.3** Data providers have a responsibility to ensure that the legal authority exists for the disclosure of personal health information to CIHI. (No related procedure.) **Policy 2.4** CIHI staff who receive personal health information from data providers for a data holding are able to explain the purposes for which the information is being collected.	**Procedure 2.1, 2.2 and 2.4** a) The program manager drafts a statement that identifies the purposes of the data holding. b) The program manager seeks input on the draft statement of purposes from the Privacy Secretariat and, as appropriate, from related advisory groups and key stakeholders. c) If required, the program manager revises the draft purposes statement based on the input received. d) The appropriate director approves the statement of purposes for the data holding and provides a copy to the Privacy Secretariat and other key stakeholders. e) Prior to the collection of personal health information, the program manager communicates with the data providers to: • Provide the statement of purposes for the data holding in order to facilitate their understanding of and support for the purposes; and • Indicate that under Policy 2.2, CIHI supports data providers informing individuals about these purposes at or before the time of collecting personal health information. f) The program manager ensures that CIHI staff who gather personal health information from data providers for a data holding are able to explain the statement of purposes to any person who makes an inquiry. g) The program manager includes a statement of purposes for the data holding in appropriate documentation, including the CIHI products and services catalogue, the CIHI Web site and other program descriptions.

Related documents

- CIHI Catalogue

Principle 3: Consent for the Collection, Use or Disclosure of Personal Health Information

CIHI acknowledges the principle that "the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate." CIHI consults with ministries of health and data providers about the implementation of this principle. As CIHI obtains personal health information from data providers (who are themselves covered by legislation) and not directly from individuals, CIHI recognizes that data providers must determine what actions are necessary to comply with any consent requirements in their jurisdictions.

Policies	Related Procedures
Policy 3.1 CIHI discusses the principle of knowledge and consent for the collection, use and disclosure of personal health information with partner organizations.	**Procedure 3.1** a) The program manager communicates with the data providers to indicate that CIHI: • Supports the principle that "the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate"; and • Recognizes that data providers must determine what actions are necessary to comply with legislation in their jurisdictions. b) The Chief Privacy Officer communicates with ministries of health to indicate that CIHI: • Supports the principle that "the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate"; and • Recognizes that data providers must determine what actions are necessary to comply with legislation in their jurisdictions
Policy 3.2 CIHI works with partner organizations to implement knowledge and consent processes for data holdings.	**Procedure 3.2** a) The program manager consults with advisory groups and partner organizations on the application of the principle of notification and consent for the collection, use and disclosure of personal health information. b) The program manager will collaborate with partner organizations, as appropriate, to support their use of notification, consent, or both. c) The Privacy Secretariat assists the program manager with the above consultations and collaborations.

Principle 4: Limiting Collection of Personal Health Information

CIHI limits the collection of personal health information to that which is necessary for its identified purposes. CIHI collects information by fair and lawful means.

Policies	Related Procedures
Policy 4.1 Both the amount and the type of personal health information collected are limited to what is necessary to fulfil the purposes identified for a data holding.	**Procedure 4.1** For each new data holding that contains personal health information: a) The program manager consults with advisory groups, the Privacy Secretariat and other appropriate stakeholders to define the personal health information necessary for the identified purposes of the new data holding. b) Following the consultation, the program manager prepares one or more data sets (e.g., minimum, comprehensive, etc.), which list the data elements, with definitions or explanations and documents the need for each identifying data element in relation to the identified purposes of the data holding. c) If required, the program manager conducts additional consultations on the draft data sets. d) Once there is broad agreement among key stakeholders on the proposed data sets, the program manager approves the data sets and provides a copy to advisory groups, the Privacy Secretariat and other key stakeholders as appropriate. e) The Privacy Secretariat maintains an inventory of the approved data sets for all data holdings that contain personal health information. f) Should a data provider submit personal health information, which goes beyond the approved data sets, the program manager asks the data provider to remove it from future data submissions. g) Should the data provider be unable or unwilling to remove personal health information which goes beyond the approved data sets from future data submissions, the program manager implements procedures to destroy it or to block access to it, as soon as possible after it is submitted to CIHI. For each existing data holding that contains personal health information: h) The program manager reviews the approved data sets at least every three years to determine if revisions to the data sets may be appropriate. i) If data set revisions appear to be needed, the program manager follows steps a) to g) above for the review process.

Policies	Related Procedures
Policy 4.2 CIHI promotes personal health information collection practices that are fair and lawful and convey to individuals the purpose for which information is being collected.	**Procedure 4.2** a) The program manager communicates with the data providers to indicate that CIHI: • Supports personal health information collection practices that accurately convey to individuals the purpose for which information is being collected; and • Recognizes that data providers must determine what actions are necessary to comply with legislation in their jurisdictions. b) The Chief Privacy Officer communicates with ministries of health to indicate that CIHI: • Supports data collection practices that accurately convey to individuals the purpose for which personal health information is being collected; and • Recognizes that data providers must determine what actions are necessary to comply with legislation in their jurisdictions.

Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information

CIHI does not use or disclose personal health information for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal health information is retained only as long as necessary for the fulfillment of those purposes.

Policies—Use	Related Procedures
Policy 5.1 CIHI uses personal health information for analyses and reporting, consistent with the identified purposes of the data holdings and CIHI's mandate and core functions.	**Procedure 5.1** The program manager: a) Reviews the uses of personal health information in the data holding and, if required, consults with appropriate advisory groups and key stakeholders. b) When the proposed use is consistent with the identified purpose of the data holding, the program manager may authorize that use of the personal health information. c) The program manager monitors all uses of personal health information in the data holding to ensure they have been authorized. d) When a new use is requested, the program manager reviews that use under steps a) to c) above.
Policy 5.2 If CIHI uses personal health information for a new purpose, it documents this purpose.	**Procedure 5.2** The program manager: a) Reviews each proposed new purpose for personal health information and consults with advisory groups, key stakeholders and the Privacy Secretariat, as appropriate, to determine if the proposed new purpose falls within the approved purposes statement for the data holding. b) If the new use is not covered by the approved purposes statement, the program manager may add the new purpose to the purposes statement if the procedural steps for "Principle 2: Identifying Purposes" are followed to amend the purposes statement for the data holding.

