2017 ANNUAL PRIVACY REPORT

CCO Legal & Privacy Office
June 2018

Ontario
Cancer Care Ontario

Table of Contents

1. Purpose of this Report

The purpose of the Annual Privacy Report is to describe Cancer Care Ontario's (**CCO**'s) Privacy Program and the ways in which the program supports CCO in achieving its overall mandate.

The report sets out the governance structure of CCO's Privacy Program, the services it provides, and the controls it implements with our data partners. The report also provides key metrics on privacy-related activities and summarizes the support provided in 2017 to numerous key CCO initiatives (please see Appendix A).

2. CCO's Privacy Program: Who are we?

CCO is committed to respecting personal privacy and safeguarding the personal health information (**PHI**) and personal information (**PI**) that it has in its custody and control. These commitments are actioned, in part, through the activities of CCO's Privacy Program. The Program is designed to ensure CCO is acting in accordance with its obligations under the *Personal Health Information Protection Act, 2004* (**PHIPA**) and the *Freedom of Information and Protection of Privacy Act* (**FIPPA**); building a culture of privacy across the organization; and working in partnership with CCO programs and business units to support them in achieving their goals and objectives.

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 empower CCO and 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. The Privacy Group 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 the privacy training program; and managing a comprehensive privacy breach management program. CCO's Board of Directors also receives regular updates on both cybersecurity and privacy, and the resources allocated to these areas.

3. CCO's Privacy Program: What do we do?

CCO is committed to respecting personal privacy, safeguarding confidential information, and ensuring the security of the PHI and PI that it maintains. CCO meets these commitments through its Privacy Program's key objectives, services and processes, which are described below.

3.1 Privacy Advisory Services

In partnership with CCO programs and business units, the Privacy Group provides advisory services that include designing and supporting the implementation of pragmatic, creative, and relevant solutions; these solutions enable programs and business units to meet their objectives and minimize residual risk to the organization. The Privacy Group is in the unique and privileged position of being an integral part of initiatives from conception to implementation. As a result of this 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.

3.2 Overview of Administrative, Physical and Technical Controls

CCO implements strong administrative, physical, and technical controls to protect PHI and PI against loss or theft, as well as against unauthorized collection, access, use, or disclosure. The Privacy Group works collaboratively with partners across the organization, including Technology Services, Analytics and Informatics, and Facilities, to implement these controls. Some of these controls include:

Administrative safeguards

- A **training** program that requires all employees to acknowledge their understanding of CCO's Privacy Policy and Information Security Code of Conduct.
- Data access **policies** and procedures to protect PHI and PI.
- **Privacy assessments** and risk mitigation plans to identify and mitigate privacy risks for existing and new programs or initiatives.
- **Privacy requirements** embedded in project plans, business requirements documents, communication materials, Requests for Proposals, service provider contracts, and in other project specific contexts.
- Robust **data sharing agreements** between CCO and our partner organizations.
- A **breach management program** to ensure privacy breaches are identified, contained, and resolved with improved controls in place.

Technical Safeguards

- The transfer of sensitive information between Partners and CCO is done over **secure channels** (i.e. authenticated and encrypted).
- Strong passwords and other **authentication solutions** are required for access to sensitive systems.
- Administrative **access** to all IT equipment and applications are controlled via proper authorization and authentication.
- Network traffic is monitored and managed using **security mechanisms** such as firewalls, intrusion detection/prevention systems, and anti-virus programs.
- All data stored on staff computers is **encrypted**. If laptops are lost or stolen, data confidentiality and integrity are not at risk.

Physical Safeguards

- CCO data centres have appropriate **environmental controls** and are physically secured against unauthorized access. They are staffed and monitored continuously by trained security personnel.
- **Access to office areas** is controlled with access badges, and traffic in the office areas is recorded by security cameras.
  Visitors and third-party vendors to Cancer Care Ontario require visitor badges and are escorted by full time staff members.
- Specific physical security zones are implemented to separate and control access to public zone, delivery and loading area, office space, and computer rooms, with increasing **physical security controls**.

3.3 Privacy Assessments and Risk Mitigation Plans

A key function performed by the Privacy Group is the development of privacy assessments. This work can take the form of Privacy Impact Assessments (**PIAs**) and risk mitigation plans. These tools serve to assess a program or information system's privacy risks and recommend mitigating strategies. They provide a level of assurance that privacy issues and risks are identified and resolved. They can also promote an understanding of how CCO handles PHI or PI and demonstrate the ways in which CCO meets its legislative and regulatory obligations and commitment to the general public.

