CIHI’s Annual Privacy Report, 2018–2019
# Table of contents

Introduction ................................................................................................................................ 3

Section 1: Legal context in Canada ............................................................................................ 3

Section 2: Data-sharing agreements .......................................................................................... 4

Section 3: Policy review ............................................................................................................. 5

Section 4: Privacy and security training and awareness ............................................................. 6

Section 5: Privacy impact assessments ..................................................................................... 7

Section 6: Renewal of CIHI’s prescribed entity status under Ontario’s *Personal Health Information Protection Act, 2004* ........................................................................................................ 8

Section 7: Privacy breaches ....................................................................................................... 8

Section 8: Privacy and Health Data Access Symposium ............................................................ 8

Section 9: Cloud strategy ........................................................................................................... 9

Conclusion ................................................................................................................................ 9
Introduction

The year 2018–2019 was another busy one as the Canadian Institute for Health Information (CIHI) continued to evolve our Privacy Program to ensure it remains sound and responsive to change and innovation. An important aspect of that evolution was our continued emphasis on recognizing the inter-dependencies between privacy and security. We continue to align CIHI’s Privacy and Information Security programs, and a hallmark of those programs is the excellent collaboration between the 2 branches responsible for them. One area where this collaboration has proven particularly effective is in the application of our Privacy and Security Risk Management Framework.

One of the highlights of 2018–2019 was the Privacy and Health Data Access Symposium hosted by CIHI in October. The symposium brought together attendees from across the country to share ideas about improving access to health data in a privacy-sensitive manner. We were very pleased with the attendance and the level of engagement of the attendees. The output from the symposium will feed into CIHI’s ongoing stakeholder consultations.

As always, we continued to monitor the legislative landscape both in Canada and internationally. Of particular interest in 2018 was the implementation of new European privacy legislation set against a backdrop of serious privacy scandals. We expect this bold new legislation, in the form of Europe’s General Data Privacy Regulation (GDPR), will have an impact in Canada both in terms of legislative change and in defining best practices.

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. CIHI has not made any submissions since CIHI’s Annual Privacy Report, 2017–2018 was published; however, the following are being closely monitored:

- The potential implementation of health privacy legislation in British Columbia and Nunavut; and
- Potential amendments to health privacy legislation in Newfoundland and Labrador, Nova Scotia, Saskatchewan and the Northwest Territories.

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, 2017–2018 was published, CIHI has ratified

- An amendment to the New Brunswick National Prescription Drug Utilization Information System (NPDUIS) DSA, establishing that New Brunswick will stop encrypting personal health numbers in drug data submitted to CIHI; and
- A DSA with Cancer Care Ontario for the disclosure of Ontario data on hip and knee patient-reported outcome measures (PROMs) to CIHI.

CIHI is currently in negotiation with the following data providers:

- New Brunswick, regarding the implementation of a new DSA between the parties;
- Winnipeg Regional Health Authority (WRHA), for a DSA to govern WRHA’s current disclosure of Canadian Organ Replacement Register (CORR) data to CIHI;
- Alberta, regarding how the jurisdictional DSA would facilitate the submission of renal PROMs data from the Northern Alberta Renal Program to CIHI;
- British Columbia, regarding the implementation of a new DSA between the parties; and
- Yukon, regarding how the DSA impacts the submission of private drug claim submission data to CIHI.
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).

With respect to data requestors, since CIHI’s Annual Privacy Report, 2017–2018 was published, CIHI ratified an amendment to the Better Outcomes Registry & Network (BORN) DSA to facilitate the disclosure of additional PHI to help BORN ascertain maternal mortality in Ontario.

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 2018–2019 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;
- Related Privacy Policy procedures — reviewed on an ongoing basis and updated as necessary;
- Privacy Impact Assessment Policy — minor editorial changes made;
- Privacy and Security Training Policy and related procedures — changes in progress;
- Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media — minor editorial changes made and references added;
- Privacy and Security Risk Management Policy, Framework and Methodology — changes in progress; and
- Privacy and Security Incident Management Protocol — communications function added.
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 learning about and discussing risk management, including lessons learned and success stories from the use of CIHI’s Privacy and Security Risk Management Methodology. 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 2018 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 mandatory privacy and security annual renewal training, and renew their confidentiality agreement, prior to January 31. This year, the training component was a refresher on some of the privacy and security obligations of the employee confidentiality agreement.

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; news media; and other media sources. Over the 2018–2019 year, we continued to see privacy breaches in the health sector, where snooping remained a frequently reported topic.
Section 5: Privacy impact assessments

CIHI has in place a Privacy Impact Assessment Policy as 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 every 5 years at a minimum 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 2018–2019, PIAs for the following are currently in progress or were completed:

- Health Human Resources Database and Nursing Database — awaiting approval;
- Clinical Administrative Database — renewal of 2012 PIA in progress;
- Canadian Patient Cost Database — awaiting approval;
- Trauma Registries — awaiting approval;
- Primary Health Care Voluntary Reporting System — update to addendum completed;
- Integrated interRAl Reporting System (IRRS) — new PIA in progress;
- National System for Incident Reporting (NSIR) — renewal of 2015 PIA completed;
- CIHI Portal — update of 2014 PIA in progress; and
- PROMs — new 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 Information and Privacy Commissioner of Ontario is required to review the information practices of organizations designated as prescribed entities under Ontario’s *Personal Health Information Protection Act, 2004*. CIHI first received prescribed entity status in 2005, and its status was subsequently renewed in 2008, 2011, 2014 and 2017. Work on the next submission is under way, in anticipation of a submission date in October 2019.

Section 7: Privacy breaches

There were no major privacy breaches, as defined by CIHI’s Privacy and Security Incident Management Protocol, in 2018–2019.

Section 8: Privacy and Health Data Access Symposium

In October 2018, CIHI hosted a symposium to bring together thought leaders from Canada and other countries to exchange opinions and ideas about improving access to health data in a privacy-sensitive manner. Attendees included representatives from federal, provincial and territorial governments and private-sector organizations, as well as health researchers, academics and privacy experts.

The overall sense was that it was time to move the access agenda forward — beyond academic reflection. There was appreciation that CIHI had taken the initiative to put this important issue back on the agenda and collective recognition that we should capitalize on the momentum offered by the symposium. Attendees acknowledged that broader access to data to improve health could be enabled as part of an initiative to develop a pan-Canadian data and information governance strategy, in which privacy would be a key component.
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 strategy that will see increased use of cloud computing and a cloud-first approach for all new information processing solutions.

Privacy and Legal Services and Information Security were involved in the development of this strategy from the earliest opportunity, ensuring that all decisions were 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

The activities described in this annual privacy report reflect the tremendous hard work of CIHI’s dedicated employees, as well as the ongoing commitment made by CIHI’s senior management to ensure that privacy and security are, and will remain, corporate priorities. As we close out a productive and successful 2018–2019, we look forward to celebrating CIHI’s 25th anniversary and to continuing to evolve our Privacy Program so that we can meet whatever new challenges and opportunities the new year brings.