Privacy Policy

Policy Level Approval:	OH Board of Directors
Policy Category:	Corporate Policy
Policy Number:	INF-001.01-P
Sensitivity Level:	Public
Policy Sponsor (or Sponsors):	General Counsel and Executive Lead – Legal Privacy and Risk
Original Date of Approval:	September 2019
Date of Posting: This Policy is effective on the date of its posting or as otherwise noted in the Policy	March 15, 2022
Version Approval Date:	September 23, 2021
Next Scheduled Year Review (MM/YY):	06/24

1 Purpose, Objectives and Scope

1.1 Purpose

Ontario Health (**OH**) is a provincial agency whose mandate is set out in the *Connecting Care Act, 2019* (**CCA**). To fulfill this mandate, OH receives Personal Health Information (**PHI**) and Personal Information (**PI**) relating to health care provided in Ontario and to Ontario residents. In respect of this PHI and PI, OH is committed to:

- Complying with its obligations under applicable privacy law, including but not limited to the *Personal Health Information Protection Act, 2004* (**PHIPA**) and the *Freedom of Information and Protection of Privacy Act* (**FIPPA**)[1] and associated regulations; and
- Protecting the privacy of individuals and the confidentiality of their PHI and PI.

OH meets this commitment through this Policy and other supporting policies and procedures.

1.2 Principles

This Policy is structured around the 10 Fair Information Principles (**FIPs**) of the Canadian Standards Association's Model Code for the Protection of Personal Information (**CSA Model Code**)[2]. The CSA Model Code is recognized as a national standard for privacy protection and is used across Canada as the basis for privacy legislation, including PHIPA.

This policy also addresses the following general principles:

- The protection of PHI and PI is critical for OH's operations related to the services it provides and supports in the larger Ontario health system.
- OH complies with all applicable legislation related to the protection of PHI and PI.
- OH complies with all orders and directives from the Information and Privacy Commissioner of Ontario (**IPC**), as well as the IPC's:
    - *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities;* and
    - *Manual for the Review and Approval of Prescribed Organizations.*

1.3 Scope

This policy applies to: non-union Employees, people leaders, board members, unionized Employees, secondees, consultants, and other individuals acting on behalf of OH ('**OH Agents'**).

[1] This Policy does not apply to i) handling of Freedom of Information (**FOI**) requests, which is addressed in OH's FIPPA Access Request Policy, ii) PI that is maintained for the purpose of creating a record that is available to the general public, or iii) PI that is excluded from the application of FIPPA as set out under s. 65(1) to (9) of FIPPA.

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

1.4 Compliance and Exemptions

- Compliance with this Policy in its entirety is mandatory unless an exception to a specific section is approved by the Chief Privacy Officer (**CPO**) or delegate in writing. Failure to comply with the requirements of this Policy, without a written exception, may result in disciplinary action up to and including revocation of appointment, termination of employment or termination of contract without notice or compensation.
- Compliance will be audited in accordance with and as per the frequency outlined in the *Privacy Audit & Compliance Policy*.
- At the first reasonable opportunity upon identifying or becoming aware of a breach of this Policy, Employee(s) and other OH Agents must notify the Privacy Office by reporting the breach to Enterprise Service Desk by Phone: 1-866-250-1554; or Email: OH-DS_servicedesk@ontariohealth.ca.
- Breaches of this Policy will be managed in accordance with the *Privacy Incident Management Policy and Procedure*.

1.5 Terminology

- The words “include” and “including” when used are not intended to be exclusive and mean, respectively, “include, without limitation,” and “including, but not limited to”.
- Words and terms in this Policy that have meanings differing from the commonly accepted definitions are capitalized and their meanings are set out in the Definitions and Acronyms section (Section 0).

2 Background

2.1 Legacy Organizations and Transfers to Ontario Health

Pursuant to s. 40 of the CCA and orders of the Minister of Health, the following organizations have been transferred to OH:

- Cancer Care Ontario
- eHealth Ontario
- HealthForce Ontario Marketing and Recruitment Agency
- Health Shared Services Ontario
- Health Quality Ontario
- The Ontario Telemedicine Network
- Trillium Gift of Life Network

each a ‘Legacy Organization’, and together the ‘Legacy Organizations’.

