DATA USE & DISCLOSURE POLICY

Approval:	Executive Team	Date Approved:	February 1, 2018
Sponsor:	General Counsel, Chief Privacy Officer & Corporate Secretary	Effective Date:	February 1, 2018
		Last Revised:	January 12, 2018
		Next Review Date:	December, 2020

- References: Ontario's *Personal Health Information Protection Act*, *2004*;
- *Cancer Act* (Ontario);
- Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario ("**CCO's Privacy Policy**");
- Privacy Audit and Compliance Procedure;
- De-Identification Guidelines;
- Business Process for Data Requests;
- Decision Criteria for Data Requests;
- Internal Data Access Procedure;
- Privacy Breach Management Procedure;
- Privacy Training and Awareness Procedure;
- Data Steward Terms of Reference;
- Data Disclosure Subcommittee Terms of Reference;
- Research Data Request Application;
- General Data Request Form; and
- Research Privacy Policy.

Policy

1 PURPOSE

The purpose of this Data Use & Disclosure Policy ("**Policy**") is to ensure that the use and disclosure of CCO data complies with Ontario's *Personal Health Information Protection Act,*

*2004 ("**PHIPA**"), supports CCO's mandate, is managed consistently, and is carried out in compliance with CCO's privacy obligations.*

2 SCOPE

This Policy applies to CCO in its capacity as a Section 45 Prescribed Entity under *PHIPA* and encompasses (a) the *use* of CCO data by data users for planning and management purposes (CCO employees and Third-Parties[1]), (b) the disclosure of CCO data to external requestors for purposes other than research, and (c) the disclosure of CCO data for the purposes of research to external requestors.

This Policy also applies to CCO in its capacity as a Prescribed Registry under clause 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 for the purposes of facilitating or improving the provision of health care with respect to colorectal, cervical and breast cancer.

Any use or disclosure of CCO data must comply with the Principles set forth in this Policy. Requests for exceptions to this Policy must be submitted in writing to the Legal & Privacy Office and must include the reason why the CCO data is being requested and its intended use, and include a justification for why the exception is necessary.

All access to CCO data that contains Personal Health Information ("**PHI**") must comply with applicable privacy laws, including *PHIPA*, and CCO's Privacy Policy. In all cases, applicable privacy laws take precedence over this Policy.

3 DEFINITIONS

Terms not defined within the body of this Policy are set out in Appendix A of Cancer Care Ontario's Privacy Policy.

4 POLICY

4.1 For the purpose of this Policy, CCO data is classified according to the following schema:

- **Identifiable Record-Level Data**: data that includes elements that directly identify an individual. By definition, identifiable record-level data contains PHI;
- **De-identified Record-Level Data**: data that includes elements that may constitute identifying information because there may be reasonably foreseeable circumstances in

---

[1] Third-Parties are defined as consultants, contractors and Third-Party service providers engaged by CCO.

which the data could be utilized, alone or with other information, to identify an individual. (e.g., if linked with publicly available data.);

- **Aggregate Data**: summed and/or categorized data that is analyzed and placed in a format that precludes further analysis (for example, in tables or graphs) to prevent the chance of revealing an individual's identity (individual records cannot be reconstructed). Aggregate data does not include personal health information (PHI);[2] and
- **Published Data**: data that is made available to the public. Published data will not include PHI.

4.2 General Principles for Use & Disclosure of CCO Data

- **Use**:
  - CCO is a Prescribed Entity under Section 45 of *PHIPA*. In this capacity, CCO may use PHI in its custody for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to, or planning for all or part of the health system, including the delivery of services("health care system planning and management purposes").
  - CCO is also a Prescribed Registry under clause 39(1)(c) of *PHIPA* and in this capacity may use PHI that it collects under this authority for the purposes of facilitating or improving the provision of health care with respect to colorectal, cervical and breast cancer.
  - 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. As a Prescribed Entity or a Prescribed Registry, CCO can collect, use or disclose PHI as if it were a Health Information Custodian under Section 3 of *PHIPA* for the purposes of research. CCO's Research Privacy Policy sets out the framework governing the collection and use of PHI at CCO for research purposes.
- **Disclosure**:
  - In its capacity as a Prescribed Entity under Section 45 of *PHIPA*, and as a Prescribed Registry under s. 39(1)(c) of *PHIPA*, CCO may only disclose PHI in its custody as required or permitted by law. CCO will only disclose PHI when other information cannot serve the purpose and will only disclose as much PHI as is necessary to serve the purpose. The permitted disclosures when necessary are as follows:
    - ➢ <u>As a Prescribed Entity</u>:

---

[2] See the CCO Data Use & Disclosure Policy

- To other Section 45 Prescribed Entities;
- To Section 39 Prescribed Registries;
- To Section 47 health data institutes;
- For research purposes under Section 44;
- To an Ontario or federal government institution where permitted or required by law; or,
- Back to the Health Information Custodian ("**HIC**") that provided it to CCO, directly or indirectly, if it does not contain any additional identifying information.