Policies—Use	Related Procedures
Policy 5.3 CIHI may conduct analyses of personal health information for external parties within CIHI's secure environment, consistent with the identified purposes of the data holdings and subject to disclosure policies in *Privacy and Confidentiality of Health Information at CIHI*. (See Policies 5.10 to 5.13.)	**See Procedures 5.10 to 5.13**
Policy 5.4 CIHI allows only authorized staff to access and use specific data holdings of personal health information on a "need-to-know" basis, that is, when required to perform their duties.	**Procedure 5.4** Employee access is controlled through the designated program manager for each data holding. Access is monitored and action taken on unauthorized attempts by employees to access data holdings. "Employee" includes students and contractors. 1. The employee's manager and the employee discuss: • The need to access a specific data holding(s); • Why access is required for the employee's job responsibilities; and • Whether the requirement is on-going or short-term. 2. The employee's manager completes the Data Access Authorization request form. As signatures are required for authorization, this document must be printed and completed manually. **Note:** Due to the nature of the work in the Data Quality area, the manager will document authorization requests by special memo, rather than the Data Access Authorization Request Form. 3. When an employee requires access to a data holding that is the responsibility of another manager, the employee's manager sends the Data Access Authorization request form to the data holding owner with a justification, which specifies: • Why access is required for the employee's job responsibilities;

Policies—Use	Related Procedures
Policy 5.4 (cont'd)	**Procedure 5.4 (cont'd)** • Whether the requirement is on-going or short-term; • The type of access required (read, create, update, delete); and • Related restrictions (e.g., no access to specified data elements.) 4. The data holding owner decides if access is to be granted, after considering: • Whether access is needed for the employee's job responsibilities (convenience alone is not sufficient justification); and • Whether short-term access could be avoided by providing the employee with a data subset. If access is denied, the data holding owner notifies the employee with an explanation of the reasons. 5. If access is approved, the data holding owner is to send the completed, approved form and supporting justification to the IS Help Desk and copy the employee, the employee's manager and, if applicable, the Privacy Secretariat. 6. Information Systems (IS) implements and monitors data holding access by: • Notifying the data holding owner, the employee and the employee's manager (if applicable), when access has been implemented; • Maintaining a record of the employees who have access to particular data holdings, including start dates and end dates for short-term access; • Asking each data holding owner, regularly and at least annually, to review the list of employees with access to their data holding(s); and • Removing access when: – the short-term end date is reached; – the employee's manager advises that an employee with data holding access is no longer employed with CIHI or access is no longer required.

Policies—Use	Related Procedures
	7. The employee's manager notifies IS when an individual with data holding access is no longer employed with CIHI or access is no longer required. When an employee leaves the organization or is transferred to another position, Human Resources will also notify IS as a safeguard measure.
Policy 5.5 Given its mandate and role, CIHI does not use personal health information to make decisions about an individual's entitlements to health services and benefits.	**Procedure 5.5** No related procedure.
Policy 5.6 CIHI may consult with relevant privacy commissioners and/or other government officials/bodies responsible for privacy protection (such as ethics review committees) prior to undertaking linkages of personal health information that are exceptional or precedent-setting in terms of their scope, scale, methods of linkage, procedures for obtaining consent, or other factors.	**Procedure 5.6** No related procedure.
Policy 5.7 CIHI only undertakes data linkage (the bringing together of two or records of personal health information to form a composite record) when: a) The individuals concerned have consented to the data linkage; or b) All of the following criteria are met: • the purpose of the data linkage is consistent with CIHI's mandate; • the public benefits (see definition below) of the linkage significantly offset the public interest in protecting the privacy of individuals; • 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;	**Procedure 5.7** 1. When a proposed data linkage involves personal health information, the program manager submits a data linkage request to the Chief Privacy Officer, which describes the proposed linkage, its purpose, and its adherence to the criteria for data linkage in policy 5.6. 2. The Chief Privacy Officer submits the data linkage request to the Privacy, Confidentiality and Security Team, which applies the criteria in policy 5.7 to decide if the linkage may proceed. 3. All new proposals for data linkage of personal health information must follow this procedure; existing ongoing data linkages must be reviewed under this procedure by March 2003.

Policies—Use	Related Procedures
Policy 5.7 (cont'd) • the data linkage is for a time-limited specific project (the linked information may be stored to allow for verification and audit of the analysis for a maximum of five years); and • the data linkage has demonstrable savings over other alternatives or is the only practical alternative. The disclosure of linked information is subject to disclosure policies in *Privacy and Confidentiality of Health Information at CIHI*. "Public benefits" means the results of the linkage are expected to contribute to: • The identification, prevention or treatment of illness, disease or injury; • Scientific understanding relating to health; • The promotion and protection of the health of individuals and communities; or • Improvements in health system policy and management. "Detrimental" means the purpose of a data linkage is not to make decisions about a subject 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. In certain circumstances, "detrimental" could include consideration of potential harm to a specified group.	

Policies—Retention	Related Procedures
Policy 5.8 CIHI retains personal health information in electronic format permanently for long-term analysis and reporting. CIHI retains paper records of personal health information that have been put into electronic format for as long as is required for the electronic records to be finalized. The length of time may vary depending on the data holding. **Policy 5.9** Personal health information that is no longer required to fulfil the identified purposes is destroyed, erased, or made anonymous.	**Procedure 5.8 and 5.9** Under development.

Policies—Disclosure	Related Procedures
Policy 5.10 CIHI discloses personal health information only for identified purposes, consistent with its mandate and core functions. **Policy 5.11** CIHI discloses or publishes aggregated personal health information only in a manner designed to minimize any risk of residual disclosure of personal health information about any individual. Typically, CIHI aggregates personal health information to levels that do not permit residual disclosure. This generally requires a minimum of five observations per cell. Aggregated personal health information generated from information already in the public domain (such as directories of health practitioners) may be exempt from this policy. **Policy 5.12** CIHI may disclose personal health information only when: a) The recipient is the data provider that originally provided the personal health information to CIHI or the relevant ministry of health, for purposes consistent with their mandate, for example, for health services and population health management, including planning, evaluation and resource allocation; b) The disclosure is required by legislation, an agreement authorized by legislation[1], or direction from the appropriate ministry of health; or c) The recipient has: • Obtained the consent of the individuals concerned and the disclosure is permitted by legislation; and • Signed an agreement that: – prohibits linking the personal health information, unless authorized to do so;	**Procedure 5.10 to 5.13, Part A** **Public Requests for Published Data** 1. When a member of the public requests published data, the employee: • Decides if referral to another CIHI department or employee is appropriate and, if so, makes the referral; • Clarifies the request and determines if related CIHI published data are available; and • Provides the requestor with relevant published data and any related information on data limitations **Notes** a) As published data have already been reviewed for privacy and confidentiality issues and have been released into the public domain, no further reviews or approvals are required. This includes data posted on CIHI's public Internet site. b) There is no need to track such requests, unless a program area decides to do so for its business needs. **Procedure 5.10 to 5.13, Part B** **Media Requests for Published Data:** When a member of the media requests published data: 1. The employee receiving the request: • Responds to the request when they have the appropriate knowledge to do so and then notifies Communications of the details (requestor, information sought, information provided and date) by e-mail; or • In other cases, refers the request to Communications. 2. Communications staff: • Lead the response when a requestor contacts Communications directly, including referring the requestor to the appropriate program manager or employee for additional detailed information or background, when appropriate; • Lead the response when a requestor has been referred to Communications by a program area; and

[1] For example, the Statistics Act authorizes Statistics Canada to require the disclosure of information.