The transfer of assets from the Legacy Organizations to OH may include data assets, such as PHI or PI, and digital assets (such as applications that process or store PHI or PI).

In addition to this Policy and supporting OH privacy policies and procedures, the privacy policies and procedures of each Legacy Organization will continue to apply to the handling of PHI and PI that has been transferred from the respective Legacy Organization to OH, and to new Collections of PHI and PI related to the operations of a Legacy Organization, until which time that the Legacy Organization's policies and procedures are repealed. This Policy is meant to complement the privacy policies of each Legacy Organization, and speak to the privacy principles to which OH adheres.

2.2 OH Status under PHIPA and FIPPA

OH is subject to Ontario's privacy legislation, PHIPA and FIPPA, as further described below.

2.2.1 PHIPA

PHIPA is a provincial health privacy law. It establishes rules for the management of PHI and the protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services.

In handling PHI, OH complies with the requirements that are particular to the role(s) described in PHIPA and its regulation. The requirements that apply may depend on, for example, the purpose for handling the PHI and the nature of the relationship of OH with Health Information Custodians (**HICs**) or other organizations, including those that are prescribed under PHIPA. A HIC is a person or organization that delivers healthcare services. Physicians, hospitals, pharmacies, laboratories, and the MOH are examples of HICs. OH is not a HIC. OH has multiple designations under PHIPA including:

- Prescribed Organization (**PO**) in respect of the Electronic Health Record (**EHR**)
- Prescribed Entity (**PE**)
- Prescribed Person (**PP**) in respect of its Prescribed Registry (**PR**)
- Health Information Network Provider (**HINP**)
- PHIPA Agent and
- Electronic Service Provider (**ESP**)

(see Appendix A for a summary of these roles and related duties and responsibilities under the PHIPA).

2.2.2 FIPPA

FIPPA has two main purposes:

1) To provide a right of access to information under the control of institutions; and
2) To protect the privacy of individuals with respect to PI about themselves held by institutions and to provide individuals with a right of access to their information.

FIPPA applies to all ministries of the Ontario Government and any agency, board, commission, corporation or other body designated as an "institution" in the regulations. OH is designated as a FIPPA institution under O. Reg. 460 of FIPPA. As such, OH complies with the requirements set out in FIPPA in regard to the Collection, Use, retention, Disclosure and disposal of PI in OH's custody or control to protect an individual's right to privacy.

3 Policy

3.1 Accountability

> The principle of accountability means that an organization is responsible for PHI and PI under its custody or control and shall designate an individual or individuals who are accountable for the organization's compliance with privacy principles.

OH is committed to:

- Complying with its obligations under PHIPA, FIPPA, and associated regulations and other applicable legislation; and
- Protecting the privacy of individuals and the confidentiality of their PHI and PI that is Collected, received, Viewed, Used, Disclosed, handled or otherwise dealt with by OH.

OH's Chair of the Board is ultimately accountable for ensuring OH's compliance with FIPPA and the OH Chief Executive Officer (**CEO**) is ultimately accountable for ensuring OH's compliance with PHIPA and its regulations as well as ensuring there is compliance with OH's policies, procedures and practices that have been implemented to protect the privacy of individuals and the confidentiality of their information (**Information Practices**). The Chair and the CEO have delegated the day-to-day authority to manage the privacy program to the CPO. The CPO reports to the General Counsel and Executive Lead, Legal Privacy and Risk.

The CPO oversees the responsibilities of the privacy program and has dedicated staff to whom specific obligations may be assigned to. These responsibilities include the management of Privacy Incidents, privacy risks, Privacy Complaints, Privacy Inquiries, access and correction requests, and requests to implement consent directives. The CPO also has oversight of privacy impact assessments (**PIAs**), privacy controls, privacy policies and procedures, privacy audit and compliance activities, and the privacy training and awareness program. The CPO is supported by the Digital Excellence in Health Executive, who has authority to manage the OH security program and provides oversight for information security at OH. More information on OH's information security program, including the governance structure, is set out in the OH *Information Security Program Governance*.

