Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

All rights reserved.

The contents of this publication may be reproduced unaltered, in whole or in part and by any means, solely for non-commercial purposes, provided that the Canadian Institute for Health Information is properly and fully acknowledged as the copyright owner. Any reproduction or use of this publication or its contents for any commercial purpose requires the prior written authorization of the Canadian Institute for Health Information. Reproduction or use that suggests endorsement by, or affiliation with, the Canadian Institute for Health Information is prohibited.

For permission or information, please contact CIHI:

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

© 2022 Canadian Institute for Health Information

How to cite this document:

Cette publication est aussi disponible en français sous le titre Rapport annuel de l’ICIS sur le respect de la vie privée, 2021-2022.
# Table of contents

- **Introduction** ................................................................. 4
- **Section 1: Legal context in Canada** ........................................ 5
- **Section 2: Data-sharing agreements** ........................................ 5
- **Section 3: Policy review** .................................................... 7
- **Section 4: Privacy and security training and awareness** ................. 8
- **Section 5: Privacy impact assessments** .................................... 9
- **Section 6: Renewal of CIHI’s prescribed entity status under Ontario’s Personal Health Information Protection Act, 2004** .................. 10
- **Section 7: Privacy breaches** .................................................. 11
- **Section 8: Privacy Audit Program** ......................................... 11
- **Section 9: CIHI’s Secure Access Environment** .......................... 12
- **Conclusion** ........................................................................ 12
Introduction

The past year has been a busy one for privacy at the Canadian Institute for Health Information (CIHI). Externally, we have been closely monitoring what has, and continues to be, a very active legislative landscape on the privacy front. With the passing of Bill 64, An Act to modernize legislative provisions as regards the protection of personal information, Quebec significantly modernized its private- and public-sector privacy regimes. Not only did the new legislation add new obligations for organizations doing business in Quebec, but it also introduced stringent enforcement measures. The new private-sector requirements will come into effect in 3 phases over the course of the next 3 years, most taking effect as of September 22, 2023.

Ontario’s new proposed privacy law will govern commercial activities more broadly than the federal Personal Information Protection and Electronic Documents Act (PIPEDA), which currently applies to businesses in the province. On the health privacy front, we are eagerly awaiting amendments to the Personal Health Information Protection Act, 2004 (PHIPA) which will involve specific requirements around de-identification.

At the federal level, Bill C-11, designed to modernize PIPEDA, died on the order paper with the September federal election, but an amended bill is expected to be tabled early in 2022.

Internally, we have begun to prepare for the next review period for our prescribed entity status under PHIPA, set to begin in the fall of 2022. As a prescribed entity, CIHI must have in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information. CIHI must have its information practices reviewed and approved by the Information and Privacy Commissioner of Ontario (IPC/ON) every 3 years. This review process provides our data providers and the Canadian public with the assurance that CIHI’s information management practices comply with PHIPA and with privacy and security best practices. The IPC/ON has indicated that the upcoming review will focus on demonstrable accountability. Accountability is a basic tenet of 21st century data protection law and governance and is reflected in privacy legislation globally: it is rooted in the notion that to be trusted, accountability always needs to be capable of being demonstrated. To help CIHI prepare for the upcoming review, CIHI’s President and CEO, who has ultimate accountability for privacy and information security at CIHI, mandated the creation of a demonstrable accountability program, which is being led by CIHI’s Chief Privacy Officer and Chief Information Security Officer.
Section 1: Legal context in Canada

CIHI's data providers supply CIHI with the data it needs to fulfill its mandate: to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care. In order to facilitate the flow of information from data providers to CIHI, it is critical that CIHI's data providers have clear lawful authority to disclose personal health information (PHI) to CIHI without an individual’s consent.

When a jurisdiction enacts or amends health privacy legislation, CIHI provides input to the jurisdiction requesting that the new or amended legislation establish explicit lawful authority for disclosures of PHI to CIHI, without an individual’s consent. CIHI provides this input either through the jurisdiction’s invitation to the public to make submissions regarding the legislation or through CIHI’s ongoing engagement with the jurisdiction.