Policies—Disclosure	Related Procedures
– limits the purposes for which the personal health information may be used or disclosed; – requires that the personal health information be safeguarded; – limits publication or disclosure to aggregated data, which do not allow identification of any individual; and – permits CIHI to conduct on-site compliance audits. **Policy 5.13** In all other cases, CIHI may disclose personal health information only when: a) The direct identifiers (such as name, full address, personal health number or health service provider number) are removed, encrypted or truncated; b) Sensitive data elements (such as date of birth, date of admission, date of discharge, postal code and clinical procedure) are removed, encrypted or truncated, if when taken together, or in combination with other data elements, they reasonably lead to identification of the individual; and c) The recipient has signed an agreement that: • prohibits re-identifying or contacting the individuals; • prohibits linking the personal health information; • limits the purposes for which the personal health information may be used or disclosed; • requires that the personal health information be safeguarded; • limits publication or disclosure to aggregated data, which do not allow identification of any individual; and • permits CIHI to conduct on-site compliance audits.	• Track all media requests for business purposes. **Note:** As published data have already been reviewed for privacy and confidentiality issues and have been released into the public domain, no further reviews or approvals are required. This includes data posted on CIHI's public Internet site. **Procedure 5.10 to 5.13, Part C** **Institution/Ministry of Health requests** When an institution requests data in any form that it had provided to CIHI or when a ministry of health requests data: 1. The institution/ministry of health must make the request in writing (letter, fax, e-mail, etc.); 2. The employee receiving the request refers it to the appropriate program manager; 3. The program manager or delegate: a) clarifies the request, if required; b) verifies that the requestor is an institution/ministry authorized contact or agent (e.g., a consultant working for an institution or ministry); c) provides the requestor with relevant data; and d) documents the request. **Notes:** • There is no need for review for privacy and confidentiality issues or further approvals if the institution requesting the data originally provided the data. • If the requestor is a ministry other than a provincial or territorial ministry of health, the procedures in parts D and E should be followed, as appropriate. **Procedure 5.10 to 5.13, Part D** **Other requests for aggregate data** When the request is for aggregate data, but does not fall under Parts A, B or C above: 1. The employee receiving the request refers it to the appropriate program manager; 2. The program manager (or delegate) communicates with the requestor to: a) clarify the request; b) explain applicable fees;

Policies—Disclosure	Related Procedures
	Procedure 5.10 to 5.13, Part D (cont'd) c) discuss whether CIHI aggregate data will meet the need; and d) explain CIHI's privacy and confidentiality policies regarding: • review of aggregate data to avoid residual disclosure of personal health information; • the need for the requestor to obtain authorizations for institution-identifiable information (Guidelines are available on the requirements for authorizations that are acceptable for CIHI's purposes); and • the need for the requestor to complete a Client Information Request Form for Aggregate Data and a Non-Disclosure/Confidentiality Agreement for Aggregate Data, available on the CIHI Web site. 3. Upon receipt of a completed Client Information Request Form for Aggregate Data, the program manager (or delegate): a) documents the request; b) Reviews the form for completeness and follows up with the requestor if required; and c) Decides if review by the Privacy, Confidentiality and Security (PC&S) Team is required (i.e., when institution-identifying information is requested and no authorizations are obtained, or when the request is unusual, sensitive or precedent setting) and, if so, refers the request to the Privacy Secretariat, with: • the name of the program area contact for the data request; • the completed Client Information Request Form and attachments; • documentation of agreements, correspondence, authorizations or restrictions that relate to the data requested; • a brief assessment from the program area of how the request relates to any agreements, authorizations or restrictions;

Policies—Disclosure	Related Procedures
	Procedure 5.10 to 5.13, Part D (cont'd) • an indication of why the request is going to the PC&S Team (i.e., for information, for advice or for review and recommendation); and • an indication that the program manager has been informed of the request. **See Part E points 4 and 5, Next Steps, if applicable.** 4. If data are approved for release, the program manager (or delegate): a) Generates the requested data from the data holding; b) Modifies the data, if required, to prevent residual disclosure of personal health information or institution-identifiable information (unless consents/authorizations obtained), usually by stripping, encrypting or truncating identifiers and suppressing cells with fewer than 5 observations; c) Checks that a signed Non-Disclosure/Confidentiality Agreement for Aggregate Data has been executed by: • signing it on behalf of CIHI; • ensuring the recipient has signed; • providing the recipient with a signed Agreement; and • keeping a signed Agreement on file; d) Checks that signed authorizations have been provided for institution-identifiable information, if applicable; e) Checks that any required fees have been paid or an invoice generated, where applicable; f) Releases the data to the requestor, with a copy of the executed Non-Disclosure/ Confidentiality Agreement for Aggregate Data; g) Updates the request documentation; h) Notifies the Privacy Secretariat if an on-site audit for compliance with the terms of the Non-Disclosure/ Confidentiality Agreement for Aggregate Data should be considered; and i) Notes the date for data return or destruction in a "Bring Forward" system for follow up, where applicable.

Policies—Disclosure	Related Procedures
	Procedure 5.10 to 5.13, Part E **Other requests for record-level data** When the request is for record-level data, but does not fall under Part C above: 1. The employee receiving the request refers it to the appropriate program manager; 2. The program manager (or delegate) communicates with the requestor to: a) clarify the request; b) explain applicable fees; c) discuss whether aggregate data or de-identified record-level data will meet the need. (Note: It is CIHI practice to scramble or strip personal health numbers, truncate postal codes to the first 3 digits, or use some other geographic grouping that is larger than a postal code and truncate date of birth to month and year or convert to age); d) explain CIHI's privacy and confidentiality policies to: • Review record-level data to avoid residual disclosure of personal health information or institution-identifiable information, by stripping, encrypting or truncating identifiers and/or aggregating the data; • Direct the requestor to obtain consents for personal health information from subject individuals and/or authorizations for institution-identifying information (Guidelines are available on the requirements for valid consents/ authorizations); and • Direct the requestor to complete a Client Information Request Form for Record-Level Data and a Non-Disclosure/Confidentiality Agreement for Record-Level Data; e) outline CIHI's review and approval process which involves: • The program manager; • the Privacy, Confidentiality and Security (PC&S) Team; • possible consultation with others (e.g., Ministry of Health, Privacy Commissioners, etc.);

Policies—Disclosure	Related Procedures
	Procedure 5.10 to 5.13, Part E (cont'd) • President and CEO for unusual, sensitive or precedent-setting requests or requests for personal health information; and • the likely date for Privacy, Confidentiality and Security Team review, if known. 3. Upon receipt of a completed Client Information Request Form for Record Level Data, the program manager (or delegate): a) Documents the request; b) Reviews the form for completeness and follows up with the requestor if required; and c) Refers the request to the Privacy Secretariat with: • the name of the program area contact for the data request; • the completed Client Information Request Form and attachments; • documentation of agreements, correspondence, authorizations or restrictions that relate to the data requested; • a brief assessment from the program area of how the request relates to any agreements, authorizations or restrictions; • an indication of why the request is going to the PC&S Team (i.e., for information, for advice, or for review and recommendation); and • an indication that the program manager has been informed of the request. 4. The Privacy, Confidentiality and Security (PC&S) Team: a) Reviews the request in relation to the principles and policies in *Privacy and Confidentiality of Health Information at CIHI*; b) Decides if input is needed from others (e.g., Ministry of Health, Privacy Commissioners, etc.) and requests same, if applicable; and c) Decides if the request: • is approved (possibly with special requirements or restrictions); or