The CPO provides the Senior Leadership Team (**SLT**), the CEO, and the Board with relevant information on material privacy matters, including updates on the status of the privacy program, significant or high-risk Privacy Breaches, privacy audit reports, new privacy legislative, regulatory and industry developments of note; the status of the IPC's triennial review; and any resulting recommendations. These updates may be ad hoc or occur through formal board committees. The CPO briefs SLT through the Annual Privacy Report as well as ad-hoc updates as required. The governance of the Privacy Program is further set out in the *Privacy Governance and Accountability Framework.*

OH is and remains responsible for the protection of PHI and PI that is Collected, received, viewed, Used, Disclosed, handled or otherwise dealt with by Employee(s) and other OH Agents, including Third-Party Service Providers who are permitted to handle PHI or PI on OH's behalf. OH uses contractual or other means, to ensure that a comparable level of protection is applied when PHI or PI is handled by Third-Party Service Providers.

3.2 Identifying Purpose(s)

> The principle of identifying purpose means the purposes for which PHI and PI is Collected shall be identified by the organization at or before the time the information is Collected.

OH documents the purposes for which it receives PHI and PI at or before the time of receipt. OH will only accept PHI or PI as permitted by applicable legislation.

OH's authority for the Collection and receipt of PHI and PI is generally derived from legislation including the CCA*, Gift of Life Act* and PHIPA, as well as documented arrangements with the Ministry of Health (**MOH**) to support both the MOH and OH's objectives. For more information on OH's authority to Collect and receive PHI, see Appendix A.

OH consults and has agreements with organizations that provide PHI and PI to OH for these purposes and encourages and supports these organizations in making the purposes known to individuals to whom the PHI and PI relates.

3.3 Knowledge and Consent

> The principle of knowledge and consent means that the knowledge and consent of the individual are required for the Collection, Use or Disclosure of PHI and PI, except when inappropriate.

When PHI and PI is Collected by or on behalf of OH, OH will inform the individual, subject to exceptions that are set out in applicable legislation, of:

- The purpose of Collection;
- The authority for the Collection; and
- The contact information of someone who can respond to inquiries about the Collection.

Where required by applicable legislation, OH will obtain consent from individuals for the Collection, Use or Disclosure of their PHI and PI. The consent will:

- Be knowledgeable, transparent and meaningful;
- Relate to the information Collected, Used or Disclosed; and
- Be obtained without deception or coercion.

3.3.1 Consent Management in respect of the EHR

OH provides, through its website, information as to how an individual can withhold or withdraw consent to the full or partial Collections, Uses and Disclosures of his/her PHI made available through the EHR. On the OH website, the *EHR Consent Directive Request Form* details the instructions for individuals to manage their consent, including contact information (email, mail, phone, person responsible) for submitting the Form and information on the level of specificity at which PHI may be made subject to a consent directive, including whose Collection, Use and Disclosure of the PHI may be restricted.

More information on consent management in respect of the EHR is documented in the *EHR Consent Directive and Consent Override Policy.* This Policy specifies the data elements that a HIC may Collect, Use or Disclose for the purposes of uniquely identifying an individual in order

to Collect PHI by means of the EHR. These specific data elements may not be subject a to a consent directive provided by an individual.

3.3.2 Consent Management as an IT Service Provider

OH, when providing IT services or systems to HICs, for example as a HINP or ESP, may assist HICs in meeting their consent obligations under PHIPA. For example, depending on the IT system and OH's agreement with the relevant HIC, OH may provide mechanisms for HICs to implement a consent request or remove a patient's record from the IT system.

3.4 Limiting Collection:

> The principle of limiting Collection means that the Collection of PHI and PI shall be limited to that which is necessary for the purposes identified by the organization. PHI and PI shall be Collected by fair and lawful means.

