CANCER CARE ONTARIO'S PRIVACY POLICY
("CCO'S PRIVACY POLICY")

Approval:	Executive Team	Date Approved:	February 1, 2018
Sponsor:	Erica Zarkovich, General Counsel, Chief Privacy Officer & Corporate Secretary	Effective Date:	February 1, 2018
		Last Revised:	November 14, 2017
		Next Review Date:	November, 2020
References: Ontario's *Personal Health Information Protection Act, 2004* and associated Ontario Regulation 329/04; Research Privacy Policy (forthcoming); Freedom of Information and Protection of Privacy Act - Privacy Policy			

Policy

1. PURPOSE

Cancer Care Ontario ("**CCO**") is a provincial government agency responsible to the Ministry of Health and Long Term Care ("**MOHLTC"**). CCO's main mandate is as set out in the *Cancer Act*. CCO is subject to Ontario's health information privacy legislation, the *Personal Health Information Protection Act, 2004* ("**PHIPA**").[1]

This Privacy Policy sets out the principles CCO follows in relation to personal health information ("**PHI**") received by CCO as a Prescribed Entity, Prescribed Registry and Health Information Network Provider ("**HINP**"). This Privacy Policy is implemented throughout CCO using appropriate means to ensure that CCO employees understand and apply the CCO privacy

[1] PHIPA is based on the 10 privacy principles set out in the *Canadian Standards Association Model Code for the Protection of Personal Information* ("CSA Model Code"). The CSA Model Code, which became recognized as a national standard for privacy protection in 1996, is used across Canada as the basis for health information privacy legislation, policies and procedures. The CSA Model Code includes the following 10 principles:

1. Accountability;
2. Identifying Purposes;
3. Consent;
4. Limiting Collection;
5. Limiting Use, Disclosure and Retention;
6. Accuracy;
7. Safeguards;
8. Openness;
9. Individual Access; and
10. Challenging Compliance.

CCO's Privacy Policy is structured around these 10 privacy principles

policies in their daily work.

2. STATUS UNDER PHIPA

A Prescribed Entity

CCO has the status as a 'prescribed entity' under s. 18(1) of Ontario Regulation ("**O. Reg.**") 329/04 to PHIPA for the purposes of s. 45 of PHIPA ("**Prescribed Entity**"). This means that CCO has the authority to collect, use and disclose PHI for the purposes 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.

A Prescribed Registry

CCO also has the status as a 'prescribed registry' under PHIPA ("**Prescribed Registry**") with respect to CCO's role in compiling and maintaining the Ontario Cancer Screening Registry ("**OCSR**") as part of Ontario's Cancer Screening Program ("**CSP**"). This designation grants CCO the authority to collect, use and disclose PHI, without consent, for the purpose of facilitating or improving the provision of healthcare.

As a Prescribed Entity and a Prescribed Registry, CCO is subject to oversight by the Information and Privacy Commissioner of Ontario ("**IPC**") and has its information practices reviewed and approved by the IPC every three years. This review process provides the public with the assurance that CCO's privacy practices comply with PHIPA and with standards of practice expected from the IPC.

A 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. As a Prescribed Entity or a Prescribed Registry, CCO can collect, use or disclose PHI as if it were a Health Information Custodian ("**HIC**") 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.

A HINP

CCO provides information systems to HICs to enable them to exchange PHI with each other. In providing such services, CCO is acting as a HINP and is subject to additional privacy requirements under O. Reg. 329/04 of PHIPA. This Privacy Policy describes the standards employed by CCO to protect PHI managed in this capacity and describes how CCO meets the privacy requirements detailed in the Regulation.

3. CCO'S PRIVACY PROGRAM

CCO is committed to complying with its obligations under PHIPA and its associated regulations, respecting personal privacy, safeguarding confidential information and ensuring the security of PHI within its custody. CCO meets this commitment through its Privacy Program.

CCO's Privacy Program sets out comprehensive privacy and security policies and procedures, as referenced throughout this Policy, to ensure compliance with PHIPA and its regulations.

4. SCOPE

This Policy applies to CCO and all of its agents in respect of CCO's role as a s. 45 Prescribed Entity, a ss. 39(1)(c) Prescribed Registry, and a HINP under PHIPA, as well as to the data holdings which CCO operates in these roles.

