CIHI's Annual Privacy Report

2019–2020

Canadian Institute for Health Information

Institut canadien d'information sur la santé

Table of contents

Introduction

2019–2020 was another very active year for privacy at the Canadian Institute for Health Information (CIHI). We continued to keep a close eye on the external privacy landscape for legislative developments as well as changes in best practices. The General Data Protection Regulation (GDPR)[i] has set the new gold standard in terms of data privacy and security and has served, on a global scale, as a catalyst to address gaps in information governance. From sweeping data privacy legislation in California to proposed amendments to federal privacy legislation in Canada, the current privacy environment is continuously and rapidly evolving. It was also a year in which the increasing role of artificial intelligence resulted in data privacy increasingly finding itself interconnected with other areas such as ethics, human rights, societal values and intellectual property rights. We anticipate that this trend will continue and is likely to place increasing strain on existing legal frameworks.

One feature of the GDPR that is particularly noteworthy is the elevation of the concept of privacy by design to the status of legislative requirement. This reinforces the imperative that privacy compliance be embedded into the cultural and business fabric of organizations. At CIHI, we have been long-standing adopters of privacy by design; this year, as part of the continued alignment of our Privacy and Information Security programs, we took the next step in maturing our current training and awareness programs. In September, as part of our 2019 Information Security Awareness Month, the Privacy and Legal Services and Information Security departments launched a Privacy and Security by Design (PSbD) curriculum. The goal is to design a curriculum that will ensure staff understand the strategic importance of PSbD and recognize their role in implementing this key concept in their work at CIHI. We continued to evolve this curriculum as part of our Privacy Awareness month in January 2020 and through a series of in-person sessions with staff across CIHI. We are excited to have undertaken this new initiative.

i. The GDPR is the European privacy legislation introduced in May 2018.

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 requests 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. CIHI has not made any submissions since *CIHI's Annual Privacy Report, 2018–2019* was published; however, the following legislative developments are relevant to CIHI and are being closely monitored:

- The potential implementation of health privacy legislation in British Columbia and Nunavut;
- Potential amendments to modernize Ontario's *Personal Health Information Protection Act*; and
- Potential amendments to the federal *Personal Information Protection and Electronic Documents Act*.

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.

With respect to CIHI's data providers, since *CIHI's Annual Privacy Report, 2018–2019* was published, CIHI has ratified a DSA with the following:

- British Columbia, for an updated umbrella DSA that governs the wide range of PHI the province submits.

CIHI is currently negotiating DSAs or amendments with the following:

- New Brunswick, for an updated umbrella DSA to govern the wide range of PHI the province submits;
- Winnipeg Regional Health Authority (WRHA), for a DSA to govern WRHA's current submission of Canadian Organ Replacement Register (CORR) data;
- Saskatchewan Cancer Agency, for a DSA to govern the agency's submission of National System for Incident Reporting (NSIR) data;
- Alliance for Healthier Communities, for the submission of primary health care PHI; and
- British Columbia College of Nursing Professionals (BCCNP), for the submission of health workforce personal information.

In addition to entering into DSAs with data providers, in some cases CIHI may also enter into a DSA or another legally binding instrument 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, 2018–2019* was published, CIHI ratified a DSA amendment with the following data requestor:

- Better Outcomes Registry and Network (BORN), to facilitate BORN's disclosure of de-identified data linked to the Public Health Agency of Canada, and to facilitate BORN's disclosure of aggregate data to third parties in general.

CIHI is currently in negotiation with the following data requestor:

- AMR Medical Research B.V. (related to the Netherlands-based International Pediatric Nephrology Association), for a DSA to govern CIHI's disclosure of de-identified CORR data.

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 was first approved by the Board in February 2010.

The following is a list of the policies reviewed during 2019–2020 and any action taken:

- *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010* (Privacy Policy, 2010) — no changes necessary;
- Procedures related to the Privacy Policy, 2010 — reviewed on an ongoing basis and updated as necessary;
- *Privacy Impact Assessment Policy* — revised to include reference to the *Privacy and Security Risk Management Policy* and processes;
- *Privacy and Security Training Policy* and related procedures — minor editorial changes;
- *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* — minor editorial changes;
- *Privacy and Security Risk Management Policy*, *Framework* and methodology — revised to address changes in the Privacy, Security and Confidentiality Committee's terms of reference; and
- *Privacy and Security Incident Management Protocol* — revised to include additional reporting requirements and to align with *CIHI's Business Continuity Plan*.

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.

At CIHI, September is Information Security Awareness Month. This year, the focus was on PSbD and the importance of integrating privacy, security and legal requirements in the foundational design of all systems and processes. Staff from the Information Security team and from Privacy and Legal Services co-hosted information sessions that were attended by staff from all CIHI offices. This year's campaign also featured regular intranet articles during the month, and a return of the annual presentation on home and personal security. In this presentation, CIHI information security experts summarized the most important events related to information security in 2019 and provided the latest recommendations to help staff secure their personal information.

January is Privacy Awareness Month at CIHI. Intranet articles appear throughout the month, and all CIHI staff must successfully complete the mandatory annual privacy and security training, and renew their confidentiality agreement, prior to January 31. This year, the training component was a new course covering the privacy and security fundamentals of working at CIHI. All active CIHI staff completed the course in January 2020; going forward, all new CIHI staff will complete the course as well.