Policies—Disclosure	Related Procedures
	Procedure 5.10 to 5.13, Part E (cont'd) • requires the approval of the President and CEO because it is unusual, sensitive, precedent-setting, or it involves personal health information. **Note:** The PC&S Team meets approximately every six to eight weeks. 5. The Privacy Secretariat staff: a) Send the request to the President and CEO, if applicable; b) Notify the program manager (or delegate) of the PC&S Team decision; and c) Maintain a record of PC&S Team decisions. 6. For approved requests, the program manager (or delegate): a) Checks that a signed Non-Disclosure/Confidentiality Agreement for Record-Level Data has been received and signs it on behalf of CIHI; b) Asks the requestor to provide a written statement in a form determined by the Privacy Secretariat confirming that consents have been obtained from subject individuals, if personal health information has been requested; c) Checks that a signed Non-Disclosure/Confidentiality Agreement for Aggregate Data has been executed by: • signing it on behalf of CIHI; • ensuring the recipient has signed; • providing the recipient with a signed Agreement; and • keeping a signed Agreement on file; d) Generates the requested data from the data holding; e) Modifies the data, if consents and/or authorizations have not been obtained, to prevent residual disclosure of personal health information or institution-identifiable information, usually by stripping, encrypting, or truncating identifiers; f) Checks that any required fees have been paid or an invoice generated, where applicable;

Policies—Disclosure	Related Procedures
	g) Releases the data to the requestor, with a copy of the executed Non-Disclosure/ Confidentiality Agreement for Record-Level Data; **Procedure 5.10 to 5.13, Part E (cont'd)** h) Updates the request documentation; i) Notifies the Privacy Secretariat if an on-site audit for compliance with the terms of the Non-Disclosure/ Confidentiality Agreement for Record-Level Data should be considered; and j) Notes the date for data return or destruction in a "Bring Forward" system for follow up, where applicable.
Policy 5.14 If CIHI receives a concern or complaint by any person, that a recipient of personal health information has made false or misleading statements in the request for data or has violated one or more conditions in the signed agreement, CIHI will investigate. When the concern or complaint is substantiated, CIHI will impose sanctions, which may include: a) A written complaint to the recipient organization; b) Recovery of data disclosed by CIHI; c) A report to the relevant research ethics review body, funding body, data provider and ministry of health, as applicable; d) Refusal of future access to data; or e) Legal action.	**Procedure 5.14** a) Any person may submit, to the Chief Privacy Officer, a concern or complaint that a recipient of personal health information has made false or misleading statements in the request for data or has violated one or more of conditions in the signed agreement covering the data disclosure. b) The Chief Privacy Officer, or designate: • Notifies the appropriate program manager and other affected parties, which may include the relevant ministries of health or privacy commissioners; • Conducts an investigation, or asks the Chief Privacy Advisor to conduct an investigation, which may involve seeking additional information from the recipient, inspecting the recipient's premises and consultation with affected parties, resulting in a report on the matter with recommendations regarding actions and/or sanctions; and • Submits the report to the President and Chief Executive Officer. c) The President and Chief Executive Officer: • Reviews the report and recommendations; • Directs the Chief Privacy Officer and appropriate program manager on the actions and sanctions to be taken; and • Provides the Board of Directors with an annual report on the complaints made and their disposition.

Data Request Scenarios

The following summarizes Procedure 5.10 to 5.13. See full text for details. This only applies to data holdings with personal health information or institution-identifiable data (i.e., not NHEX or OECD.)

	Request Type	Who Approves	Request Format	Agreement Required	Tracking Required	Comments
A	Public requests for published data or data posted to external web site	▪ Any staff	Any means	No	No	As data are already in the public domain, no further review or approval required
B	Media requests for published data or data posted to external web site	▪ Any staff with appropriate knowledge ▪ Otherwise Communications	Any means	No	by Communications	
C	Institution requests for data they provided in any form, or Health Ministry requests on a case-by-case basis	▪ Program Manager or delegate	In writing (letter, fax or e-mail)	No	Yes	
D	Other requests for aggregate data—including institution-identifiable information	Program Manager or delegate if ▪ Reviewed for residual disclosure of personal health information, and ▪ Authorizations obtained for institution-identifiable information PC&S Team in other cases CEO if ▪ Institution-identifiable information and no authorizations obtained ▪ Unusual, sensitive or precedent setting	*Client Information Request Form for Aggregate Data*	*Non-Disclosure/ Confidentiality Agreement for Aggregate Data*	Yes	

	Request Type	Who Approves	Request Format	Agreement Required	Tracking Required	Comments
E	Other requests for record-level data	Program Manager if ▪ personal health number/chart number is removed/encrypted and ▪ Postal Code is truncated to FSA and ▪ age is limited to year of birth, age or age groupings and ▪ date of admission/ discharge is limited to month/year and ▪ reviewed for residual disclosure of personal health information, and ▪ the release is not unusual, sensitive or precedent setting PC&S Team if the above conditions are not met and CEO if ▪ unusual, sensitive or precedent setting Note: External review by the Chief Privacy Advisor and privacy commissioners may also be involved at the discretion of the PS	*Client Information Request Form for Record-Level Data*	*Non-Disclosure/ Confidentiality Agreement for Record-Level Data*	Yes	Personal Health Number **MUST** be stripped or encrypted unless: ▪ consents have been obtained ▪ an act requires (or an agreement permits) disclosure ▪ data are being requested by the original provider or their ministry of health

Related Documents

- Data Access Authorization Request Form
- Client Information Request Form for Aggregate Data
- Non-Disclosure/Confidentiality Agreement for Aggregate Data.
- Client Information Request Form for Record-Level Data
- Non-Disclosure/Confidentiality Agreement for Record-Level Data.
- CIHI Consent/Authorization Requirements for Disclosures/Linkages

Principle 6: Accuracy of Personal Health Information

Personal health information is as accurate, complete and up-to-date as necessary for the purposes for which CIHI uses it.

Policies	Related Procedures
Policy 6.1 Personal health information is as accurate, complete and up-to-date as necessary for the approved purposes of the data holdings. **Policy 6.2** CIHI updates personal health information only when necessary to fulfil the purposes for which the information was collected. **Policy 6.3** CIHI uses educational programs, data quality programs, data coding standards and data edits to foster the collection and use of quality personal health information for its purposes. Data providers are responsible for ensuring the personal health information they provide to CIHI is accurate, complete and up-to-date for the purpose specified.	**Procedure 6.1, 6.2 and 6.3** a) The CIHI program manager implements practices and processes to foster the collection of quality data, which may include: • The development and communication of data coding standards; • The training of data provider staff in the use of data coding standards; • The use of data edits to identify data errors and omissions; and • The use of other measures, such as CIHI's Data Quality program, to enhance the quality of personal health information in the data holding. b) The program manager ensures that personal health information is only updated in accordance with the purposes of the data holding.

Principle 7: Safeguards for Personal Health Information

CIHI protects personal health information with security safeguards appropriate to the sensitivity of the information.