OH limits the Collection and receipt of PHI and PI to that which is permitted by applicable legislation. OH does not Collect or receive PHI or PI if other information such as De-identified and/or Aggregate Data will serve the purpose and is committed to and takes reasonable steps to limit the PHI and PI it Collects and receives to that which is reasonably necessary for the authorized purpose. These steps include implementing Information Practices in respect of:

- Entering into agreements with data contributors to set out the minimum elements of PHI and PI required for the identified purpose, including as set out in the *EHR Policy for Receiving PHI*;
- Conducting PIAs to review the PHI and PI to be Collected or received against the identified purpose in accordance with the *PIA Standard*;
- Reviewing the list of data elements with the data contributor to identify what elements of PHI and PI are required to meet the identified purpose; and
- Conducting data assurance activities to validate that the PHI and PI Collected and received by OH matches the intended data transfer set out in relevant agreements.

3.5 Limiting Use, Disclosure, Retention:

> The principle of limiting Use, Disclosure and Retention means that PHI and PI shall not be Used or Disclosed for purposes other than those for which it was Collected, except with the consent of the individual or as required by law. PHI and PI shall be retained only as long as necessary for fulfilment of those purposes.

3.5.1 Limiting Use and Disclosure

OH only Uses or Discloses PHI and PI where permitted by applicable law, including FIPPA, PHIPA, the *Gift of Life Act* and the CCA. OH does not Use or Disclose PHI or PI if other

information, such as De-identified and/or Aggregate Data will serve the purpose, and does not Use or Disclose more PHI or PI than is reasonably necessary to meet the purpose.

For example, OH may Use and Disclose PHI or PI for the following purposes[3]:

- OH may Use PHI that OH Collected as a Prescribed Entity for the purposes of planning, management and analysis of the health system;
- OH may Use and Disclose PHI that OH Collected as a Prescribed Person to maintain the Ontario Cancer Screening Registry registries for the purpose of facilitating or improving the provision of health care;
- OH may Use PHI received as a Prescribed Organization for the purposes of developing and maintaining the EHR;
- OH will Disclose PHI pursuant to a direction issued by the Minister of Health (**Minister**):
    - Requiring OH to provide to the Minister, PHI that is accessible by means of the EHR that the Minister is permitted to Collect under subsection. 55.9 (1) of PHIPA; OH must comply with such a direction[4]; and
    - Directing the Disclosure of PHI, under ss. 55.10 of PHIPA, that is accessible by means of the EHR, as if the Minister had custody and control of the information, in accordance with s. 39(1)(c), s. 39(2), s. 44 or s. 45 of PHIPA. OH must comply with the direction. A direction of the Minister may specify the form, manner and timeframe in which the PHI that is the subject of the direction is to be provided to the Minister or Disclosed;
- OH may use PHI that it receives as a HINP or ESP to provide electronic information services to a HIC.

OH has in place controls to limit the Use and Disclosure of PHI/PI. These controls include:

- Securely destroying PHI and PI that is no longer required by OH;
- Limiting employee(s) or other OH Agent's access to PHI, PI and IT systems (e.g. EHR) to only those who require authorized access;
- Implementing role-based access controls based on responsibilities required by employee(s) and other OH Agents to fulfill the requirements of their job;
- In accordance with the *Privacy Use and Disclosure Policy*, Employee(s) and other OH Agents are not permitted to view, access, Use, handle, Disclose or otherwise deal with PHI or PI until they have agreed to comply with the restrictions that apply to OH and have agreed not to Use or Disclose PHI or PI if De-identified or Aggregate Data will serve the purpose; and
- In accordance with the *Confidentiality Agreement Policy*, OH requires all Employee(s) and other OH Agents to sign a confidentiality agreement that binds the individual to the stated restrictions before he/she gets access to PHI or PI, and annually thereafter.

---

[3] Additional permitted uses are set out in PHIPA and its regulation. For more information, see the OH *Prescribed Entity and Prescribed Statement of Information Practices*, and the OH *EHR Statement of Information Practices*.