At the time of writing this report, CIHI has not made any submissions since CIHI’s Annual Privacy Report, 2020–2021 was published. More generally, the following legislative developments are relevant to CIHI and are being closely monitored:

- Pending update to PHIPA and its Regulation to provide guidance around requirements to de-identify PHI;
- Quebec’s Bill 64, An Act to modernize legislative provisions as regards the protection of personal information; and
- Quebec’s Bill 19, An Act respecting health and social services information and amending various legislative provisions.

Section 2: Data-sharing agreements

As a health system user of PHI, CIHI enters into data-sharing agreements (DSAs) with data providers from across the country. DSAs facilitate the flow of data to CIHI and support CIHI’s mandate.

Since CIHI’s Annual Privacy Report, 2020–2021 was published, CIHI has signed DSAs with the following data providers:

- New Brunswick Department of Social Development — governing data submitted by New Brunswick’s long-term care (LTC) facilities (i.e., Integrated interRAI Reporting System [IRRS] data); and
- New Brunswick Department of Health — governing the remaining New Brunswick data submitted to CIHI. This updated DSA replaces the prior umbrella DSA and the prior pharmaceutical data DSA. (New Brunswick’s Canadian Patient Experiences Reporting System [CPERS] data continues to be governed by CIHI’s DSA with the New Brunswick Health Council.)
CIHI is also in DSA negotiations with the following data providers:

- Northwest Territories — to add the Tłı́chǫ Community Services Agency to the DSA as one of the data providers;
- British Columbia — to update CIHI’s DSAs with the province;
- Statistics Canada — to replace the expired DSA under which CIHI is provided with LTC-related survey data; and
- Ontario Health — to govern its submission of home care data to CIHI on behalf of local health integration networks.

In addition to entering into DSAs with data providers, in some cases CIHI may also enter into a DSA with a data requestor. A DSA with a data requestor becomes necessary when a request is for a significant volume of record-level data and when the need for the data is ongoing and, generally, is related to a broader program of work (as opposed to a time-limited, project-specific research initiative).

Since CIHI’s Annual Privacy Report, 2020–2021 was published, CIHI has signed a DSA with the following data requestor:

- Heidelberg University Hospital — to facilitate CIHI’s disclosure of de-identified record-level data for inclusion in the International Pediatric Nephrology Association’s Global Renal Replacement Therapy Registry, which supports the study of the epidemiology, demography and treatment of pediatric renal diseases.

CIHI amended DSAs with the following data recipients:

- Health Canada — to facilitate CIHI’s disclosure of additional aggregate and de-identified record-level health workforce data, and to accommodate more frequent (i.e., monthly) data disclosures; and
- ICES — to allow ICES to provide CIHI data to the Ontario Ministry of Health and certain Indigenous organizations for pandemic response, as well as to knowledge users associated with the Applied Health Research Question Program.

CIHI is also negotiating amendments with the following data recipient:

- Better Outcomes Registry & Network (BORN) — to update the DSA to address extended data retention periods that have been approved by a research ethics board or that are required in order for BORN to fulfill its mandate.
Section 3: Policy review

CIHI is committed to the ongoing review of its privacy policies, procedures and practices in order to determine whether any amendments are needed or any new ones are required. This review takes place annually; any proposed changes to CIHI’s privacy policies are brought to the Senior Management Committee for review and approval. In the case of material changes to CIHI’s Privacy Policy, 2010, approval from the Board of Directors is required. The Privacy Policy, 2010 was first approved by the Board in February 2010.

In October 2021, CIHI received formal notification from the IPC/ON that its status as a prescribed entity under Section 45 of Ontario’s PHIPA had been approved for a further 3-year period. At the same time, included with the notification were 22 recommendations, 1 of which was to “develop and implement distinct policies and procedures in accordance with the policy structure and naming conventions set out in Appendix A of the manual. The stated goal of this is to better align CIHI’s policies with the expectations set out in the manual and thereby facilitate locating relevant content in any future review.”