Policies	Related Procedures
Policy 7.1 The security safeguards protect personal health information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. CIHI protects personal health information that it holds or transmits regardless of the format in which it is held. **Policy 7.2** The nature of the safeguards depends on the sensitivity of the information that has been collected, the amount, distribution and format of the information and the method of storage. A higher level of protection safeguards more sensitive information. **Policy 7.3** Care is used in the disposal or destruction of personal health information to prevent unauthorized parties from gaining access to the information.	**Procedure 7.1 and 7.2** a) The Director, Information Systems, or designate(s) is responsible for protecting personal health information in electronic formats against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification, by: • Developing, implementing and monitoring procedures and processes to support the secure collection, access, retention, destruction, storage, transfer and release of personal health information; • Implementing privacy and security enhancing technologies to counter threats to personal health information; • Maintaining business recovery plans; • Responding to security incidents and breaches and taking corrective action to prevent similar breaches in the future; • Maintaining detailed inventories of system hardware, software and data; • Maintaining up-to-date system control and audit logs; and • Regularly reviewing and testing the effectiveness of the safeguards. b) The program manager is responsible for protecting personal health information in non-electronic formats against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification, by: • Implementing and monitoring program procedures and processes to safeguard personal health information from such risks, in keeping with the policies; • Designating staff who have responsibilities under the program procedures; and • Regularly reviewing and testing the effectiveness of the safeguards. c) The Manager, Human Resources and Administration, or designate, is responsible for protecting personal health information against loss or theft, as well as unauthorized access,

Policies	Related Procedures
	disclosure, copying, use, or modification, by developing, implementing and monitoring policies, procedures and systems that: • Control access to CIHI offices; • Provide staff with photo identification; • Ensure visitors are screened and supervised; and • Provide for the secure disposal and destruction of non-electronic records containing personal health information.
Policy 7.4 CIHI makes its employees aware of the importance of maintaining the confidentiality of personal health information through a privacy-training program and mechanisms for communicating information about CIHI's policies and procedures.	**Procedure 7.4** (a) The Manager, Human Resources and Administration or designate(s) ensures that each new employee: • Receives a copy of CIHI's *Privacy and Confidentiality of Health Information at CIHI* and signs a confidentiality pledge as a condition of employment; and • Attends the mandatory orientation session on CIHI's privacy principles, policies and practices. (b) The Chief Privacy Officer or designate(s); • Prepares and delivers the orientation session on CIHI's privacy principles, policies and practices; • Prepares and delivers the additional training sessions on CIHI's privacy principles, policies and practices to meet the needs of specific groups of employees; and • Prepares *Communiqués* on privacy matters, which are co-approved and issued by the Vice President, Operations.
Policy 7.5 CIHI prepares privacy impact assessments for its data holdings, both existing and proposed.	**Procedure 7.5** a) The Chief Privacy Officer maintains a template for privacy impact assessments (see Appendix B.) b) The program manager, or designate, completes a draft privacy impact assessment for the data holding, in consultation with program staff, the Privacy Secretariat and others as appropriate. c) The Chief Privacy Officer obtains input on the draft privacy impact assessment from the Chief Privacy Advisor.

Policies	Related Procedures
	d) The program manager, or designate, revises the draft privacy impact assessment. e) The program manager submits the draft privacy impact assessment to the Operations Management Committee for review and approval. f) Once approved, the Chief Privacy Officer, makes the privacy impact assessment publicly available, including posting on CIHI's Web site.

Related Documents

- Corporate Administrative Procedures (security related)
- Privacy Impact Assessment Template
- Completed Privacy Impact Assessments

Principle 8: Openness about the Management of Personal Health Information

CIHI makes information available about its policies and practices relating to the management of personal health information.

Policies	Related Procedures
Policy 8.1 CIHI is open about its policies and practices with respect to the management of personal health information. Individuals are able to acquire information about CIHI's policies and practices without unreasonable effort. This information is made available in a form that is generally understandable. **Policy 8.2** The information made available includes: a) The name or title, and address of the person who is accountable for CIHI's privacy policies and practices and to whom inquiries or complaints may be forwarded; b) The means for gaining access to personal health information held by CIHI and how to request access to the more complete personal health information held by data providers; c) A description of the types of personal health information held by CIHI, including a general account of their use; and d) A copy of any brochures or other information that explain CIHI's mandate, activities, policies, standards, or codes. **Policy 8.3** CIHI makes information on its privacy policies and practices available in a variety of ways. The method chosen depends on the nature of CIHI's functions and other considerations. For example, CIHI may choose to make brochures available in its offices, mail information to its data providers, provide on-line access, or establish a toll-free telephone number.	**Procedure 8.1, 8.2 and 8.3** a) Following consultation with the Manager, Communications, the Chief Privacy Officer determines the most appropriate means to make information available to individuals about CIHI's management of personal health information. Such means may include: • CIHI's Web site; and • Brochures, booklets and/or copies of key privacy related documents. b) The Chief Privacy Officer ensures that the following are publicly available: • General information on CIHI's privacy practices; • Frequently asked questions about CIHI's privacy practices; • Descriptions of CIHI's holdings of personal health information and what personal health information is made available to related organizations; • CIHI's privacy principles and policies document: *Privacy and Confidentiality of Health Information at CIHI*; • The name and address of the Chief Privacy Officer as the staff member to contact regarding: – inquiries about CIHI's privacy practices, – the procedure to access one's own personal health information (See Principle 9.), or – how to request access to more complete personal health information held by data providers; and • The name and address of the President and Chief Executive Officer as the individual accountable for CIHI's privacy policies and practices and the name and address of the Chief Privacy Officer as the staff member to whom inquiries or complaints can be forwarded.

Policies	Related Procedures
	c) When an individual makes a request for information on CIHI's privacy practices, the staff member receiving the request responds by: • Directing the individual to information on CIHI's Web site and/or providing copies of publicly available documents; and • Referring the inquiry to the Privacy Secretariat for response, if further assistance is required.

Related Documents

- CIHI Catalogue
- CIHI Privacy Brochure
- CIHI Web site (www.cihi.ca)
  - Privacy and Data Protection
  - Program Description
  - Frequently Asked Questions

Principle 9: Individual Access To and Amendment of Own Personal Health Information

Upon request, CIHI informs an individual of the existence, use and disclosure of his or her personal health information and gives access to that information. When an individual challenges the accuracy and completeness of the personal health information and requests to have it amended as appropriate, CIHI refers the individual to the data provider and makes amendments, if required, after receiving notification from the data provider of its decision on the amendment request.

Note:
In general, CIHI does not have readily identifiable personal health information and in certain situations, CIHI may not be able to provide access to all the personal health information it holds about an individual. Exceptions to the access requirement are limited and specific. The reasons for denying access are provided to the individual. Exceptions may include information that:

- Is prohibitively costly to provide;
- Contains references to other individuals;
- Cannot be disclosed for legal, security, or commercial proprietary reasons; or
- Is subject to solicitor-client or litigation privilege.

Amendment requests need to be considered by the data provider, as it is in the best position to determine the appropriateness of the requested amendments.