[4] The Minister may only collect the PHI from the EHR in accordance with s. 55.9(1) of PHIPA.

3.5.2 Limiting Retention

OH retains PHI and PI only as long as necessary to fulfill the identified purposes for which it was Collected or received by OH.

- As a Prescribed Organization, the retention schedule of PHI that is accessible by means of the EHR is set out in the *EHR Retention Policy*, which includes information about whether the records are retained in identifiable form, the length of retention and the secure manner of retention.
- As an IT service provider (i.e., HINP or ESP), OH may retain the PHI as directed by HICs and set out under applicable agreements.
- As a Prescribed Entity, PHI may be retained to support retrospective analysis for the purposes of planning and management of the provincial healthcare system.
- As a Prescribed Person, PHI may be retained to support the Ontario Cancer Screening Program and other Prescribed Registries as applicable to OH.

3.6 Accuracy

> The principle of accuracy means PHI and PI shall be as accurate, complete, and up to date as is necessary for the purposes for which it is to be Used.

OH puts in place reasonable controls that ensure PHI and PI shall be as accurate, complete, and up to date as is necessary for the purposes for which it is to be Used.

This is achieved, for example, by:

- Providing mechanisms to organizations and individuals to support the accurate entry of PHI or PI into OH systems (such as data validation controls);
- Validating the information has been provisioned or Disclosed to OH in accordance with data standards and specifications; and
- Implementing safeguards to maintain the integrity of PHI and PI once the information has been Collected or received. Integrity means that the PHI or PI has not been altered inadvertently or improperly and can be relied upon for the purposes for which it was Collected or received.

3.7 Safeguards

> The principle of safeguards means that PHI and PI shall be protected by security safeguards appropriate to the sensitivity of the information.

OH has in place administrative, technical and physical safeguards to protect the privacy of individuals whose PHI and PI is received by OH, and the confidentiality of that information. These safeguards protect PHI and PI against loss, theft, unauthorized access, Disclosure, copying, Use, modification, retention or disposal, and they correspond to the sensitivity, amount and nature of the PHI and PI Collected or received. The following is a list of some of these safeguards.

3.7.1 Administrative Safeguards

- OH uses confidentiality agreements to reinforce OH Agents' understanding of the responsibility to protect PHI and PI.

- Third-party Service Providers are required to sign and adhere to an agreement prior to accessing PHI/PI. These agreements set out the requirements for the secure transfer of PHI and PI to the Third-Party Service Provider as required for the service, as well as the secure transfer and disposal of the PHI and PI once the agreement is terminated or as requested by OH;
- OH, when providing services as a HINP enters into a written agreement with each HIC that sets out required safeguards as well as restrictions related to OH's access and Use to PHI;
- OH notifies the applicable data providers (including HICs) at the first reasonable opportunity of any privacy breach related to PHI that OH receives as a PHIPA Agent, HINP, ESP, PO, PP or PE.
- OH conducts PIAs and threat risk assessments (**TRAs**), for example, when there are significant changes to the way PI/PHI is handled by OH.

3.7.2 Technical Safeguards

- OH adopts industry standards and tests its systems to ensure PHI and PI held by OH is secure.
- OH keeps electronic records of accesses and transfers of PHI.
- Records of PHI and PI no longer required to fulfill the identified purpose, are destroyed in a secure manner.
- OH uses encryption, for example, to protect PHI and PI during storage and transmission.

More information on the technical safeguards put in place by OH including the manner in which records Collected or received by OH are securely retained, transferred or disposed of, are found in OH security policies, including the *Media Destruction, Sanitization and Disposal Standard*, *Personal Health Information Handling Standard*, and the *Secure Transfer of Sensitive Information Standard*.

3.7.3 Physical Safeguards

- OH provides a secure physical environment for the equipment on which PHI or PI is stored and for Employee(s) and OH Agents who Use PHI or PI.
- OH puts in place reasonable controls to:
    - Secure the physical premises;
    - Controlled access to OH offices;
    - Provide employees and other OH Agents with appropriate identification;
    - Screen visitors and verify that they are authorized to be on the premises; and
    - Implement and monitor video surveillance for forensics purposes.
- Some operational areas which process PHI or PI may require restricted access with a secondary level of access controls.

