Cancer Care Ontario

Action Cancer Ontario

Data Use & Disclosure Standard

Document Control:

Owned by:	Privacy & Access Office
Implemented by:	Privacy & Access Office, Informatics
Last Revised:	June 12, 2014
Next Review Date:	August 1, 2014
Approved by:	Chief Privacy Officer
Effective Date:	July 1, 2014

1. Purpose

The purpose of this Standard 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 Standard applies to CCO in its capacity as a Section 45 prescribed entity under PHIPA and encompasses:

1. the *use* of CCO data by data users for planning and management purposes (CCO employees and Third Parties[1]).
2. the *disclosure* of CCO data to external requestors for purposes other than research; and;
3. the *disclosure* of CCO data for the purposes of research to CCO employees and external requestors.

This Standard also applies to CCO's 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.

An*y use or d*isclosure of CCO data must comply with the principles and procedures set forth in this Standard. Requests for exceptions to this Policy must be submitted in writing to the Data Access Committee; must specify the CCO data requested and its intended use; and provide 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 will take precedence over this Standard.

3. Data Classification

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

a) **Identifiable Record-Level Data**: data that includes elements that directly identify an individual. By definition, identifiable record-level data contains PHI;

b) **De-identified Record-Level Data**: data that includes elements that may constitute identifying information because there may be reasonably foreseeable circumstances in which the data could be utilized, alone or with other information, to identify an individual. (e.g., if linked with publicly available data.) Thus, de-identified record-level data may contain PHI;

c) **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

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

[2] See the CCO Data Use & Disclosure Standard

d) **Published Data**: data that is made available to the public. Published data does not include PHI.

4. 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.

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 by law, subject to the permitted disclosures as set out in PHIPA and its accompanying regulations. These permitted disclosures are as follows:

As a prescribed entity:

- 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 that provided it to CCO, directly or indirectly, if it does not contain any additional identifying information.

As a prescribed registry:

- a participant's primary care provider (i.e. a health information custodian as defined under section 3 of the Personal Health Information Protection Act, 2004) so that he/ she is aware of the participant's screening information and results;
- a primary care provider (i.e. a health information custodian) who will provide 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. a health information custodian) that will refer 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]

[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. Use of CCO Data by Data Users

This section of the Standard applies to requests by data users for access to:

- identifiable record-level data
- de-identified record-level data

Data users include CCO employees and Third Parties (see above definition) 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 will be 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 will be 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 can be used to identify an individual.

CCO expressly forbids the use of de-identified record-level data, either alone or with other information, to identify an individual.

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 will be administered by the Data Steward for the data holding.

6. Access to Record-Level Data

Prior to being granted access to CCO record-level data, all employees and Third Parties must:

a) 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 must be signed by the user's supervisor, the Data Steward for the data-holding, and the Senior Manager, Data Management. . See CCO's Direct Data Access Procedure;
b) Complete Privacy and Security Orientation training, and annual Privacy and Security Refresher training thereafter and
c) 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.

7. Third Party Service Provider Access to Record-Level Data

In addition to the requirements set out above in Section 6, 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, must enter into a written agreement with CCO ("Template Agreement for Third Party Service Providers"),

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

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 should work 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 Privacy & Access Office 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 shall e-mail the Privacy & Access Office and the Legal Department to notify them of the breach of the Third Party Service Provider written agreement. The Business Unit shall 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.

8. Breach of Policy

Violations of this Policy by data users may 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 Program Area Supervisors are responsible for ensuring that Third Parties employed within their Program Area are familiar with and adhere to this Standard.

9. 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.

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 legitimate purposes.

- CCO will provide the least sensitive level of data that is practicable in order to fulfill the purpose identified by the requestor.

- 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 will review other aggregate data for residual risk of identification. See CCO's De-Identification Guidelines.

- CCO will charge external requestors for its time in preparing and delivering CCO data in response to approved requests in accordance with the published Tariff of Costs.

10. 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 will consider 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;
- 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, must submit:

- An REB approved research protocol;
- An *Application for Disclosure of Information from Cancer Care Ontario for Research Purposes*), with the REB approval appended.

Researchers requesting 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.

11. Disclosure Of CCO Aggregate Data

CCO will disclose aggregate data to requestors in accordance with the Business Process for Data Requests.

12. Access Procedures

See CCO's Direct Data Access Procedure.

13. 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 will prepare and deliver 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 Access Committee.

Policy decisions of the Data Access Committee will be incorporated into the Data Use and Disclosure Standard decision-making process to ensure consistency of decision making. Decisions of the Data Access Committee that have general applicability will be made available to requestors.

14. Timelines

CCO's goal is to provide a timely response to all data access requests, that is, within 1-2 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 will give priority to requests by internal data users. CCO will prioritize requests by external requestors according to its business needs and capabilities.

15. Awareness

Guidelines and training will be provided for CCO employees, consultants and contractors to ensure compliance with this Standard. See CCO's Privacy and Security Training and Awareness Procedure.

16. Review

This Policy will be reviewed and amended by the Data Access Committee as required.

17. Compliance

This Standard supports the implementation of Principle 5, as provided under CCO's Privacy Policy. All CCO employees and Third Parties must comply with this Standard, as well as CCO's Business Process for Data Requests, compliance with which will be reviewed in accordance with the Privacy Audit and Compliance Standard.

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")
CCO Privacy Audit and Compliance Standard
CCO De-Identification Guidelines
CCO Business Process for Data Requests
CCO Decision Criteria for Data Requests
CCO Direct Data Access Procedure
CCO Direct Data Access Audit Procedure
CCO Privacy Breach Management Procedure
CCO Privacy Training and Awareness Procedure
CCO Data Steward Terms of Reference
CCO Data Access Committee Terms of Reference
Application for Disclosure of Information from Cancer Care Ontario for Research Purposes
General Data Request Form