Policies	Related Procedures
Policy 9.1 Upon request, CIHI informs an individual whether CIHI holds personal health information about the individual. CIHI indicates the source of this information and refers the individual to the data providers concerned for access to the full personal health information held by them. CIHI also grants the individual access to his or her personal health information. CIHI may choose to make personal health information available through a health care practitioner. In addition, CIHI provides an account of the use that has been made or is being made of this personal health information and an account of the third parties to which it has been disclosed. **Policy 9.2** An individual is required to provide sufficient information to permit CIHI to provide an account of the existence, use and disclosure of personal health information. The information provided is only used for this purpose.	**Procedure 9.1. 9.2, 9.3 and 9.4** a) An individual may make a written request to: Privacy Secretariat Canadian Institute for Health Information 377 Dalhousie Street, Suite 200 Ottawa, Ontario, K1N 9N8 Fax: (613) 241-8120 The request may be for: • Access to his or her own personal health information held by CIHI; • The source of this personal health information; • An account of the use of this personal health information; and/or • An account of third parties to which this personal health information has been disclosed. b) The request must include: • Authentication of the requestor's identity in a form acceptable to CIHI. Forms of authentication may include: – certified copies of two pieces of formal identification including a photograph (e.g., driver's license, health card, etc.);

Policies	Related Procedures
Policy 9.3 In providing an account of third parties to which it has disclosed personal health information about an individual, CIHI attempts to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed personal health information about an individual, CIHI provides a list of organizations to which it may have disclosed information about the individual. **Policy 9.4** CIHI responds to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested personal health information is provided or made available in a form that is generally understandable. For example, if CIHI uses abbreviations or codes to record information, an explanation is provided.	– an affidavit from a notary public or lawyer that certifies that the requestor is the individual they claim to be; and – a signed statement, by a person who qualifies as a guarantor for passport purposes (such as a physician, police officer, pharmacist, school principal, professional accountant or bank signing officers), which certifies that the guarantor has known the requestor for at least two years and that the requestor is the individual they claim to be; • Sufficient identifying details for communication with the requestor and to permit an accurate search for the requestor's personal health information, such as full name, full address, phone number, e-mail address, full date of birth, gender and health care number. This information will only be used for the purpose of communicating with and authenticating the identity of the requestor; and • The time period for the requested personal health information. c) Upon receipt of a request, the Privacy Secretariat contacts the requestor to: • Clarify the nature and extent of the request; • Advise of the nature of the personal health information in CIHI's data holdings; • Advise that the requestor may contact the data providers if more complete personal health information is desired; • Obtain more details, if needed, to accurately locate the requestor's personal health information in CIHI's data holdings; and/or • Advise if further authentication of identity is required. d) The Privacy Secretariat sends an acknowledgement that the request has been received and includes any clarifications of its nature and scope. e) The Privacy Secretariat leads the response by: • Contacting appropriate CIHI program areas to request that they search for and provide copies of responsive records and/or information about sources, uses and disclosures, along with time required by the program area to perform this work;

Policies	Related Procedures
	• Reviewing the records with the program areas to determine if access will not be provided because the information is prohibitively costly to provide, contains references to other individuals, cannot be disclosed for legal, security, or commercial proprietary reasons, or is subject to solicitor-client or litigation privilege; • Preparing the records for examination or copying by severing all excepted personal health information; • Preparing, with assistance from program areas, explanations of abbreviations or codes so that the personal health information will be generally understandable; and/or • Determining if access should be provided through a health care practitioner. f) Fee Estimates • The Privacy Secretariat develops a fee estimate for access to the requestor's personal health information. • Where the Privacy Secretariat determines that the fee estimate represents an unreasonable barrier to access to personal health information for the requestor, the Privacy Secretariat will waive the fee in part or in full, as appropriate. • Where a fee or part fee is charged to the requestor, the Privacy Secretariat collects applicable fees prior to providing access. • Whether a fee or partial fee is charged or waived, the Privacy Secretariat will develop a fee assessment to account for the value of time spent assessing the requestor's personal health information. g) The Privacy Secretariat normally provides the requestor with a decision on the request within 30 working days, and in all cases within 60 calendar days, of the receipt of the request and provides the reasons for any denial of access. h) The Privacy Secretariat arranges for the requestor to access the personal health information. i) The Privacy Secretariat maintains a log of all access requests and the time required to process each.

Policies	Related Procedures
Policy 9.5 When an individual requests amendment of his or her personal health information, CIHI refers the individual to the data provider to request amendment of personal health information held by the data provider. **Policy 9.6** 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. Depending upon the nature of the personal health information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, CIHI transmits the amended personal health information to third parties having access to the information in question. **Policy 9.7** When a data provider notifies CIHI of an unresolved challenge to the accuracy and completeness of the personal health information, CIHI attaches or links the record of the unresolved challenge to the record of personal health information. When appropriate, the existence of the unresolved challenge is transmitted to third parties having access to the personal health information in question.	**Procedure 9.5, 9.6 and 9.7** a) When an individual requests amendment of his or her personal health information, CIHI refers the individual to the data provider(s) that originally provided the personal health information to CIHI. b) When a data provider notifies CIHI of its decision on an individual's request for amendment, the program manager: • Makes the appropriate amendments to the individual's personal health information; • Attaches or links any record of an unresolved challenge to the record of personal health information; • Notifies third parties to whom the personal health information was previously disclosed, if appropriate; and • Notifies the Privacy Secretariat, which maintains a log of amendment notifications.

Principle 10: Complaints About CIHI's Handling of Personal Health Information

An individual is able to address a challenge concerning compliance with its principles to CIHI's President and Chief Executive Officer, who is accountable for CIHI's compliance.

Policies	Related Procedures
Policy 10.1 CIHI has procedures in place to receive and respond to complaints or inquiries about its privacy policies and practices related to the handing of personal health information. The complaint procedures are easily accessible and simple to use. **Policy 10.2** CIHI informs individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. **Policy 10.3** CIHI investigates all complaints. If a complaint is found to be justified, CIHI takes appropriate measures, including, if necessary, amending its privacy policies and practices.	**Procedure 10.1, 10.2 and 10.3** a) Should any individual inquire about CIHI's privacy complaints procedure, CIHI staff provides the individual with a copy of this procedure. b) An individual may make a written complaint about CIHI's compliance with its privacy principles, policies, procedures or practices to: President and Chief Executive Officer Canadian Institute for Health Information 90 Eglinton Avenue East, Suite 300 Toronto, Ontario, M4P 2Y3 Fax: (416) 481-2950 The written complaint should provide: • Sufficient detail to permit investigation; and • Contact information for communication with the complainant, such as full name, full address, phone number, fax number and e-mail address. <u>First Level Review</u> c) Upon receipt of a complaint, the President and Chief Executive Officer forwards the complaint to the Chief Privacy Officer. d) The Chief Privacy Officer or designate sends an acknowledgement that: • The complaint has been received; and • Explains the complaint process. e) When the complaint relates to CIHI's handling of an access or amendment request (see Principle 9), the Chief Privacy Officer forwards the complaint to the Chief Privacy Advisor for investigation (see step (i) below). f) The Chief Privacy Officer or designate contacts the complainant to: • Clarify the nature and extent of the complaint; • Provide information on CIHI's complaint procedure; and • Obtain more details, if needed, to accurately locate the complainant's personal health

