# 2018 ANNUAL PRIVACY REPORT

**CCO Legal & Privacy Office**

**June 2019**

Ontario

# Contents

## Purpose of this Report

The purpose of the Annual Privacy Report is to provide a summary of the key activities of Cancer Care Ontario's (CCO's) Privacy Program in 2018 and the ways in which the program continued to support CCO in achieving its overall mandate. The report sets out the structure of CCO's Privacy Program, the services it provides, and certain controls it implements.

## Background

CCO is a provincial agency responsible for continually improving cancer and chronic kidney disease (**CKD**) services and it acts as the Ontario Government's advisor on cancer and renal systems. In addition, CCO manages an Access to Care Program which implements information management/information technology solutions in healthcare organizations across the Province.

In order to fulfill its mandate, CCO requires access to personal health information (**PHI**) and personal information (**PI**) from stakeholders across Ontario's health care system. CCO derives its authority to collect, use, and disclose this information from its designations under Ontario's *Personal Health Information Protection Act, 2004* (**PHIPA**), the *Freedom of Information and Protection of Privacy Act* (**FIPPA**) and the *Cancer Act.* The following list describes the various privacy legal authorities which CCO relies upon for its operations:

Prescribed Entity (**PE**)
Subsection 45(1) of PHIPA permits health information custodians (**HICs**) to disclose PHI without consent to a prescribed entity (**PE**) for the purpose of analysis or compiling statistical information with respect to the management, evaluation or monitoring of the allocation of resources to or planning for all or part of the health system, including the delivery of services.

CCO is designated as a 'prescribed entity' for the purposes of subsection 45(1) of the PHIPA, under subsection 18(1) of Ontario Regulation (**O. Reg.**) 329/04. Many of CCO's programs operate under its PE authority. In this capacity, CCO collects PHI from health care organizations that are directly involved in the care and treatment of patients and from government institutions and agencies, such as the Ministry of Health and Long Term Care (**MOHLTC**), for health system planning and management purposes.

Prescribed Person (**PP**)
CCO is also designated as a 'prescribed person' (**PP**) under subsection 39(1)(c) of PHIPA with respect to its role in compiling and maintaining screening information for colorectal, cervical and breast cancer in the Ontario Cancer Screening Registry (**OCSR**) under subsection 13(1) of O. Reg. 329/04. This designation grants CCO the authority to collect, use and disclose PHI for the purposes of facilitating or improving the provision of health care with respect to the OCSR.

Researcher
CCO operates a research program to develop new knowledge through epidemiological, intervention, health services, surveillance, and policy research, as well as knowledge synthesis and dissemination. CCO can use PHI it collected as a PE or a PP for the purposes of research, subject to restrictions and conditions set out in PHIPA.

Electronic Service Provider (**ESP**) and Health Information Network Provider (**HINP**)
CCO provides electronic information services to HICs to enable them to collect, use, modify, disclose, retain or dispose of PHI, and/or to exchange PHI with each other. In providing such services, CCO is acting as an ESP and/or HINP, pursuant to O. Reg. 329/04, s. 6 (1) and 6(2) of PHIPA. These roles strictly limit CCO's use of PHI to that which is required to support electronic services to HICs.

Institution
CCO is an 'institution' as defined in FIPPA and is subject to its provisions. FIPPA regulates the collection, use, disclosure and retention of PI and provides the public with a right of access to records in the custody or under the control of an institution.

## CCO's Privacy Program

CCO is committed to respecting personal privacy and safeguarding the PHI and PI that it has in its custody and control. To support this commitment, CCO has a robust Privacy Program which is designed to ensure a privacy culture at CCO and that CCO is acting in accordance with PHIPA and FIPPA.

CCO's privacy governance structure provides assurance that the management of the Privacy Program is aligned with CCO's objectives, and is consistent with legislative and regulatory requirements, as well as with privacy best practices. The Program resides within the Legal & Privacy Office (**LPO**), whose mission is to uphold public trust by providing valuable advice in compliance and risk management. The Program is led by the Chief Privacy Officer (**CPO**), who reports directly to CCO's President and Chief Executive Officer (**CEO**). The Privacy Office supports the CPO in managing the day-to-day operations of CCO's Privacy Program, including identifying and mitigating privacy risks; leading policy development initiatives; overseeing privacy training; and handling the privacy breach management program.

In partnership with CCO programs and business units, the Privacy Office provides advisory services that include supporting the implementation of pragmatic and creative solutions. These solutions enable programs and business units to meet objectives while minimizing residual risk to the organization. Because of the close partnership, privacy requirements are embedded in new projects, processes, and programs in ways that facilitate CCO's ability to fulfill its mandate while remaining in compliance with privacy legislation.