More information about OH's safeguards is set out in OH's security policies and procedures.

3.8 Openness

> The principle of openness means that an organization should be open about its PI and PHI policies and practices. Individuals should be able to access an organization's policies and practices relatively easily.

OH has a responsibility to be open and transparent about how it manages and protects PHI and PI and to inform individuals of their privacy rights. Through its website, OH makes the following information available to the public and other stakeholders (including HICs that contribute PHI to the EHR), to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information:

- Information about its policies and practices relating to the management and handling of PHI and PI;
- A plain language description of the EHR, including a general description of the safeguards in place, Information Practices that apply to the PHI that is accessible by means of the EHR, and a list of the types of PHI that are accessible by means of the EHR;
- For each system that retrieves, processes, or integrates PHI that is accessible by means of the EHR, and for services that OH provides as a HINP:
    - A written copy of the results of assessment with respect to the threats, vulnerabilities and risks to the security and integrity of the PHI that is accessible by means of the EHR or service; and
    - How each system, EHR, or service may affect the privacy of the individuals to whom the information relates;
- The email and mailing address to use to gain further information regarding OH's Information Practices.

3.9 Individual Access

> Upon request, an individual shall be informed of the existence, Use and Disclosure of his or her PHI and PI and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Pursuant to FIPPA, an individual can request access and correction to records of his or her PI in the custody or under the control of OH (including PHI collected by OH as a Prescribed Person and Prescribed Entity). OH provides the public with the contact information and instructions on how to make a FIPPA request on OH's public website. OH will receive and process such requests in accordance with requirements set out in FIPPA.

3.9.1 Managing Access and Correction Requests in Respect of the EHR

As a Prescribed Organization, OH has put in place processes approved by the MOH to facilitate HICs in responding to a request made by an individual to a HIC under Part V of PHIPA to access or correct a record of the individual's PHI that is accessible by means of the EHR. For more information about these processes, see OH's *Electronic Health Record Request for Access to PHI Policy and Procedure* and *Electronic Health Record Request for Correction to Personal Health Information Policy and Procedure.*

3.9.2 Managing Access and Correction Requests as a Service Provider

OH, when providing services or systems to HICs or other individuals (i.e., direct to consumer services), may accept and manage access and corrections requests from individuals as permitted by PHIPA, including for example on behalf of HICs. More information on OH's access and correction processes can be found on OH's privacy website or by contacting the HIC's administrator in respect of a specific information system.

3.10 Challenging Compliance

> The principle of challenging compliance means an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Individuals may submit an inquiry, concern, or complaint regarding OH's Information Practices, its compliance with PHIPA or FIPPA, the types of PHI or PI Collected or received by OH, or the purposes for which PHI or PI is Collected, received, Used, Disclosed, handled or otherwise dealt with by OH. Individuals may also make inquiries, concerns and complaints related to the information practices of a HIC and a HIC's compliance with PHIPA in respect of the EHR.

They can do so by writing to:

Chief Privacy Officer

Legal, Privacy, Risk Department, Ontario Health

525 University Avenue, 5th Floor

Toronto, ON M5G 2L7

privacy@ontariohealth.ca

Should a request be best handled by a HIC (for example, requests related to a HIC's information practices), OH will redirect the individual's request to the appropriate HIC(s) and inform the individual of such action.

A person may also submit a concern or complaint regarding i) the compliance of OH or a HIC with PHIPA or FIPPA and its regulations, or ii) access and correction requests for PHI/PI, 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

Email: info@ipc.on.ca

Toronto Area: 416-326-3333
Long distance: 1-800-387-0073
TDD/TTY: 416-325-7539

4 Responsibilities

4.1 Board of Directors

The Board of Directors is responsible for approving this Policy.