Policies	Related Procedures
	information in CIHI's data holdings, when required to investigate the complaint. g) The Chief Privacy Officer or designate investigates and responds to the complaint by: • Maintaining a log of activities related to the investigation and preparation of a response to the complainant; • Advising appropriate program areas and other relevant parties (such as the appropriate ministry of health or data provider) that a complaint has been received; • Requesting background information in relation to the complaint: • Reviewing the information to determine whether CIHI has complied with its privacy principles, policies and procedures in relation to the complaint; • Working with involved parties to seek resolution of the complaint; and • Providing a written response to the complainant, with a copy to the President and Chief Executive Officer, which summarizes the nature and findings of the investigation and, when appropriate, outlines the measures that CIHI is taking in response to the complaint, which may include amending its privacy policies, procedures and practices. h) The Chief Privacy Officer or designate: • Maintains a log of all complaints which includes the hours required to investigate and respond to the complaint; and • Provides information on all complaints to the President and Chief Executive Officer for the annual report to the Board of Directors. (See item m) below.) <u>Second Level Review</u> i) If the complainant is not satisfied with the results of the first level review, or if the complaint is related to CIHI's handling of an access or amendment request (see Principle 9), the Chief Privacy Officer forwards the complaint to the Chief Privacy Advisor for investigation and resolution. j) The Chief Privacy Advisor contacts the complainant to:

Policies	Related Procedures
	• Clarify the nature and extent of the complaint; • Provide information on CIHI's complaints process; and • Obtain more details, if needed, to accurately locate the requestor's personal health information in CIHI's data holdings, when required to investigate the complaint. k) The Chief Privacy Advisor investigates the complaint by: • Advising appropriate CIHI staff and other relevant parties (such as the appropriate ministry of health or data provider) that a complaint has been received; • Requesting background information from CIHI staff in relation to the complaint; • Reviewing the information to determine whether CIHI has complied with its principles, policies and procedures in relation to the complaint; • Working with involved parties to seek resolution of the complaint; and • Providing a written report to the President and Chief Executive Officer, with a copy to the complainant, which summarizes the nature and findings of the investigation and, when appropriate, makes recommendations in response to the complaint, which may include amending CIHI privacy policies, procedures and practices. l) The President and Chief Executive Officer: • Reviews the report of the Chief Privacy Advisor; • Determines what further action by CIHI, if any, is required; and • Provides a written response to the complainant, with a copy to the Chief Privacy Advisor, which summarizes the nature and findings of the investigation and, when appropriate, outlines the measures that CIHI is taking in response to the Chief Privacy Advisor's recommendations, which may include amending CIHI's privacy policies, procedures and practices. m) The President and Chief Executive Officer provides the Board of Directors with an annual report on the complaints made and the disposition of the complaints.

IV Policies for Institution-Identifiable Information

Institution-identifiable information means information that:

- Directly identifies a health institution; or
- Potentially identifies a health institution through the combination or linking of data elements.

Policies	Related Procedures
1. CIHI only discloses institution-identifiable information when the disclosure also complies with Part III of *Privacy and Confidentiality of Health Information at CIHI*. 2. Subject to 1 above, CIHI only discloses institution-identifiable information: a) To relevant ministries of health; b) To others, subject to the approval of CIHI's President and Chief Executive Officer and the signing of a Non-Disclosure Agreement that outlines conditions on data retention, use, disclosure, publication, and disposal; c) In CIHI publications with the approval of CIHI's President and Chief Executive Officer; and d) When the data are already in the public domain. 3. CIHI provides prior notification to institutions when institution-identifiable information is released under 2 b) or c). 4. Additionally, under 2 b) or c), CIHI obtains institutional authorizations before disclosing institution-identifiable information collected prior to April 1996 5. In all other cases, CIHI discloses institution-identifiable information only: a) With the institution's authorization; or b) When required by law. 6. CIHI may conduct analyses of institution-identifiable information for external parties within CIHI's secure environment, consistent with the identified purposes of the data holdings and subject to CIHI's disclosure policies in *Privacy and Confidentiality of Health Information at CIHI*. 7. Precedent setting and sensitive requests require the written approval of the CIHI's President and Chief Executive Officer.	The procedures for processing requests for institution-identifiable information are integrated with the procedures for processing requests for personal health information. See **Procedure 5.10 to 5.13** Part III of this document.

Policies	Related Procedures
8. If CIHI receives a complaint by any person that a recipient of institution-identifiable information has made false or misleading statements in the request for data or has violated one or more conditions in the Non-Disclosure Agreement, CIHI will investigate. When the concern or complaint is substantiated, CIHI imposes sanctions, which may include: a) A written complaint to the recipient organization; b) Recovery of data disclosed by CIHI; c) A report to the relevant research ethics review body, funding body, data provider and ministry of health, as applicable; d) Refusal of future access to data; or e) Legal action.	

Related Documents

- Client Information Request Form for Aggregate Data
- Non-Disclosure/Confidentiality Agreement for Aggregate Data.
- Client Information Request Form for Record-Level Data
- Non-Disclosure/Confidentiality Agreement for Record-Level Data.
- CIHI Consent/Authorization Requirements for Disclosures/Linkages

Appendix A: Glossary

Access
The entitlement of an individual (or his or her legally authorized representative) to examine or obtain copies of his or her own personal health information held by an organization.

Collection
The process of gathering or obtaining personal health information, either directly from an individual or indirectly, for example, from an individual's legally authorized representative or a health services organization.

Confidentiality
The duty to ensure that information is accessible only to authorized persons.

Consent
Voluntary agreement by an individual, or his or her legally authorized representative, to allow the collection, use or disclosure of the individual's personal health information.

Data Linkage
The bringing together of two or more records of personal health information to form a composite record.

Data Provider
An organization or individual that discloses health data to CIHI.

De-identified Information
Personal health information that has been modified, so that the identity of the subject individual cannot be determined by a reasonably foreseeable method.
This involves:
- Removal of name and address, if present; and
- Removal or encyption 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 they do not permit identification of the subject individual by a reasonably foreseeable method.

Disclose
To release or make available personal health information to a person, other than the person the information concerns or a person employed by, or in the service of, the party holding the information.

Health Information
A broad term encompassing information of all types about health and health care, including personal health information, institution-identifiable information, and health expenditure information.

Institution-identifiable Information
Information that:
- Directly identifies a health institution; or
- Potentially identifies a health institution through the combination or linking of data elements.

Partner Organization
An organization that collaborates with CIHI in carrying out CIHI's mandate. Partner organizations include ministries of health, data providers and Statistics Canada.

Personal Health Information
Information about an individual that:
- Identifies the 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 and that may include information related to:
  - the physical or mental health of the individual;
  - the provision of health services to the individual;
  - the registration of the individual for the provision of health services;
  - the donation of any body part or bodily substance of the individual, or is derived from the testing or examination of any such body part or bodily substance;
  - payments or eligibility for health care;
  - a number, symbol or particular assigned to an individual to uniquely identify the individual for health system purposes;
  - information that is collected in the course of the provision of health services to the individual; or
  - registration and practice information about a health professional.

Privacy
The right of an individual to control the collection, use and disclosure of personal health information about himself or herself.