This Policy is supplemented by the CCO Research Privacy Policy that further sets out the privacy requirements that apply to CCO when providing services to CCO affiliated researchers conducting research studies.

This Policy does not apply to CCO's collection, use and disclosure of personal information ("**PI**") under the *Freedom of Information and Protection of Privacy Act* ("**FIPPA**"), for which CCO's privacy requirements are set out under the FIPPA Privacy Policy.

CCO's Privacy Policy complies with PHIPA. If there is a discrepancy between the Policy and PHIPA, PHIPA takes precedence.

5. POLICY

PRINCIPLE 1: Accountability

CCO's President and Chief Executive Officer is ultimately accountable for ensuring compliance with PHIPA and ensuring compliance with CCO's privacy and security policies, procedures and practices implemented.

CCO's President and Chief Executive Officer has delegated day-to-day responsibility for ensuring compliance with PHIPA and CCO's privacy and security policies and procedures to members of CCO management, notably the Chief Privacy Officer ("**CPO**") for privacy and the Vice-President, Technology Services for security.

The CPO is supported in carrying out her responsibilities by a network of individuals with specific privacy and security related responsibilities, including:

- a Director, Legal & Privacy Office ("**LPO**"), who is responsible for overseeing the operation of privacy processes within CCO and compliance with CCO privacy policies; and
- a Group Manager, Privacy, who reports to the Director, LPO, and who manages the day-to-day operation of CCO's Privacy Program.

A variety of other roles, notably Privacy Managers, Senior Specialists and Specialists support CCO in the discharge of CCO's privacy obligations. The organizational chart provided on CCO's website sets out the structure of CCO's Privacy Program.

The Vice-President, Technology Services is responsible for overseeing information technology security safeguards for CCO data. She is supported by:

- a Director, Architecture and Information Security Services who oversees the Enterprise Information Security Office ("**EISO**");
- a Group Manager, Technology Services, who reports to the Director, Architecture and Information Security Services and who manages the day-to-day operation of EISO; and
- Information Security Advisors who provide advisory services to Business Units to enable the development and implementation of information security controls.

CCO is responsible for PHI used by its agents and has developed and implemented privacy policies, standards, procedures and guidelines that set out the privacy roles and responsibilities for CCO employees. They set out the controls and specific means by which CCO and its agents will meet (i) the commitments set out in the CCO Privacy Policy, (ii) privacy legislative and regulatory requirements, and (iii) other goals in relation to the protection of PHI.. CCO provides privacy and security training to all CCO employees to ensure they understand and apply CCO's privacy requirements in their daily work.

CCO is responsible for PHI that is used by Third-Parties acting on its behalf. CCO uses contractual or other means to ensure that a comparable level of protection is applied when PHI is handled by Third-Parties.

Related Documents

- Cancer Care Ontario Privacy Policy
- Privacy Governance Framework
- Privacy and Security Training and Awareness Procedure
- Privacy and Security eLearning Curriculum
- Privacy and Security Acknowledgement Form
- Enterprise Information Security Policy
- Schedule to Service Agreement Template - CCO Principles and Procedures for the Provision and Use of PI and PHI - Access Terms & Conditions
- Confidentiality Policy
- Statement of Confidentiality

PRINCIPLE 2: Identifying Purposes for PHI

Consistent with CCO's role as a s. 45 Prescribed Entity under PHIPA, CCO collects PHI to plan, fund and report on the performance of our roles in the healthcare system. CCO also collects PHI pursuant to ss. 39(1)(c) of PHIPA to compile and maintain the Ontario Cancer Screening Registry, for the purposes of facilitating and improving the provision of health care for Ontarians.

For example, CCO collects PHI to:

- calculate survival rates;
- estimate cancer and chronic kidney disease incidence and demand for services;
- report wait times for radiation, chemotherapy, and cancer surgery;
- report on the quality of cancer services in Ontario;
- develop clinical guidelines;
- reimburse hospitals for specific cancer drugs;
- manage CCO's Cancer Screening Program or CSP;
- advise the MOHLTC on healthcare issues;
- create outreach programs that support early screening activities for the population; and
- support research by CCO scientists and research associates.