To meet this requirement, CIHI undertook a “mapping and gapping” exercise where all CIHI policies, procedures and guidelines subject to IPC/ON oversight were reviewed against the specific requirements set out in the IPC/ON manual to identify and address any gaps. At the same time, a requirement for a number of new policies was also identified, and these policies have been drafted and implemented. They include CIHI’s Privacy Audit Policy, Policy for the Execution of Confidentiality Agreements and Corporate Action Plan (CAP) Policy. At the time of writing, the majority of the relevant policies, procedures and guidelines have been updated and implemented. It is expected that any remaining revisions will be completed by the end of March 2022 to address the recommendations.
Section 4: Privacy and security training and awareness

Privacy and security awareness forms part of CIHI's mandatory privacy and security training. CIHI’s Privacy and Security Training Policy encompasses both privacy and security orientation for new employees and ongoing privacy and security training for current employees. In addition, the policy sets out the requirements for traceable, mandatory privacy and security training for all CIHI staff. Staff awareness is critically important to CIHI’s culture of privacy and security.

Information Security Awareness Month

At CIHI, September is Information Security Awareness Month. This year, the focus was on how to maintain privacy and security while working from home and how this applies to day-to-day activities. The Information Security team hosted a virtual information session about ransomware for all CIHI staff. This year’s campaign also featured regular intranet articles during the month addressing various topics, as well as a refresher about security when working from home.

January is Privacy Awareness Month

January is Privacy Awareness Month at CIHI. Intranet articles appear throughout the month, and all CIHI staff must successfully complete mandatory annual privacy and security training, and renew their confidentiality agreement, prior to January 31. This year, the training component was a course covering sharing information via different Microsoft 365 applications and what steps to take to ensure staff share appropriately. All active CIHI staff completed the course in January 2022.
As well, in response to CIHI enabling the ability to share OneDrive files and folders externally in February 2022, staff from Privacy and Legal Services, Information Security, and Infrastructure, Business Operations and Technology Services have been regularly publishing articles and reminders on the intranet about safe and secure sharing via OneDrive.

Section 5: Privacy impact assessments

CIHI’s Privacy Impact Assessment Policy is its governing document on the conduct of privacy impact assessments (PIAs). To assess privacy risks, PIAs have been conducted for all CIHI databases containing either PHI or health workforce personal information. The PIAs are renewed at least every 5 years or in the following circumstances:

- When significant changes occur to functionality, purposes, data collection, uses, disclosures, relevant agreements or authorities for a program, initiative, process or system, and such changes need to be reflected in the PIA;
- When other changes occur that may potentially affect the privacy and security of those programs, initiatives, processes or systems; or
- When CIHI’s chief privacy officer determines that an update of a PIA or a new PIA is required and recommends the same.

Privacy and Legal Services has created a PIA log and schedule to track and record the conduct of PIAs.

For 2021–2022, PIAs for the following are currently in progress or were completed:

- Integrated interRAI Reporting System (IRRS) — PIA completed;
- Secure Access Environment — PIA completed;
- Insured Persons Repository (IPR) — new PIA in progress;
- National Rehabilitation Reporting System (NRS) — renewal of 2015 PIA in progress;
- Patient-Level Physician Billing (PLPB) Repository — renewal of 2015 PIA in progress;
- Ontario Mental Health Reporting System — renewal of 2016 PIA in progress;
- Continuing Care Reporting System — renewal of 2016 PIA in progress;
- Home Care Reporting System — renewal of 2016 PIA in progress; and
- Hospital Mental Health Database — renewal of 2016 PIA in progress.
Section 6: Renewal of CIHI’s prescribed entity status under Ontario’s *Personal Health Information Protection Act, 2004*

Every 3 years, the IPC/ON is required to review the information practices of organizations designated as prescribed entities under Ontario’s PHIPA. CIHI first received prescribed entity status in 2005, and its status was subsequently renewed in 2008, 2011, 2014 and 2017. CIHI submitted its report at the end of October 2019 for the renewal period November 1, 2017, to October 31, 2020.

On October 31, 2020, CIHI received formal notification from the IPC/ON that, based on its review of CIHI’s report and affidavit, it is satisfied that CIHI continues to have in place practices and procedures to protect the privacy of individuals whose PHI it receives and to maintain the confidentiality of that information in accordance with the requirements of PHIPA. Accordingly, effective October 31, 2020, the Commissioner advised that the practices and procedures of CIHI continue to be approved for a further 3-year period.