4.2 Chair of the Board of Directors

The Chair of the Board of Directors is accountable for OH's compliance with FIPPA and subject to any delegations, is responsible for ensuring that there are proper governance mechanisms and controls in place to ensure compliance with this Policy.

4.3 Chief Executive Officer (CEO)

The CEO is accountable for OH's compliance with PHIPA and subject to any delegations, is responsible for ensuring that there are proper mechanisms and controls in place to ensure compliance with this Policy.

4.4 Chief Privacy Officer (CPO)

The CPO is responsible for:

- Maintaining this policy and ensuring that employees and other OH Agents are aware of its requirements.
- Overseeing compliance with any part of this policy, and the Information Practices that support it.
- Overseeing day-to-day management of the privacy program, and for monitoring compliance with this Policy and the Information Practices that support it.

4.5 Managers/Supervisors

Managers and Supervisors are responsible for ensuring that, within their areas of responsibility, all employees and other OH Agents are aware of and comply with this policy and the Information Practices that support it.

4.6 Employees and other OH Agents

Employees are responsible for compliance with this Policy and the Information Practices that support it.

5 Definitions and Acronyms

Defined terms are capitalized throughout this document.

Term / Acronym	Definition
Aggregate Data	Data that is summed and/or categorized in a manner that prevents the ability to reveal an individual's identity (individual records cannot be reconstructed). Aggregate data does not include PHI or PI.
CCA	*Connecting Care Act, 2019 and the regulations thereunder, as may be amended or relaced from time to time.*
CEO	Chief Executive Officer
Collect	Has the meaning set out in section 2 of PHIPA with respect to PHI; and in respect of PI has the same meaning. "Collect" means to gather, acquire, receive, or obtain the information by any means from any source, and "Collection" and "Collected" has a corresponding meaning.
Consent Directive	Means a directive, made in accordance with s. 55.6 of PHIPA, that withholds or withdraws, in whole or in part, an individual's consent to the Collection, Use and Disclosure of their PHI by means of the EHR by a HIC for the purposes of providing or assisting in the provision of health care to the individual.
CPO	Chief Privacy Officer
De-Identification	Has the meaning set out in s. 47(1) of PHIPA with respect to PHI; and in respect of PI has the same meaning. "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 Data	Data which has any information that identifies the individual removed. It is not reasonably foreseeable in the circumstances that the data could be utilized, either alone or with other information, to identify an individual.
Disclose	Has the meaning set out in s. 2 of PHIPA with respect to PHI in the control of a HIC or a person; and in respect of PI has the same meaning. "Disclose" means to make the information available or to release it to another HIC or to another person, but does not include to Use the information, and "Disclosure" has a corresponding meaning.

Term / Acronym	Definition
EHR or Electronic Health Record	Has the meaning set out in s. 55.1 of PHIPA and generally means the electronic systems that are developed and maintained by OH pursuant to Part V.1 of PHIPA for the purpose of enabling HICs to Collect, Use and Disclose PHI by means of the systems.
Employee	A person employed and compensated by OH as an Employee, and is classified as either permanent full-time, permanent part-time, temporary full-time, temporary part-time, paid student or casual, as set out in the *Employee Classification Guideline*. A consultant or contractor is not an Employee.
ESP or Electronic Service Provider	A Third-Party Service Provider contracted or otherwise engaged to provide services for the purpose of enabling the use of electronic means to Collect, Use, modify, Disclose, retain or dispose of records of PHI.
FIPPA or *Freedom of Information and Protection of Privacy Act,1990*	Ontario 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 include the regulations made thereunder, as may be amended or replaced from time to time.
FIPs	Fair Information Privacy Principles that were established from the *Canadian Standard Association Model Code for the Protection of Personal Information.*
HIC or Health Information Custodian	Has the meaning set out in s. 3 of PHIPA and generally means a person or organization that has custody or control of personal health information for the purpose of health care or other health-related duties. Examples include physicians, hospitals, pharmacies, laboratories and the MOH, but does not include OH.
HINP or Health Information Network Provider	Has the meaning set out in s. 6(1) of Ontario 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.
Information Practices	OH's policies, procedures and practices put in place to protect the privacy of individuals and the confidentiality of their information.
IPC	Information and Privacy Commissioner of Ontario
Minister	Minister of Health
MOH	Ontario Ministry of Health
O. Reg. 329/04	Ontario Regulation 329/04 made under PHIPA
OH	Ontario Health, the agency of the Government of Ontario to which this Policy applies.