CCO documents the purposes for which it collects PHI for each of its data holdings, and consults with organizations that disclose PHI to CCO on these purposes. CCO collects PHI from healthcare organizations and professionals (primary data collectors) as permitted under PHIPA. CCO encourages and supports these primary data collectors in making the purposes for which PHI is disclosed to CCO known to individuals who provide such PHI. The CPO will ensure that an overview of CCO's Privacy Program in the form of a Statement of Information Practices is published and made available to primary data collectors.

CCO's data holdings and the purpose for which CCO collects PHI for each of its data holdings is listed in CCO's Data Holdings List. CCO Business Units are responsible for:

- creating a statement of purposes for data holdings under their responsibility;
- ensuring the statement of purposes is up to date; and
- ensuring a copy of the approved statement is provided to the LPO for inclusion in privacy-related documentation and the CCO Data Holdings List.

The LPO is responsible for approving final statements of purpose once created. If statements of purpose are reviewed or amended, the LPO must be consulted on the review or amendment and will approve the review or amendment.

CCO also makes the following information available to HICs and the public when providing IT services in CCO's role as a HINP:

- a plain language description of the CCO IT services provided;

- the administrative, physical and technical safeguards (including directives, guidelines and policies) that have been implemented to protect PHI against unauthorized use or disclosure, and to protect the integrity of the information;
- contact information for CCO's Legal & Privacy Office or LPO.

CCO employees receive privacy and security training and are aware of the purposes for which PHI is collected for the data holding(s) associated with their Business Unit. CCO ensures that disclosures of PHI from its data holdings are consistent with the disclosures permitted by PHIPA and its regulation.

Related Documents

- List of CCO Data Holdings
- Statement of Information Practices
- Privacy FAQs
- Privacy and Security Training and Awareness Procedure
- Privacy and Security eLearning Curriculum
- Privacy and Security Acknowledgement Form
- Health Information Network Provider Toolkit

PRINCIPLE 3: Knowledge and Consent for the Collection, Use or Disclosure of PHI

CCO collects, uses and discloses PHI in accordance with the authorities set out in PHIPA. As a Prescribed Entity and a Prescribed Registry, pursuant to s. 45 and 39(1)(c) of PHIPA, CCO collects and uses information disclosed to it by primary data collectors (including health information custodians or HICs), without the consent of the patient for programs which support planning and management for, as well as the facilitating or improving the provision of healthcare.

CCO also handles or uses PHI in its role as a HINP when providing services to enable HICs to use electronic means to share PHI with one another. HICs are responsible for complying with the knowledge and consent components of PHIPA. However, for the Cancer Screening Program or CSP, CCO provides participants with the opportunity to opt out of program correspondence (i.e. invitations, results, notifications and screening reminders).

CCO ensures that its information management practices are easily accessible to primary data collectors and the public.

Related Documents

- Statement of Information Practices
- List of CCO Data Holdings
- Privacy FAQs

- Cancer Screening Program Participation Form
- Data Use and Disclosure Standard

PRINCIPLE 4: Limiting Collection of PHI

CCO limits the collection of PHI to that which is necessary for identified purposes and in accordance with the requirements set out in PHIPA. CCO does not collect PHI if other information will serve the purpose and does not collect more PHI than is reasonably necessary to meet the purposes outlined above. To that end, CCO has established policies, procedures and practices, to ensure that the amount and type of PHI collected is limited to that which is reasonably necessary for its purpose and to ensure that the collection is permitted by PHIPA.

This process may be informed by Business Units or advisory committees, and may further be guided by data sharing agreements between CCO and other entities. Where a data sharing agreement is required, the CCO Privacy Manager will ensure the agreement includes:

- a statement of the authority and purpose for the collection;
- a description of data elements required for the collection;
- an acknowledgement that the PHI collected pursuant to the data sharing agreement is necessary for the purpose for which it was collected;
- the secure manner in which the records of PHI will be transferred;
- the secure manner in which the records of PHI will be securely retained;
- the reasonable steps to be taken to ensure that the PHI subject to the DSA is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of PHI are protected against unauthorized copying, modification or disposal;
- details of the destruction or return of the PHI, including timing and method;
- details of breach notification and/or containment in respect of the DSA

Where data elements are disclosed to CCO by a data provider that falls outside the purposes identified for a data holding, the CCO Privacy Manager will work with the business lead and the data provider to return or destroy the unnecessary data elements, so as to minimize the data elements required to meet the purposes of the identified for a data holding.