As reported last year, included with the notification were 22 recommendations, marking a change from the previous 3 review periods where CIHI received only 4 recommendations in total. Of the 22 recommendations received in the current review period, 1 was to complete CIHI’s existing initiative to develop a policy and related procedures for privacy audits. The remaining 21 recommendations resulting from the 2020 review do not substantially improve CIHI’s privacy and security programs. For example, one of the recommendations is to “develop and implement distinct policies and procedures in accordance with the policy structure and naming conventions set out in Appendix A of the manual. The stated goal of this is to better align CIHI’s policies with the expectations set out in the manual and thereby facilitate locating relevant content in any future review.” The remainder reflect minor changes to CIHI’s privacy and security documentation and/or clarifications in its report to the IPC/ON as to how CIHI documentation currently aligns with the manual.

Work is ongoing to complete these recommendations prior to the next submission date of October 31, 2022 (1 year prior to the renewal date of October 31, 2023).
As mentioned earlier in the report, CIHI undertook a “mapping and gapping” exercise where all CIHI policies, procedures and guidelines subject to IPC/ON oversight were reviewed against the specific requirements set out in the IPC/ON manual to identify and address any gaps. This work is proceeding well, and the majority of the relevant policies, procedures and guidelines have been updated and implemented. It is expected that any remaining revisions will be completed by the end of March 2022 to address the recommendations.

Section 7: Privacy breaches

There were no privacy breaches, as defined by CIHI’s Privacy and Security Incident Management Protocol, in 2021–2022.

Section 8: Privacy Audit Program

Privacy completed the planned compliance survey audit of third-party record-level data recipients in the second quarter of 2021–2022. The purpose of the Privacy Compliance Survey Audit is to initiate self-audit by all organizations that have received CIHI record-level data via the Corporate Data Request Program and to provide a means for CIHI to bring organizations that are not meeting their responsibilities into compliance. This process is designed to reduce the risks to CIHI data across the full cohort of organizations receiving CIHI data via the Corporate Data Request Program.

Remote access to CIHI data by data recipients was a part of, but not the focus of, the 2021 survey audit. The 1 question in the 2021 survey audit addressing remote access was high level and not designed to fully assess the range of compliance issues associated with remote access to CIHI data by data recipients. However, in light of the fact that working from home will continue to be a reality and that CIHI’s minimum security requirements associated with third-party data requests were updated in November 2021, it is important that CIHI understands in greater detail the administrative and technical controls that have been put in place to ensure secure remote access to CIHI data. Consequently, a second follow-up compliance survey audit of all third-party record-level data recipients will be conducted in 2022. The follow-up audit will focus on ensuring compliance with CIHI’s technical requirements for remote access to CIHI data.
Section 9: CIHI’s Secure Access Environment

CIHI has developed a Secure Access Environment (SAE) where external clients (researchers) will have secure, controlled remote access to CIHI data via a secure and encrypted session. This will eliminate, to a great extent, the storage of PHI and de-identified data used for research purposes outside of CIHI’s secure environment.

Some important features of the SAE include the following:

- The SAE is protected by a firewall; no internet access is permitted from within the SAE.
- The SAE provides central administration of project and user accounts.
- Access to the SAE requires multi-factor authentication, which ensures privacy of connection and prevents unauthorized access.
- Through contractual obligations, users are prohibited from accessing the SAE from outside Canada.
- Only aggregate outputs that adhere to CIHI’s Vetting Rules may leave the SAE, to prevent inadvertent disclosure of confidential personal health information.
- It provides read-only access; record-level data cannot be copied or removed from the SAE.
- The SAE provides secure storage and backup for authorized project data.

As of Q4 2021–2022, the SAE is available to external requestors for record-level CIHI data.

Conclusion

In the new year, we will continue to monitor legislative developments for potential impacts on CIHI and will keenly track evolving best practices in the areas of privacy and information security. We are excited to continue our work on the Demonstrable Accountability Program, as we view it as a key mechanism by which we can ensure the effective operationalization of our Privacy and Information Security Framework. Recognizing that demonstrable accountability is a process of continuous improvement, we will be working on a sustainability model for this important body of work.