Privacy resources

Privacy and Legal Services makes available to staff a number of resources regarding privacy changes and trends within and outside Canada. One such resource is a yearly compilation of health care–related privacy items. This document provides an overview of key privacy developments, primarily in the health care sector, from across the country, as well as emerging privacy issues that may have potential implications for CIHI. The document is sourced from annual reports published by commissioners/ombudsmen, reports (where published) on relevant privacy breaches investigated by commissioners/ombudsmen, the news media and other media sources.

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.

In 2019–2020, PIAs for the following were in progress or completed:

- CIHI Portal — renewal of 2014 PIA in progress;
- Population Risk Adjustment Group (PRAG) Project: POP Grouper — renewal of 2015 PIA in progress;
- Patient-Level Physician Billing (PLPB) Data Repository — renewal of 2015 PIA in progress;
- Canadian Patient Experiences Reporting System (CPERS) — renewal of 2015 PIA in progress;
- Canadian Joint Replacement Registry (CJRR) — update of 2015 PIA in progress;
- NSIR Addendum — update of 2018 PIA in progress;
- Integrated interRAI Reporting System (IRRS) — new PIA in progress;
- Health Human Resources Database, Nursing Database and Health Workforce Database — PIA completed;
- Clinical Administrative Databases — PIA completed;
- Canadian Patient Cost Database — PIA completed;
- Trauma Registries — PIA completed; and
- Patient-Reported Outcome Measures (PROMs) Program for Hip and Knee Arthroplasty — PIA completed.

Section 6: Renewal of CIHI's prescribed entity status under Ontario's *Personal Health Information Protection Act, 2004*

Every 3 years, the Information and Privacy Commissioner of Ontario (IPC/ON) is required to review the information practices of organizations designated as prescribed entities under Ontario's *Personal Health Information Protection Act*. 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. As of the writing of this report, the IPC/ON has not responded with any comments.

Section 7: Privacy breaches

There were no major privacy breaches, as defined by CIHI's *Privacy and Security Incident Management Protocol*, in 2019–2020.

Section 8: Privacy Audit Program

Privacy and Legal Services reported on 2 audits under the Privacy Audit Program in 2019–2020:

1. In 2018, for the first time, CIHI used an online survey tool to replace its annual certification process. In the annual certification process, for each project for which CIHI has disclosed record-level data for time-limited research activities, Privacy staff contact the recipient organization each year and require confirmation of continued compliance with the terms of the agreement under which the data was disclosed. Privacy initiated this process primarily as a means to ensure continued contact with organizations responsible for CIHI record-level data over the 3 or more years of data retention for a typical research project. A typical annual certification process requires all organizations to reply by email, certifying their continuing compliance with the conditions of the disclosure agreement and updating their contact information.

   CIHI's first Privacy Compliance Survey Audit required organizations to complete a short online survey audit designed to provide more detailed compliance verification in specific areas of concern to CIHI's Privacy and Information Security departments. Privacy reported the findings to the Governance and Privacy Committee in October 2019.

   In addition to serving as an important reminder for recipients about their privacy and security obligations under CIHI's disclosure agreement, the survey audit was an effective way to bring organizations that were not meeting their responsibilities into compliance. As such, an online survey audit will become a standard component of CIHI's Privacy Audit and Compliance Monitoring Program, and deployed at a frequency that reduces the risk of survey fatigue (e.g., every 3 years).

2. In September 2019, Privacy staff conducted a full on-site privacy compliance audit of the University Health Network (UHN), specifically a research project using PHI supplied by CIHI. External privacy audits constitute an important component of CIHI's Privacy Audit Program. They have the added educational value of identifying best privacy practices and strengthening policies, procedures and practices that could more adequately protect data disclosed to external third parties. The process is designed to verify, in a collaborative manner, that data recipients adhere to the terms and conditions in agreements they sign with CIHI. External data recipient audits are normally conducted annually.

   The audit did not identify any non-conformities with respect to the obligations set out in the agreement that UHN signed prior to receiving PHI from CIHI. In addition, 3 opportunities for improvement were identified by CIHI.

Section 9: Cloud strategy

CIHI must ensure the highest possible protection of the confidentiality, integrity and availability of the health information we maintain. Emerging stakeholder demands mean that CIHI must provide a technology infrastructure that is not only secure, but also nimble, easily scalable and cost-effective. To this end, CIHI has adopted a cloud-first approach for all new information processing solutions.

Privacy and Legal Services and Information Security were involved in developing this strategy from the earliest opportunity, and all decisions regarding the selection and use of cloud providers are subject to a rigorous risk management process, in accordance with CIHI's *Privacy and Security Risk Management Framework*.

The terms that CIHI has negotiated with its cloud providers for use of their secure, off-site servers allow CIHI to meet its strict privacy and security requirements, as well as all obligations in its DSAs.

Conclusion

Another productive year has come to a close, and we are looking ahead to a new year in which we will build our joint privacy and security training curriculum, positioning PSbD as an essential tool to enable CIHI to meet its statutory and legal obligations and to maintain stakeholder trust. We will monitor the external landscape for anticipated changes in privacy legislation at the federal, provincial and territorial levels. We also look forward to the opportunity to continue to evolve our Privacy Program to keep pace with changes in best practices: those seem inevitable in an environment where rapidly changing technologies present novel privacy and security challenges.

help@cihi.ca

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

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

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

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

cihi.ca

21559-0120