Related Documents

- Data Sharing Agreement Initiation Procedure
- Data Sharing Agreement Standard
- Privacy Impact Assessment Standard
- Data Holdings List

PRINCIPLE 5: Use, Disclosure and Retention of PHI

Use

CCO only uses and discloses PHI for the purposes for which it was collected, and/or as permitted or required by PHIPA. CCO will not use and disclose PHI if other information, namely de-identified or aggregate information, will serve the purpose. CCO will not disclose more PHI than necessary to meet the purpose.

CCO uses PHI for:

- the purposes of planning and management of the provincial healthcare system including:
  - determining key indicators such as survival rates, wait times, disease incidence and the demand for services;
  - creating reports to advise the MOHLTC and other health care partners; and
  - reimbursing hospitals for various services and programs
- to compile and maintain the Ontario Cancer Screening Registry or OCSR for the purpose of facilitating or improving the provision of healthcare; and
- to provide IT services to enable HICs to use electronic means to disclose PHI to one another.

As part of this work, CCO performs data linkages. For example, the Cancer Screening Program or CSP, performs data linkage for identifying eligible population for screening as well as to conduct planning and management activities.

Access and Disclosure

CCO employees, Third-Parties and volunteers, are authorized to access PHI on a "need-to-know" basis only where it is required to perform official CCO duties. CCO prohibits the access to or use of more PHI than is reasonably necessary to meet the identified purpose and has appropriate processes to be followed upon termination or cessation of the employment, contractual, or other relationship to ensure access privileges are terminated and CCO property is returned.

PHI is disclosed by CCO, as authorized by law, to organizations such as the Institute of Clinical and Evaluative Sciences ("**ICES**"), the Canadian Institute for Health Information ("**CIHI**"), Statistics Canada, HICs, and to researchers who comply with research requirements set out in PHIPA. All data disclosures, including the disclosure of identifiable record level data, de-identified record level data or aggregate data, to persons external and internal to CCO must comply with CCO's Data Use and Disclosure Standard and where required by PHIPA.

Retention

CCO retains PHI as long as necessary to fulfill the purposes of the data holding and in accordance with PHIPA. Generally, given CCO's role as a Prescribed Entity and Prescribed Registry, PHI will be retained long term to support retrospective analysis for the purposes of planning and management of the provincial healthcare system and to support the OCSR.

All records of PHI, including records of PHI in paper format and in electronic format, no longer required to fulfill the identified purpose, must be destroyed in a secure manner and in a manner that is compliant with PHIPA[2].

CCO holds each data holding containing PHI "separate and apart" from CCO's other data holdings (*i.e.*, held in a separate database within the same database management system).

The Data Steward is responsible for maintaining an inventory of data holdings that includes information on:

- the format of the data (paper or electronic);
- its physical location;
- the time span of the data; and
- secure destruction of data when it is no longer required.

Related Documents

- Data Use and Disclosure Standard
- Privacy Impact Assessment Standard
- List of CCO Data Holdings
- Privacy and Security Training and Awareness Procedure
- Confidentiality Policy
- Statement of Confidentiality
- Internal Data Access Policy
- Employee Exit Process
- Business Process for Data Requests
- De-identification Standard
- Data Access Committee Terms of Reference
- Data Sharing Agreement Standard
- Data Sharing Agreement Initiation Procedure
- Data Sharing Agreement Template
- Data Linkage Policy
- Policy on Retention of Records Containing PHI
- Enterprise Information Security Policy
- Business Continuity Plan
- Disaster Recovery Plan
- Information Security Code of Conduct
- Operational Security Standard
- DBAN Disk Wipe Procedure
- Digital Media Disposal Guideline

---

[2] Please see CCO's Enterprise Information Security Policy; Operational Security Standard; Digital Media Disposal Standard; Digital Media Disposal Procedure; Information Classification and Handling Guideline; and Hard-Copy PHI Disposal Procedure.

PRINCIPLE 6: Accuracy of PHI

CCO maintains the accuracy of PHI as necessary for the activities it conducts in support of its planning and management mandate and to support its activities for the Ontario Cancer Screening Registry or OCSR.