3.4 Privacy and Security Training

CCO's compulsory privacy and security training is 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

[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.

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 complete a refresher on an annual basis.

3.5 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 for them.

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 tends to promote 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.

All complaints received by CCO in 2017 were investigated and closed as per CCO's Privacy Inquiry and Complaints Procedure.[2]

3.6 Privacy Breach Management

A privacy breach constitutes an unauthorized collection, use or disclosure of PHI or PI. An example of a breach is when a CCO employee accesses PHI where it is not required for the purposes of their job duties. All breaches are investigated by the Privacy Group in collaboration with the relevant business units, with mitigating strategies and recommendations identified and implemented in order to prevent future breaches from occurring. In 2017, the Privacy Group further refined its approach to privacy breach management by implementing additional escalation and monitoring activities. In addition to completing a detailed privacy breach report, the Privacy Group now implements streamlined reporting of all suspected and confirmed privacy breaches via email to the Group Manager, Privacy immediately upon discovery. If the risk level associated with the breach exceeds the threshold of low[3], breaches are then escalated to the Director immediately. All breaches are monitored by the Director on a weekly basis.

The Privacy Group also added the new category of "passive breach" to its Privacy Breach Management Manual in 2017. A passive breach is an instance where (1) PI/PHI is received by CCO in error and that CCO does not require; or (2) PI/PHI is transmitted to CCO in an unauthorized manner (for example, by email). Metrics are included in section 4 below.

3.7 Data Sharing Agreements

CCO enters into data sharing agreements (**DSA**) with its data partners so as to identify the roles and responsibilities of the parties as it pertains to the collection, use and disclosure of PHI and PI. DSAs facilitate the sharing of accurate and timely information required to fulfill CCO's mandate.

CCO has entered into standardized master data sharing agreements (**MDSA**) with each of the regional cancer centres and many other hospitals and independent health facilities in Ontario. This process has streamlined the data sharing process while ensuring that CCO's privacy best practices are embedded

---

[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] As set out in CCO's Privacy and Information Security Risk Management Procedure which aligns with CCO's Enterprise Risk Management Framework.

[3] As set out in CCO's Privacy and Information Security Risk Management Procedure which aligns with CCO's Enterprise Risk Management Framework.

into these relationships. The MDSA has eliminated the need to negotiate new DSAs with these facilities every time CCO launches a new program or project. Instead, a shorter document is completed, which forms part of the MDSA, and sets out the specific details of the project at issue.

3.8 IPC Triennial Review

As a PE and a PP, CCO must have its information management practices reviewed and approved by the IPC every three years. In October 2017, CCO received approval to continue to collect, use, and disclose PHI without the consent of the individual. This approval is effective until October 2020.

The Privacy Group has been very active this year in working to secure the new three year approval granted by the IPC. A draft of the Report is submitted to the IPC a year in advance to allow CCO and the IPC to work together on any questions or issues of concern. While CCO submitted its initial draft 2017 Triennial Review Report (the **Report**) to the IPC in 2016, covering the reporting period of November 1, 2013 to October 31, 2016, significant changes were made to the report over the course of 2017 based on feedback and questions from the IPC.

The Report included a sworn affidavit from CCO's Chief Executive Officer and President confirming that CCO has privacy procedures and practices in place that are compliant with PHIPA, its regulations, and the IPC's *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the Manual"); and that CCO has taken steps that are reasonable to protect PHI from unauthorized collection, use, and disclosure. If the IPC is satisfied with the information provided by CCO, it will issue an approval to continue operating as a PE and PP, along with any recommendations it considers appropriate.

In the 2017 approval letter from the IPC, CCO received seven recommendations to further enhance its privacy practices and procedures. These recommendations were as follows:

- implementing a policy to distinguish between uses and disclosure of PHI for research purposes;
- obtaining written confirmation from recipients of aggregate data that they will not attempt to re-identify individuals;
- ensuring information related to Privacy on CCO's public facing website is up to date;
- reviewing CCO's list of PHI data holdings to ensure appropriate legal authorities are identified;
- ensuring that all privacy and security policies and procedures are reviewed at least once prior to each Triennial Review period;
- ensuring privacy complaint indicators are provided in full compliance with the requirements of the Manual; and
- ensuring that linked records of PHI are de-identified as soon as practicable and that, to the extent possible, only de-identified data is used by CCO for PE purposes.

The Privacy Group works closely with other CCO business units in operationalizing its regulatory requirements and in implementing the above recommendations. Some of the above recommendations have already been completed and the rest are in process. We have an ongoing dialogue with the IPC regarding these initiatives.