## Privacy Impact Assessments

A key function performed by the Privacy Office is the development of privacy risk assessments. This work can take the form of Privacy Impact Assessments (**PIAs**), which serve to assess a program or information system's privacy risks and recommend mitigating strategies. These assessments provide a level of assurance that privacy issues and risks are identified and addressed. In 2018, the following PIAs were completed:

- Gastrointestinal (**GI**) Endoscopy Minimum Data Set (**MDS**) Implementation for Data Submission Portal (**DSP**) Deployment
- Ontario Palliative Care Network (**OPCN**) Repository
- Hip and Knee Patient-Report Outcome Measure (**PROMs**) in Interactive Symptom Assessment and Collection Application (**ISAAC**)

- Quality Management Partnership – 2016/2017 Quality Reports
- Lung Cancer Screening Pilot for People at High Risk 2018/19 Activities
- Sandy Lake Screening Activity Report for Sioux Lookout Zone
- Wait Times Information System: Mental Health & Addiction Access to Care Expansion
- Ontario Laboratory Information System (**OLIS**) Phase 2B
- Gastrointestinal (**GI**) Endoscopy Minimum Dataset (**MDS**) Implementation for Data Submission Portal (**DSP**) Deployment: Fecal Immunochemical Test ("**FIT**") Kit Implementation, Phase 2
- Positron Emission Tomography (**PET**) Scans Insured Claims Data Collection

## Privacy Training and Awareness

CCO's privacy and security training is compulsory and critical to ensuring the protection of PHI and PI. The objective of the training program is to ensure that all agents[1] of CCO understand the purposes for which CCO can collect, use and disclose PHI and PI; their obligations to safeguard the information in CCO's custody; and their role in complying with CCO's policy, legislative and regulatory requirements. All agents fulfill the requirements of the privacy and security training program when first on-boarded at CCO and then subsequently on an annual basis.

In 2018, the Privacy Office also provided a number of specialized training and awareness activities for specialized teams and individuals. These training activities included:

- De-identification/Privacy Roadshow
- Privacy Training for CCO Directors
- CCO Contact Centre Privacy Training
- Patient Family Advisor Privacy Training
- Quarterly Cyber Security Law Update

CCO also conducted two tabletop incident management exercises involving fictitious privacy and security breaches. The purpose of these exercises was to familiarize key personnel with their roles and responsibilities during an incident or business disruption as well as provide an opportunity to review key procedures and policies to ensure effectiveness. The participants were from various teams across CCO including Communications, Legal, Privacy, Technology Services and Security. Through the tabletop exercises, CCO identified opportunities for improved alignment of processes, procedures and frameworks and work is underway to action those learnings.

## Complaints

Any individual may submit a complaint or concern to CCO relating to its privacy policies and procedures or to its compliance with legislative and regulatory requirements. The majority of complaints received by CCO from members of the public are resolved quickly once CCO's role and legislative authority pursuant to PHIPA, in addition to an introduction of CCO's Privacy Program, is described to them.

[1] The term agent(s) in this report means a person that, with the authorization of CCO, acts for or on behalf of CCO in respect of PHI/PI. This meaning is aligned the use of the term agent in the IPC's *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*. For clarity, agents include full- and part-time employees, service providers and other representatives such as consultants, students, and researchers.

Most complaints received by CCO are related to CCO's Cancer Screening programs. These programs involve direct contact with the public through various types of correspondence letters. The public facing nature of this program creates an increased awareness of CCO's collection, use, and disclosure of PHI for the purposes of facilitating access to the cancer screening programs. All individuals who have expressed concerns with CCO having access to their PHI through CCO's screening programs are given the opportunity to opt-out from receiving future screening correspondence. The complaints received by CCO in 2018 were investigated pursuant to CCO's Privacy Inquiry and Complaints Procedure[2].

## Breach Management

CCO has a robust breach management program that aims to ensure CCO staff are equipped to appropriately identify, manage, investigate and resolve privacy breaches that occur. CCO employees and third parties are trained on what constitutes a privacy breach though CCO's privacy and security training programs and they are made aware of their responsibility for reporting a breach or suspected breach. The LPO plays a leadership role in coordinating any breach investigation and response activity.

In 2018, CCO did not experience any high risk privacy breaches, as defined in CCO's Privacy Breach Management Procedure.

## Data Sharing Agreements

CCO regularly enters into data sharing agreements (**DSAs**)[3] with its data partners to identify the roles and responsibilities of the parties with respect to the collection, use and disclosure of PHI and PI. DSAs facilitate the sharing of information which is required to fulfill CCO's mandate.

CCO has standardized master data sharing agreements (**MDSAs**) with each of the regional cancer centres, as well as a number of hospitals and independent health facilities in Ontario. This allows for streamlined data sharing while ensuring that privacy requirements and best practices are embedded into these relationships. CCO will also enter into others types of data sharing agreements on an as needed basis. In 2018, the following key DSAs were entered into:

- New Drug Funding Program (**NDFP**) Data Sharing Agreement with Amgen & McKesson
- Amending Agreement No. 3 to the Data Sharing Agreement between Health Shared Services Ontario (**HSSO**) and Cancer Care Ontario with OACCAC (now HSSO)
- Information Sharing Agreement between College of Physicians and Surgeons of Ontario (**CPSO**) and Cancer Care Ontario
- Amending Agreement No. 16 to the CCO/MOHLTC Data Privacy Agreement for a Prescribed Entity with MOHLTC
- Agreement for CIHIs Collection of Ontario Patient-Reported Outcome Measures (**PROMs**) with Canadian Institute for Health Information (**CIHI**)
- Research Transfer Agreement (Developing Analytics Tools for Disease Pathway Concordance) with University of Toronto

[2] A complaint is considered closed once the complaint has been received, investigated, documented and responded to in accordance with CCO's Privacy Inquiry and Complaints Procedure.