CCO's Analytics & Informatics Division is responsible for establishing a CCO data quality program, practices and processes appropriate to CCO's programs and services. The CCO Business Unit, in conjunction with the Analytics & Informatics Division, will determine the appropriate data submission specifications and other related requirements for the data holdings in their area, and convey these to respective primary data collectors and others with access to the data. A Data Steward or program lead for the data holding is responsible for ensuring compliance with established data quality practices and processes.

Some CCO programs, such as the Cancer Screening Program or CSP will allow individuals to correct the data that applies to them, upon the receipt of the appropriate written authorization.

Related Documents:

- Business Process for Data Requests
- Cancer Screening Program Participant Form

PRINCIPLE 7: Safeguards for PHI

CCO has physical, administrative and technical systems in place to safeguard PHI in its custody against loss, theft, unauthorized access, disclosure, copying, use, or modification. The nature of the safeguards corresponds to the sensitivity of the information collected the amount, distribution and format of the information; and the method of storage.

Physical Safeguards

CCO provides a secure physical environment for the equipment on which PHI is stored and for the employees who use PHI.

The Facilities Manager is responsible for ensuring, that:

- the physical premises are secure;
- there is controlled access to CCO offices;
- employees are provided with appropriate identification;
- visitors are appropriately screened and authorized to be on the premises; and
- video surveillance is used for forensics purposes and is not monitored.

Some operational areas which process PHI may require restricted access with a secondary level of access controls.

Administrative Safeguards

CCO uses confidentiality agreements to reinforce employee and Third-Party understanding of their responsibility to protect PHI and to create a culture of privacy at CCO. All employees and contracted Third-Parties are required to comply with CCO's privacy and security requirements, including, for example, to advise the LPO at the first reasonable opportunity of any privacy breach or suspected privacy breach.

The CPO and VP, Technology Services are responsible for ensuring that data accessed by staff and Third-Parties is in compliance with the CCO's privacy and security requirements and that access to PHI is audited on a regular basis.

CCO, when providing IT services as a HINP, enters into a written services agreement with each HIC. The services agreement includes a description of the administrative, technical and physical safeguards in place to protect the confidentiality and security of PHI, as well as the following restrictions:

- CCO is in compliance with PHIPA and its associated regulation;
- CCO does not use PHI to which it has access in the course of providing IT services except as necessary in the course of providing the services;
- CCO does not disclose PHI to which it has access in the course of providing IT services; and
- all CCO employees and contracted Third-Parties agree to comply with CCO's privacy and security requirements.
- CCO notifies the applicable HIC at the first reasonable opportunity of any privacy breach.

The CPO ensures that there are adequate processes in place to ensure that PHI is safeguarded, including:

- appropriate confidentiality agreements and privacy & security training programs;
- appropriate contracts with data providers and Third-Parties; and
- appropriate contracts with disposal firms for the secure destruction of paper records containing PHI.

CCO requires all employees, third parties, researchers, students and volunteers, working for, or on behalf of CCO, to be aware of the importance of maintaining the confidentiality of PHI through its privacy and security training and awareness program. Specifically, where Third-Parties support CCO activities and require access to CCO systems they are subject to the same privacy and security training requirements as CCO employees.

CCO requires that PIAs, and as appropriate, security analyses and threat risk assessments, be completed for any purposes as listed in the *Privacy Impact Assessment Standard*, including when CCO is providing IT services in its role as a HINP. When providing services as HINP,

CCO will make a general description of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information available to each applicable HIC upon request.

CCO also has a comprehensive privacy risk management program to ensure privacy risks are identified, mitigated and responsibly managed.

Technical Safeguards

CCO adopts industry standards and tests its systems to ensure PHI in its custody, and the equipment and communication systems utilized by CCO are secure.

When providing services as a HINP, CCO keeps and makes available to each applicable HIC, to the extent reasonable practical, an electronic record of all access and transfers of PHI associated with the HIC.