Through this approval, CCO can continue with its mission to improve the performance of Ontario's health systems by driving quality, accountability, innovation and value through the collection of PHI.

3.9 Privacy Policy Review

CCO is required by PHIPA and the IPC to have an extensive suite of policies and procedures ensuring the protection of PHI. The Privacy Group is committed to reviewing CCO's privacy policies, procedures and guidelines regularly to ensure they continue to be compliant with regulatory requirements, and with privacy legislation and best practices.

In 2017, the Privacy Group identified potential updates to its suite of privacy policies and procedures to enhance alignment with the requirements of the IPC as identified through the IPC Triennial Review and the operations of the Privacy Program overall. These updates will be implemented throughout 2018. Updates to CCO's existing Privacy Policy and Data Use and Disclosure Policy were drafted in 2017 to better reflect current practice, with final approval granted in early 2018.

CCO also finalized updated De-identification Guidelines in 2017 to better assist CCO employees with de-identifying data sets containing PHI and measuring the risk of re-identification of an individual contained in a CCO data set. The guidelines apply to both disclosures of CCO data to external parties and internal uses of CCO data by employees and they incorporate the use of CCO's de-identification tool, Eclipse. Updates on CCO's De-identification Project are set out in section 5 below.

3.10 FIPPA Privacy Program

CCO was designated as an Institution under FIPPA in 2010. This legislation has the following two components:

1. The right of individuals to access information under the control of institutions; and
2. The protection of the privacy of individuals' PI held by institutions.

Since 2010, CCO has implemented processes related to Freedom of Information (**FOI**) requests and has launched new programs that operate under FIPPA, such as Person-Centred Care. CCO's maturity as an Institution has continued to grow with the development of innovative programs and projects that include the collection, use and disclosure of PI.

CCO has a robust privacy program governing its collection, use, and disclosure of PHI and continues to enhance its FIPPA Privacy Program to protect the privacy of individuals whose PI is managed by CCO. The FIPPA Privacy Program formalizes requirements for the collection, use, and disclosure of PI that are consistent with or similar to its requirements for PHI. In 2017 the Privacy Group continued to implement the FIPPA Privacy Policy finalized in 2016 to ensure the consistent management of PI and protection of individuals' privacy.

4. Privacy by Numbers: Key Metrics[4]

The following key privacy metrics highlight some of the work accomplished by the Privacy Group in 2017 and provides an indication of CCO's compliance with legislative and regulatory requirements as well as with its privacy policies and procedures.

Privacy Assessments	2017
PIAs and risk mitigation plans completed on CCO initiatives	14

Data Sharing Agreements	2017
DSAs and/or DSA amendments executed for CCO	14

Policy Development and Review	2017
Existing policies audited for compliance and updated	13
New policies developed	1
Privacy Breaches	2017
Correspondence Privacy Breaches	
A "Correspondence Breach" results when a Cancer Screening program correspondence letter is opened by an unintended individual (i.e. by an individual to whom the information in the letter does not belong).	
Correspondence letters sent out by CCO for the three Cancer Screening Programs.	8,957,145
Letters identified as resulting in privacy breach (i.e. a letter that was opened by an unintended individual).	673
Correspondence Privacy Breach Rate (i.e. the percent of correspondence that resulted in a privacy breach).	0.008%
Program (Non-correspondence) Privacy Breaches by Type	
Unauthorized Collection - Passive Breach[5] (e.g. a hospital sent an email/fax with PHI to CCO in error).	14
Unauthorized Use (e.g. an internal CCO report contained PHI in error).	2
Unauthorized Disclosure (e.g. a hospital viewed a report with PHI from another hospital because an error access controls).	8
Total	**24**[6]

Policy Breaches[5]	2017
Authorized Collection - Passive Policy Breach[6] (e.g. CCO received PHI through a transfer method other than that method which had been approved).	105
Internal Policy Breach (e.g. PHI sent internally by email to authorized recipients when PHI should have be viewed on secure H: drive).	6
Total	**111**

Privacy Complaints by Program/Subject	2017
Ontario Cervical Screening Program	6
Ontario Breast Screening Program	3
Colon Cancer Check	3
General Screening Complaints	11
Total	**23**

5. Key Initiatives

Through the successful development and implementation of various new initiatives and programs, as well as enhancements to existing programs, CCO continued to fulfill its mandate in 2017. A sample of the initiatives that the Privacy Group supported in 2017 are listed in Appendix "A". In addition, set out below are details of certain key initiatives in which the Privacy Group played a significant role.