Privacy Impact Assessment
A tool used to assess the possible privacy-related consequences of systems and practices for the collection, use and disclosure of personal information, including personal health information.

Residual Disclosure
Situations in which the identity of an individual could be determined by reasonably foreseeable methods from personal health information (including when the data have been aggregated or have had direct identifiers stripped, encrypted, or masked).

Record-level Data
Data in which each record is related to a single individual or organization (sometimes referred to as "micro data.")

Security
The protection of personal health information from unauthorized or unintentional loss, theft, access, use, modification, or disclosure.

Use
The treatment and handling of personal health information within an organization. Disclosure does not constitute "use."

Appendix B: CIHI'S Privacy Impact Assessment Template

1. Introduction and Overview

2. Description of the Database
   - Need for the Database
   - Current and Intended Scope
   - Objectives
   - Conceptual Technical Architecture

3. Data Collection
   - Statutory Authoritites for Collection, Use and Disclosure of Information
   - Limits on Data Collected
   - Sources of Data
   - Personal Information
   - Location of the Data
   - Data Retention/Destruction
   - Consent Issues

4. Use and Disclosure of Data
   - Users of Database Information
   - Disclosure of Information
   - Access Rights for Individuals to their Personal Information

5. Privacy Standards: Concerns and Security Measures
   - Identifiers and Records Linkages
   - Security Safeguards
   - Disclosure Avoidance Practices; Release of Small Cell Size

6. Conclusions

Appendix C: Information Flow Diagram—Overview

The Information Flow Diagram on the following page provides an overview of the flow of personal health information to CIHI and its subsequent use and disclosure.

The shaded box represents CIHI.

The organizations listed down the left side are the types of data providers. The arrows from the data providers indicate information flows to specific CIHI data holdings by those data providers. For example, the provincial/territorial regulating authorities for Registered Nurses send data to RNDB.

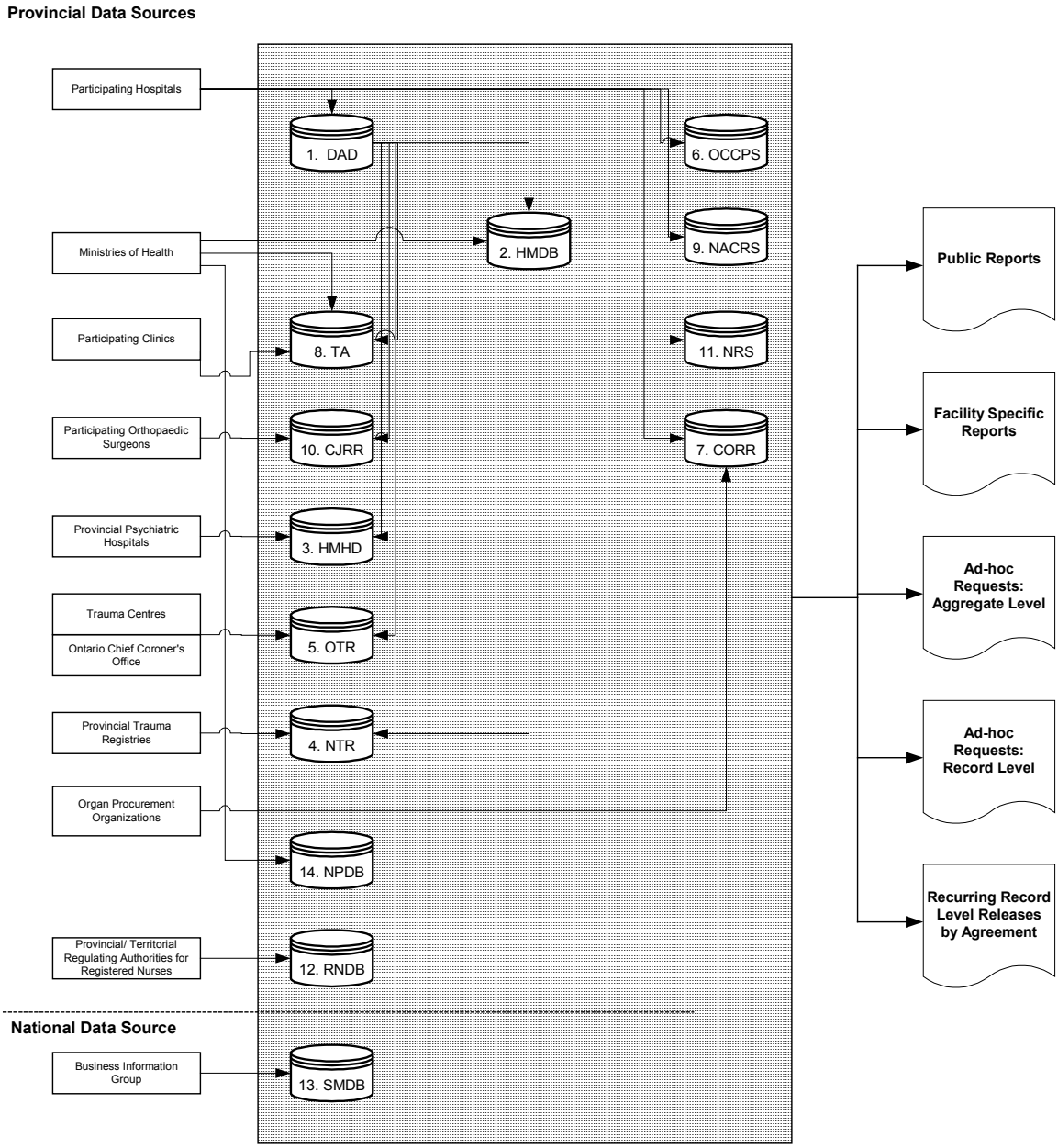
Depending on the province or territory, some data providers may not submit data. For example:
- Hospitals in Quebec do not provide data to DAD; and
- OTR and OCCPS only contain Ontario data.

The arrows within the box show how data from one data holding may be used to feed information to another data holding. For example, HMD provides data to NTR.

The small graphics on the right side illustrate the various types of disclosures that occur. All disclosures are subject to the privacy principles and policies in *Privacy and Confidentiality of Health Information at CIHI, April 2002, 3rd edition.*

The diagram represents the information flow at December 2001. The abbreviations for the data holdings are as follows:
- Canadian Joint Replacement Registry (CJRR)
- Canadian Organ Replacement Register (CORR)
- Discharge Abstract Database (DAD)
- Health Personnel Database (HPDB)
- Hospital Mental Health Database (HMHD)
- Hospital Morbidity Database (HMD)
- National Ambulatory Care Reporting System (NACRS)
- National Physician Database (NPDB)
- National Rehabilitation Reporting System (NRS)
- National Trauma Registry (NTR)
- Ontario Chronic Care Patient System (OCCPS)
- Ontario Trauma Registry (OTR)
- Registered Nurses Database (RNDB)
- Southam Medical Database (SMDB)
- Therapeutic Abortion Database (TA)

Information Flow Diagram—Overview



***This overview presents a high-level illustration of CIHI information flows.**
It does not depict provincial/territorial variations, nor variations for specific data holdings.