Supporting Documents:

- Physical Security Policy
- Access Card Procedure
- Visitor Access Policy
- Video Monitoring Policy
- Confidentiality Policy
- Statement of Confidentiality
- Template Third Part Service Provider Agreement
- Privacy and Security Training and Awareness Procedure
- Privacy and Security Acknowledgement Form
- Information Security Code of Conduct
- Privacy Impact Assessment Standard
- Privacy and Information Security Risk Management Procedure
- Change Management Policy
- Information Security Policy
- Logging, Monitoring and Auditing Standard
- Logical Access Control Standard
- Information Classification and Handling Standard
- Information Classification and Handling Guideline
- Cryptography Standard
- Logging, Auditing and Monitoring Standard
- Health Information Network Provider Toolkit

PRINCIPLE 8: Openness about the Management of PHI

CCO makes information available in paper and/or electronic form to primary data collectors, the

public and other stakeholders about its policies and practices relating to the management of PHI, including with respect to the collection, use and disclosure of PHI.

The LPO ensures that the following are publicly available:

- general information on CCO's privacy practices;
- descriptions of CCO's data holdings of PHI; and
- contact information for CCO's LPO.

Related Documents:

- Statement of Information Practices
- Privacy FAQs
- CSP Privacy FAQs
- CCO external website Privacy Page
- List of CCO Data Holdings
- Privacy Inquiries and Complaints Procedure

PRINCIPLE 9: Individual Access to and Amendment of PHI

Pursuant to FIPPA, the public can request access the records held by CCO.. CCO provides the public with the contact information and instructions on how to make a FIPPA request on the CCO public website:

https://www.cancercare.on.ca/about/who/foi/ .

CCO has a FIPPA program in place to process Freedom of Information ("**FOI**") requests from the public. Individuals may make a request for records held by CCO to CCO's FOI coordinator.

The CSP will provide individuals with an opportunity to update information that pertains to them, such as address or telephone number which is stored in the OCSR for cancer screening correspondence purposes.

Related Documents:

- Freedom of Information FAQs
- CSP Participant Form

PRINCIPLE 10: Complaints or Inquiries About CCO's Handling of PHI

Any person may submit an inquiry, concern, or complaint regarding CCO's information practices, its privacy policies and procedures, its compliance with PHIPA, or the purposes for

which PHI is collected to CCO's LPO. They can do so by writing to:

Chief Privacy Officer
CCO Legal & Privacy Office
Cancer Care Ontario
620 University Avenue
Toronto, ON M5G 2L7

or by emailing: legalandprivacyoffice@cancercare.on.ca.

CCO makes information regarding how to submit an inquiry or complaint, including the title and address that the inquiry or complaint should be directed to, available on CCO's website.

The LPO reviews and logs all complaints.

A person may also submit a concern or complaint to the IPC. They can do so by writing to:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8

Any privacy breach, suspected privacy breach, or privacy risk will be investigated according to the relevant Privacy Breach Management Policy by the LPO.

A log of privacy breaches, suspected privacy breaches, and privacy risks is maintained by the LPO.

CCO fosters an environment in which issues and concerns regarding privacy breaches, suspected privacy breaches, or privacy risks may be raised and discussed openly. For further detail on reporting potential wrongdoing, please refer to CCO's Policy on Ethical Conduct.

Related Documents:

- Privacy Breach Management Policy
- Privacy Breach Management Manual
- Privacy Inquiries and Complaints Procedure

APPENDIX A: DEFINITIONS

Agent: means a person that acts for on on behalf of CCO for the purposes of CCO, and not for the agent's own purposes, whether or not the agent has the authority to bind CCO, whether or not the agent is employed by CCO, and whether or not the agent is being remunerated.

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 PHI.[3]

Business Unit: CCO programs and/or departments accountable for a Data Holding.

CCO Data: has the meaning set out in CCO's Data Use & Disclosure Standard and includes Identifiable Record-Level Data, De-Identified Record-Level Data, Aggregate Data and Published Data.

CCO Staff: all CCO employees, whether full or part-time, temporary or permanent, all individuals paid by, or under contract with CCO, including but not limited to consultants and independent contractors, and any individual working for or on behalf of CCO on an unpaid basis or for nominal consideration.

Collect: has the meaning set out in section 2 of PHIPA. In relation to PHI, **"collect"** means to gather, acquire, receive or obtain the information by any means from any source, and **"collection"** has a corresponding meaning.

CSA Model Code: is the Canadian Standards Association *Model Code for the Protection of Personal Information*.[4]

Data Access Request: a data access request made to the Data Access Committee in the format as set out in the *Business Process for Data Requests.*

Data Element: is a category used to identify a data type.