➢ <u>As a Prescribed Registry</u>:

- A participant's primary care provider (i.e. HIC as defined under section 3 of *PHIPA*, 2004) so that he / she is aware of the participant's screening information and results;
- A primary care provider (i.e. HIC) who provides a participant with follow-up care if the participant receives a positive screening result and he/ she does not already have a primary care provider;
- A Regional Cancer Centre (i.e. HIC) that refers a participant for further screening or care where the participant cannot be connected to a primary care provider in a timely manner;
- A Prescribed Entity (e.g. CCO) for the management, evaluation, monitoring, or planning of all or part of the health system, including CCO in its capacity as a prescribed entity;[3]
- Researchers for research studies;[4] and
- A health data institute for analysis of the health system.[5]

4.3 Use of CCO Data by Data Users

- This section of the Policy applies to requests by data users for access to:
  - Identifiable record-level data

---

[3] *Ontario Regulation 329/04*. Section 13(5).

[4] *Personal Health Information Protection Act, 2004.* Section 44(1)–(6). *Ontario Regulation 329/04*. Section 13(5).

[5] *Ontario Regulation 329/04*. Section 13(5). No Health Data Institutes have currently been designated.

- De-identified record-level data

- Data users include CCO Staff and Third-Parties who require access to CCO record-level data (de-identified and identifiable) for health care system planning and management purposes or for improving the provision of healthcare, as applicable.
- Data users are granted access to CCO data holdings containing identifiable record-level data on a "need to know" basis to perform their assigned duties, and where access to de-identified and/or aggregate data will not serve the identified purposes.
- Data users are granted access to only as much identifiable record-level data as is reasonably necessary to meet the identified purpose.
- CCO expressly forbids the use of de-identified record-level data, either alone or with other information, including cell-sizes (n) of less than or equal to 5 (n<=5), where it may be used to identify an individual.
- CCO expressly forbids the use of de-identified record-level data, either alone or with other information, including prior knowledge of an individual, to identify an individual.
- CCO expressly forbids users from attempting to decrypt information provided in an encrypted form.
- Data users granted access privileges to CCO record-level data are responsible for their actions while carrying out these privileges.
- Requests by data users for access to CCO data are approved by the Data Steward for the data holding.[6]

4.4 Access to Record-Level Data

- Prior to being granted access to CCO record-level data, all CCO Staff and Third-Parties must:
  - Complete and sign a request for direct data access, identifying the data holding to which they require access, the purpose for access, and the type of access required. This request is approved by the user's supervisor, the Data Steward for the data-holding, and the Senior Manager, Data Management. See CCO's Internal Data Access Procedure;
  - Complete Privacy and Security Orientation training, and annual Privacy and Security Refresher training thereafter; and

[6] See CCO's Internal Data Access Procedure.

- Sign a Privacy and Security Acknowledgment form verifying completion of Orientation and/or Refresher training, and confirming understanding of the privacy principles discussed in the training.

4.5 Third-Party Service Provider Access to Record-Level Data

- In addition to the requirements set out above in Section 4.4, Third-Parties (contractors, consultants and Third-Party service providers) that access CCO record-level data or otherwise provide services to enable CCO to collect, use (retain, transfer, modify or dispose of) or disclose record-level data, enter into a written agreement with CCO ("Template Agreement for Third-Party Service Providers"), which sets out the privacy and security obligations of the Third-Party, prior to being granted access to, or receiving, Identifiable record-level data, or De-identified record level data that constitutes PHI. All Third-Parties must comply with the terms of the executed Template Agreement for Third-Party Service Providers entered into between CCO and the Third-Party. The Business Unit works with Legal to execute the required Template Agreement for Third-Party Service Providers prior to the commencement of the engagement.

- Pursuant to the Procurement Policy, the Business Unit is responsible for Third-Party Service Provider contract management, including ensuring that records of PHI provided to a Third-Party are securely returned and disposed of in accordance with the written agreement with that Third-Party Service Provider. The Director of Procurement is responsible for maintaining a log of agreements with all Third-Parties identifying those who have access to PHI. CCO's Director of Procurement is responsible for enforcing the Procurement Policy.

- If the Third-Party Service Provider fails to securely return the PHI or provide a certificate of destruction as the case may be within the relevant time frame set out in the written agreement, the Business Unit must notify the Third-Party signatory that the PHI has not been returned or destroyed in accordance with the terms of the written agreement. The Business Unit must copy the LPO on this notice sent to this Third-Party. The Business Unit should give the Third-Party a reasonable amount of time to meet the terms of the written agreement with respect to the return or destruction of the PHI, but such time shall not exceed 30 calendar days. If, after 30 calendar days, the Third-Party has not returned or destroyed the PHI in accordance with the written agreement, the Business Unit must e-mail the LPO to notify them of the breach of the Third-Party Service Provider written agreement. The Business Unit must include in the e-mail the relevant provisions of the written agreement, including the specific terms breached, as well as any communications sent to, or received from, the Third-Party Service Provider.

4.6 Breach of Policy

- Violations of this Policy by data users will result in the loss of data access privileges, as well as the imposition of contractually defined penalties, up to and including termination or legal remedies. See CCO's Privacy Breach Management Procedure.