[3] Data Sharing Agreement: means an agreement which outlines the terms and conditions for a Data Exchange, which may include the disclosure of one or more Data Sets by CCO to an External Party, or the collection of one or more Data Sets by CCO from an External Party

- Amending Agreement No. 15 to the CCO/MOHLTC Data Privacy Agreement for a Prescribed Entity with MOHLTC
- End-Use License Agreement for Postal Code Conversion File and Postal Code Conversion File Plus with Statistics Canada

## Privacy Audit

Privacy audits are a key component of CCO's overall Privacy Program. CCO's Privacy Audit and Compliance Standard ensures that CCO conducts audits and ongoing reviews of its privacy policies, procedures and practices. The Privacy Office is responsible for coordinating audits and reviews of CCO's information management practices involving PHI and PI, including operational practices, to assess compliance with the CCO Privacy Policy and associated standards and procedures. CCO Business Units, with guidance from the Privacy Office, also perform *ad hoc* privacy audits to ensure PHI and PI related to their program work is being collected, used and disclosed appropriately. Examples of audits completed in 2018 are as follows:

- CCO Wide PHI Access Audit (conducted quarterly): Review of all current active CCO user accounts with access to PHI to confirm whether access is still required.
- Surveillance Reporting Audit: Review of previously disclosed statistical tables and figures in biennial report to ensure small cell suppression rules had been appropriately applied.
- Data Disclosure Audit: Review of pathology data previously disclosed to external researchers to confirm no only PHI required for the Research Purpose was disclosed.
- SSL User Audit: Review of user permitted access to PHI on SSL to confirm access was still required.
- iPORT User Audit: Review of ATC and Cancer users in iPORT to confirm access to PHI was still required.
- iPORT Technical Audit: Review of iPORT functionality to test for situations where user may inadvertently be given access to PHI they were not authorized to view.
- eClaims Technical Audit: Review of eClaims functionality to ensure users cannot access more PHI then they are authorized to view.
- Path Lab Audit: Review of Path Lab access to ensure users have not been granted access to more PHI than required for their job duties.

## Policy Review

CCO is committed to the ongoing review of its privacy policies, procedures and practices. In accordance with privacy best practices, applicable legislation, and direction from the Information and Privacy Commissioner (**IPC**) of Ontario, CCO has an extensive suite of policies and procedures in place to ensure the protection of PHI and PI. The Privacy Office reviews CCO's privacy policies, procedures and guidelines regularly to ensure they continue to meet our obligations and commitments.

For example, in 2018, the Privacy Office created or updated policies, procedures and guidelines as outlined below:

- Data Use and Disclosure Policy
- Privacy Breach Management Procedure
- Privacy and Information Security Risk Management Procedure

- Research Policy
- Privacy and Security Training and Awareness Procedure
- De-identification Guidelines
- Statement of Information Practices

## Key Enterprise Data Management Initiatives

The Privacy Office works closely with stakeholders across CCO to implement effective information governance and safeguarding confidential information through Enterprise Data Management Initiatives. A sample of these initiatives that the Privacy Office supported in 2018 are described below.

### *Towards Actionable Insight*

Towards Actionable Insights (**TAI**), is a strategic plan designed to improve the way CCO manages data, conducts analysis, and uses information in decision-making. Through TAI, CCO is working to define, implement, and operationalize data quality and metadata related guidelines, processes, roles, responsibilities and associated technology to consistently manage this activity across CCO's data assets. For example, the data quality initiative has defined, implemented, and operationalized data quality-related guidelines and processes to support consistent management of data quality across CCO's data assets. This will foster trust in data, allowing users to be confident in the data's use and application in the creation of information. Further, as initiative focused on metadata management will provide visibility into CCO's data and information assets to generate efficiencies when locating and leveraging CCO's data assets.

### *De-identification Program*

In 2018 the LPO supported CCO's data de-identification program through the development of new guidelines for data de-identification and small cell suppression. Both guidelines are designed to standardize CCO's approach to de-identification and ensure a consistent approach to small cell suppression. As part of this Program, the Eclipse tool is used to measure the risk of re-identification inherent in certain data sets.

### *H: Drive Management Solution*

The H drive is CCO's secure drive for the management of data containing PHI/PI as well as an area for operational and quality assurance processes. In 2018, CCO established the H Drive Management Solution Project that looks to build on CCO's existing audit and logging processes by procuring an IT solution. This solution will automate and streamline current manual audit and reporting activities and will bring improved operational efficiencies to CCO. This technical solution will enhance CCO's capabilities in monitoring and controlling the storage and retention of PHI/PI within CCO, ensuring continued compliance with CCO's regulatory requirements.