Data Exchange: the disclosure of one or more Data Sets from CCO to an External Party, or the collection of one or more Data Sets by CCO from an External Party.

Data Holding: is a full collection of data, categorized by Data Element, and relied upon to support specific business purposes.

Data Holdings List: is a central, online repository which describes all CCO Data Holdings, including pre-formatted data, organized data, enhanced data, reports and data sources.

---

[3] See the *Data Use & Disclosure Standard*

[4] Canadian Standards Association, "CAN/CSA – Q830-96, Model Code for the Protection of Personal Information," March 1996, reaffirmed 2001.

Data Linkage: is the process by which PHI about an individual from one Data Holding is combined with that of another Data Holding, to create new information about the individual, which may include new PHI.

Data Provider: any person from whom CCO collects one or more Data Set(s).

Data Set: a subset of a Data Holding made up of populated Data Elements, which could be Identifiable Record-Level Data, De-identified Record-Level Data, Aggregate Data or Published Data.

Data Sharing Agreement or DSA: 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.

Data Steward: is the person who is accountable for ensuring that privacy, security and data quality requirements are met for Data Holdings under their stewardship, and for maintaining an inventory of the Data Holding. A Data Steward will be assigned for each Data Holding to monitor all uses of PHI and ensure the uses are consistent with CCO's mandate and the purposes for the Data Holding.

Decision Criteria: the decision criteria as set out in the *Decision Criteria for CCO Data Requests.*

De-Identification: has the meaning set out in section 47(1) of PHIPA. In relation to PHI, "De-Identification" means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

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. See the *Data Use & Disclosure Standard*.

Disclose: has the meaning set out in section 2 of PHIPA. In relation to PHI in the custody or under the control of a Health Information Custodian or a person, means to make the information available or to release it to another Health Information Custodian or to another person, but does not include to use the information, and "**Disclosure**" has a corresponding meaning.

External Party: is (a) a person that has requested a Data Set from CCO for disclosure to the person; or (b) a person from which CCO has requested a Data Set, for collection by CCO. An External Party may include CCO, in its capacity as a Prescribed Entity, where it is disclosing a Data Set to or collecting a Data Set from CCO in its capacity as a Prescribed Registry, or vice versa.

***Freedom of Information and Protection of Privacy Act* or FIPPA:** is provincial legislation with two main purposes: 1) to make provincial government institutions more open and

accountable by providing the public with a right of access to records; and 2) to protect the privacy of individuals with respect to their Personal Information held by provincial government organizations. References to FIPPA includes the Regulations thereunder, as may be amended or replaced from time to time.

Health Information Custodian or HIC: is a listed individual or organization under section 3 of PHIPA that, as a result of their power or duties, has custody of PHI. Examples of health information custodians include:

- health care practitioners (i.e. doctors, nurses, pharmacists, psychologists, and dentists);
- hospitals (public or private);
- psychiatric facilities;
- pharmacies;
- laboratories;
- long-term care home;
- retirement homes and homes for special care;
- community access centers;
- ambulance services; and
- Ministry of Health and Long-Term Care.

Health Information Network Provider or HINP: has the meaning set out in section 6(1) of PHIPA regulation 329/04, and means a person who provides services to two or more HICs where the services are provided primarily to HICs to enable the HICs to use electronic means to disclose PHI to one another, whether or not the person is an agent of any of the HICs.

Identifiable Record-Level Data: data that includes elements that directly identify an individual. By definition, Identifiable Record-Level Data contains PHI. See the *Data Use and Disclosure Standard*.

Information and Privacy Commissioner of Ontario or IPC: is the Information and Privacy Commissioner of Ontario and his/her lawful delegate(s) and staff members, as the context permits. The IPC plays a crucial role under PHIPA and FIPPA. In general terms, the IPC's mandate is to:

- independently review the decisions and practices of government organizations concerning access and privacy;
- independently review the decisions and practices of HICs in regard to PHI;
- conduct research on access and privacy issues;
- provide comments and advice on proposed government legislation and programs;
- review the PHI policies and practices of entities and prescribed persons under PHIPA; and
- educate the public about Ontario's access, privacy, and personal health information laws and related issues.

Legal & Privacy Office or LPO: the department within CCO that, among other things, ensures that CCO's operations comply with PHIPA and FIPPA.