- CCO staff must notify the LPO at the first reasonable opportunity, in accordance with the Privacy Breach Management Policy, if any agent breaches or if the CCO staff member believes there may have been a breach of this policy or its procedures.
- CCO Business Units are responsible for ensuring that Third-Parties employed within their Business Unit are familiar with and adhere to this Policy.

4.7 Disclosure of CCO Record-Level or De-Identified Data to External Requestors For Purposes Other Than Research

- This Policy applies to requests by external requestors for access to CCO data for purposes other than research.
- For procedures, please refer to Business Process for Data Requests, which addresses requests for record-level data (identifiable or de-identified) for non-research purposes. In responding to requests from external requestors:
  - CCO's goal is to make timely and accurate data available to external requestors throughout the health sector for approved purposes;
  - Where personal health information is being disclosed, CCO must be satisfied that the disclosure is permitted by PHIPA and its regulation and that any and all conditions or restrictions set out in PHIPA and its regulation have been satisfied. For details please consult CCO's Business Process for Data Requests and CCO's Data Disclosure Subcommittee: Terms of Reference & Decision Criteria for CCO Data Requests.
  - CCO must be satisfied that other information, such as De-identified Data (if identifiable information is requested) and Aggregate Data (if de-identified record-level information is requested) will not serve the identified purpose of the disclosure, and that no more PHI is being requested than is reasonably necessary to meet the identified purpose;
  - Except for approved research studies (see below), CCO will not provide Aggregate Data with cell sizes (n) less than or equal to five (n<=5) where there is a reasonable risk of identifying an individual, and reviews other Aggregate Data for residual risk of identification. See CCO's De-Identification Guidelines; and
  - CCO charges external requestors for its time in preparing and delivering CCO data in response to approved requests in accordance with the published Tariff of Costs.

4.8 Disclosure Of CCO Record-Level (Identifiable Or De-Identified) Data For Research Purposes

- CCO is committed to supporting cancer research and the research needs of the health sector, and encourages the use of its data for *bona fide* research.
- In responding to requests for CCO data for research purposes, CCO considers whether:

- The request is consistent with CCO's mandate under the *Cancer Act* and *PHIPA*;
- The research protocol, where applicable, is peer reviewed or otherwise demonstrates reasonable scientific merit; and
- It is feasible for CCO to provide the data requested under current operating conditions.

- Researchers requesting access to CCO Record-Level or De-Identified Data, submit to CCO:
  - A written application (i.e., a Research Data Request Application);
  - A written research plan; and
  - A copy of the decision of the research ethics board approving the written research plan and that the written research plan complies with the requirements in PHIPA and its regulation.
- Prior to the disclosure of PHI for research purposes, the researchers to whom PHI will be disclosed, CCO's Chief Privacy Officer, and CCO's Vice President, Analytics & Informatics must execute a Research Data Disclosure Agreement, in accordance with the Business Process for Data Requests.
- Researchers granted access to CCO Record-Level Data received through its various data sharing agreements must provide CCO's Information Management Coordinator with a copy of any report of the research findings for review a minimum of 30 business days before such report is published.

4.9 Disclosure Of CCO Aggregate Data

- CCO discloses Aggregate Data to requestors in accordance with the Business Process for Data Requests.

4.10 Internal Access Requests

- Internal access requests will be reviewed and approved in accordance with CCO's Internal Data Access Policy and Procedure.

4.11 Appeals Process

- In cases where requests for access to CCO data is denied, or restrictions are placed on the data elements requested, the Information Management Coordinator prepares and delivers a written summary of the reasons for denial or restricted access. Applications may be re-submitted following compliance with the modifications recommended in the summary.
- Decisions are subject to a right of appeal to the Data Disclosure Subcommittee.
- Policy decisions of the Data Disclosure Subcommittee will be incorporated into this Data Use and Disclosure Policy to ensure consistency indecision making.

4.12 Timelines

- CCO's makes its best efforts to is to respond to all data access requests within one to two weeks for requests for Aggregate Data and within 60 days for requests for research data (from the date that a complete access request is submitted to the Information Management Coordinator), except where otherwise notified by the Information Management Coordinator. CCO gives priority to requests by internal data users. CCO prioritizes requests by external requestors according to its business needs and capabilities.

4.13 Awareness

- CCO Staff are expected to understand and adhere to the requirements set out in this Policy. Guidelines and training are provided for CCO Staff, consultants and contractors to ensure awareness of, and compliance with, this Policy. See CCO's Privacy and Security Training and Awareness Procedure.

4.14 Review

- This Policy is reviewed and amended by the Data Disclosure Subcommittee as required.

4.15 Compliance

- This Policy supports the implementation of Principles, as provided under CCO's Privacy Policy.
- All CCO employees and Third-Parties must comply with this Policy, as well as CCO's Business Process for Data Requests.
- Compliance with this Policy will be enforced by the Legal & Privacy Office, and the Legal & Privacy Office will conduct audits to ensure compliance with this Policy in accordance with CCO's Privacy Audit and Compliance Standard.