5.1 De-identification Project and Program

In 2015, CCO procured a data de-identification tool to strengthen its data governance and risk management capabilities. The tool supports both *ad hoc* de-identification of datasets in the first phase of implementation, and automated de-identification of datasets in the second phase. The tool's risk measurement capabilities assist CCO staff with the measurement of risk of re-identification for each data set before it is released to external or internal recipients. Throughout 2017, the LPO continued to support the De-identification Project as a co-sponsor with the Analytics and Informatics team. CCO also continued to work closely with the vendor of the tool to ensure that CCO can objectively assess the risk of re-identification of an individual on a consistent basis, and implement appropriate de-identification methodologies.

The LPO and Analytics and Informatics teams have now transitioned from a pilot project to a De-identification Program. One early success of the Program has been the successful measurement of re-identification risk and the application of de-identification methodologies to multiple data sets required for prescribed entity purposes.

Going forward, CCO will continue to leverage the de-identification tool to the extent possible to produce high quality, de-identified data sets that suit a variety of business purposes including external data disclosures (e.g. for research requests), internal data analysis, report production and quality assurance testing. As CCO's internal data access requirements and reporting needs continue to evolve, CCO will continue to mature its de-identification capabilities and capacity.

5.2 High Risk Lung Cancer Screening Pilot

CCO is working with three Ontario hospitals (Health Sciences North, Lakeridge Health, and The Ottawa Hospital) to launch organized high risk lung cancer screening using low-dose computed tomography to improve lung cancer survival through early detection while minimizing the potential harms of screening. The goal is to use the findings from the Pilot to inform the design and implementation of a provincial program that addresses the needs of patients in the screening phase and also enables integrated care across the cancer journey. This aligns with the Ontario Cancer Plan IV priority to ensure the delivery of integrated care across the cancer care continuum.

CCO is collecting data from the three pilot hospitals for the purpose of evaluating the pilot, providing recommendations to the Ministry of Health and Long-Term Care (MOHLTC) on a province-wide program, and to work with the pilot hospitals to improve the performance and quality of the screening services they provide.

The data to be collected, used and disclosed by CCO as part of this Pilot includes patient demographic and clinical information, which constitutes PHI as defined under s. 4 of the PHIPA.

A Privacy Impact Assessment was conducted in March 2017 to identify privacy risks related to the High Risk Lung Cancer Screening Pilot and recommend controls to mitigate those risks. The assessment consisted of analyzing the collection, use, and disclosure of PHI by CCO to ensure activities are in compliance with PHIPA, CCO's contractual obligations and CCO's privacy policies and procedures. The PIA concluded that CCO has the legislative authority as a prescribed entity under s. 18(1) of Ontario Regulation (O. Reg.) 329/04 of PHIPA to collect, use and disclose PHI pursuant to s. 45 of the PHIPA for the purposes of this Pilot.

5.3 Abnormal Follow-Up Adherence and Barriers (ABFAB) Pilot

The ColonCancerCheck (CCC) screening program operates under CCO's prescribed person (PP) designation pursuant to s.39 (1) (c) of the PHIPA. The ABFAB pilot operates as an extension of this program under CCO's PP legislative authority.

Over the past year, the Privacy Group supported the first phase of the ABFAB initiative and began laying the foundation for the next phase. The overarching goal of ABFAB is to improve colonoscopy follow up in patients with abnormal guaiac fecal occult blood test (gFOBT) by piloting four different patient navigation strategies. CCO will use the ABFAB pilot results for the second phase, the ABFAB research study.

For the purpose of the pilot, PHI was:

- used to identify the eligible patients for the pilot and the study;
- disclosed to physicians;
- disclosed to Diagnostic Assessment Programs (DAPs);
- collected from cancer screening patients and their physicians to evaluate their experience with the pilot;
- used to facilitate follow-up after an abnormal FOBT result; and
- used to analyze and report findings.

Throughout 2017, the Privacy Group supported the ABFAB project in the following ways:

- Prepared a PHIPA authorities analysis
- Prepared a privacy risk mitigation plan
- Reviewed the REB protocol
- Reviewed the project analytics plan

Personal health information from the ABFAB pilot results will be used by CCO for research purposes pursuant to s. 13(4) of O. Reg 329/04 and s. 37(1) (j) of the PHIPA in the second phase of the project to meet the research objectives outlined in the ABFAB Study Protocol.