Personal Health Information or PHI: has the meaning set out in section 4 of PHIPA. Specifically it is "identifying information" about an individual that:

- relates to the physical or mental health of the individual;
  relates to the provision of health care to the individual;
- is a plan of service under the *Home Care and Community Services Act*, 1994;
- relates to payments or eligibility for health care or eligibility for coverage for health care;
- relates to the donation of any body part or bodily substance of the individual or that is derived from the testing or examination of any such body part or bodily substance;
- is the individual's health number; and/or
- identifies an individual's substitute decision-maker.

PHI also includes identifying information about an individual that is not PHI listed above but that is contained in a record that includes PHI listed above.

Information is "identifying" when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

***Personal Health Information Protection Act,* 2004 or PHIPA:** Ontario's health-specific privacy legislation which governs the manner in which PHI may be collected, used, and disclosed within the health care system. Includes the Regulations thereunder, as may be amended or replaced from time to time.

Personal Information or PI: has the meaning set out in section 2 of FIPPA. Specifically, it means recorded information about an identifiable individual, including:

- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- any identifying number, symbol or other particular assigned to the individual;
- the address, telephone number, fingerprints or blood type of the individual;
- the personal opinions or views of the individual except where they relate to another individual;
- correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the individual; and
- the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Privacy Impact Assessment or PIA: a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may

have on individuals' privacy.[5] It also helps to eliminate or mitigate those risks. The PIA examines how PHI is collected, stored, used, and disclosed.

Prescribed Entity: an entity that is prescribed in the regulations for the purposes of section 45 of PHIPA, to which a Health Information Custodian is permitted to disclose PHI for the purpose of analysis or compiling statistical information for 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. As a Prescribed Entity, CCO has the authority to collect, use, and disclose PHI for the purposes of health system planning and management.

Prescribed Registry: is a person that is prescribed in the regulations for the purposes of section 39(1)(c) of PHIPA, to which a HIC is permitted to disclose PHI to such person who maintains a registry of PHI for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or body substances. As a Prescribed Registry in respect of its Ontario Cancer Screening Registry, CCO has the authority to collect, use, and disclose PHI for the purposes of facilitating or improving the provision of health care with respect to its role in compiling and maintaining the Ontario Cancer Screening Registry.

Privacy Breach: is a breach of privacy, whether intentional or inadvertent, and includes:

- the misuse or improper/unauthorized collection, use, or disclosure of PHI that is not in compliance with the PHIPA;
- the contravention of a provision in a CCO Data Sharing Agreement, a research agreement, a research data disclosure agreement, a statement of confidentiality, or an agreement with a Third Party concerning the collection, use or disclosure of PHI;
- circumstances where PHI is stolen, lost or subject to (a) unauthorized use or disclosure or (b) unauthorized copying, modification or disposal; and/or
- a contravention of CCO's Privacy Policy or any related privacy policy, standard or procedure identified in the CCO Privacy Policy.

Privacy Risk: The possibility that an event may occur that results in (i) non-compliance with privacy laws - PHIPA and the FIPPA - regulations, CCO privacy policies or procedures, (ii) a failure to safeguard or prevent unauthorized collection, use or disclosure of personal information, or personal health information, or (iii) otherwise jeopardize CCO's status under PHIPA; all of which would adversely affect the achievement of CCO's objectives.

Published Data: data that is made available to the public. Published data does not include PHI. See Data Use and Disclosure Standard.

Research: has the meaning set out in section 2 of PHIPA. Research is a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research.

---

[5]see: IPC, *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*

Research may or may not include a protocol, research ethics board approval, and/or dedicated funding, whether internal or external.

Third-Party: includes consultants, contractors and third-party service providers.

Threat Risk Assessment: is a process for identifying and evaluating the potential threats to a system, and then for determining mitigating strategies against the risks where it is determined appropriate. For example, a potential risk to a system is a power outage or someone hacking into a system. The risk of these events occurring is considered along with their potential impact on the system and appropriate plans or measures developed to either prevent or manage their occurrence.

Use: has the meaning set out in section 2 of PHIPA. In relation to PHI in the custody or under the control of a HIC or other person (such as CCO), **"Use"** means to handle or deal with the information, subject to section 6(1); but does not include to disclose the information, and **"Use",** as a noun, has a corresponding meaning.