5.4 TAI Support

The Towards Actionable insights (TAI) Program is the action plan to realize CCO's Data & Analytics Strategy. In 2017, the Privacy Group supported Phase 2 of the Program which involves several key initiatives around the required people, processes, data and technology required to transform the current state to the desired future state as detailed in the Data & Analytics Strategy. Support included attendance at and contributions to various TAI working groups and sponsors meetings to ensure privacy requirements were considered in the evolution of the Program.

The Privacy Group also supported the metadata management, data quality and strategic sourcing TAI initiatives in 2017. This included providing input and privacy requirements into project documentation, identifying potential privacy risks and mitigating strategies. In 2018, Privacy will support the continued evolution of the TAI Program and, as part of this work, will develop a privacy impact assessment for the data lake component of the project.

5.5 Trillium Gift of Life Network ("TGLN")

The ORN and Trillium Gift of Life Network (TGLN) have established a 5-year joint governance structure to enhance access and improve patients' experience with kidney transplantation, with a focus on living kidney ~~[~~donations~~]~~ (**TGLN-ORN Collaboration**). The TGLN-ORN Collaboration aims to ensure there is an integrated, person-centred, collaborative kidney care continuum in Ontario and to bridge the gap between deceased and living donations. Specifically, the objective of this collaboration is to enhance access and improve patients' experiences with kidney transplantation, with a focus on living kidney donation.

As part of this initiative, 13 Regional Renal Programs currently receive aggregate and patient-level transplant referral and wait list records from CCO (the remaining Regional Renal Programs are expected to start receiving this data by Fall 2019). These records are derived from TGLN Data held by CCO.

CCO and TGLN have not historically shared data. To ensure that this data exchange was authorized by law and conducted in a manner that respects the privacy rights of individuals, in 2017 the Privacy Group completed a complex and comprehensive privacy impact assessment and negotiated a DSA with TGLN.

Appendix A: Select Initiatives Supported in 2017

(This list does not include daily operational program support or the ongoing support provided to the data acquisition team or various data governance committees, such as the Data Disclosure Sub-committee.)

PORTFOLIO	INITIATIVE 2017
Access to Care	- eCTAS - Wait Times – Mental Health Services - SETP – Interim Reporting Solution
Prevention and Cancer Control	- High Risk Lung Cancer Pilot - Gastrointestinal Endoscopy Data Submission Portal Project - Fecal Immunochemical Test Kit Implementation - Ontario Breast Screening Program (OBSP) – Radiology Outcome Reports Privacy Review - ABFAB - Occupational Cancer Research Centre – WSIB - Breast Screening Facebook Campaign
Quality Management Partnership (**QMP**)	- MOHLTC Data Acquisition - QMP Report Design - QMP Evaluation Survey - Pathology DSAs with data partners
Clinical Programs and Quality Initiatives	- PET Out of Province– Agreement - Acute Leukemia Manual Data Collection - Stem Cell Transplant Manual Data Collection - CHM PREM - Kyphoplasty and Vertebroplasty Manual Data Collection - ISAAC Hip and Knee - ISAAC EMR expansion - Advisor Connect Regional Roll-out - Avastin Study
Ontario Renal Network (**ORN**)	- Ontario Renal Reporting System Release 7 - Ontario Renal Network Website Redesign - OLIS Data Acquisition - ORN-ICES Kidney Dialysis and Transplantation - ORN Symptom Management - ORN Integrated Dialysis Care - ORN Glomerulonephritis Specialty Clinics - Goals of Care data - Kidney Talks Conference
Planning and Regional Programs	- Funding Agreement reviews
Ontario Palliative Care Network (OPCN)	- OPCN Repository Privacy Impact Assessment # 1 - Advisory Council Confidentiality Agreements
Chief Technology Office	- ISAAC Integration Projects - ITSM ticketing System - CCN Transition Agreement
People, Strategy & Communications	- CCO Websites Re-design - eCCO Re-design - Human Capital Management System Implementation (Phase 2) - Employee Engagement Survey
Analytics and Informatics	- Data De-identification Project and transition to a program - Data Destruction Process - Internal Data Access Policy and Procedures - Strategic Sourcing (Towards Actionable Insights – **TAI**) - Data Quality and Enterprise Metadata Management (TAI)
Aboriginal Cancer Control Unit (**ACCU**)	- Kenora Chiefs Advisory Screening Activity Report - Sioux Lookout Zone SAR transition to eReports - Cancer Care Ontario – Chiefs of Ontario – Institute for Clinical Evaluative Sciences Partnership