Term / Acronym	Definition
OH Agent	A person that acts for or on behalf of OH for the purposes of OH, and not for the Agent's own purposes, whether or not the Agent has the authority to bind OH, whether or not the Agent is employed by OH, and whether or not the Agent is being remunerated.
PHI or Personal Health Information	Has the meaning set out in s. 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.
PHIPA or *Personal Health Information Protection Act, 2004*	The Ontario health privacy law. It establishes rules for the management of PHI and the protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services. References to PHIPA include the regulation made thereunder, as may be amended or replaced from time to time.
PHIPA Agent	In relation to a HIC, means a person that, with the authorization of the HIC, acts for or on behalf of the custodian in respect of PHI for the purposes of the HIC, and not the agent's own purposes, whether or not the agent has the authority to bind the HIC, whether or not the agent is employed by the HIC and whether or not the agent is being remunerated.

Term / Acronym	Definition
PI or Personal Information	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.
PIA	Privacy Impact Assessment.
Prescribed Entity or PE	An entity that is prescribed in Ontario Regulation 329/04 for the purposes of s. 45 of PHIPA, to which a HIC is permitted to Disclose PHI, without the consent of the individual to whom the information relates, 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.
Prescribed Organization or PO	The organization prescribed in Ontario Regulation 329/04 as the organization for the purposes of Part V.1 of PHIPA. The Prescribed Organization has the power and the duty to develop and maintain the EHR in accordance with Part V.1 of PHIPA and the regulations made thereunder.
Prescribed Person or PP	A person that is prescribed in the regulations for the purposes of s. 39(1)(c) of PHIPA, to which a HIC is permitted to Disclose PHI, without the consent of the individual to whom the information relates, 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.
Prescribed Registry or PR	A registry of PHI that is prescribed in Ontario Regulation 329/04 maintained for the purpose of enabling or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances.

Term / Acronym	Definition
Privacy Breach	An event or series of events where one or more of the following occurs: • Collection, Use or Disclosure of PHI or PI not in compliance with PHIPA or its regulation, or with FIPPA or its regulations (i.e. without legal authority); • There is a contravention of OH's privacy policies, procedures or practices; • There is a contravention of data sharing agreements, research agreements, confidentiality agreements or agreements with third party service providers retained by OH, including written acknowledgements acknowledging and agreeing not to use PHI or PI which has been de-identified and/or aggregated, to identify an individual; or • Where PI or PHI is stolen, lost or subject to unauthorized Collection, Use or Disclosure or where records of PHI or PI are subject to unauthorized copying, modification or disposal.
Privacy Complaint	Concerns or complaints relating to: • The privacy policies, procedures and practices implemented by OH and OH's compliance under PHIPA, FIPPA and associated regulations; and • Compliance of a HIC with PHIPA and its regulation in respect of PHI that is accessible by means of the EHR developed or maintained by OH.
Privacy Incident	A real or suspected Privacy Breach.
Privacy Inquiry	Inquiries relating to: • The privacy policies, procedures and practices implemented by OH and OH's compliance under PHIPA, FIPPA and related regulations; and • Inquiries relating to the privacy policies, procedures and practices of a HIC, or the compliance of a HIC with PHIPA and its regulation, in respect of PHI that is accessible by means of the EHR developed or maintained by OH.
SLT	Senior Leadership Team
Third-Party Service Provider	A third-party contracted or otherwise engaged to provide services to OH, including Electronic Service Providers.
TRA	Threat Risk Assessment
Use	In relation to PHI or PI in the custody or under the control of a HIC or a person, "Use" means to view, handle or otherwise deal with the information, but does not include to Disclose the information, and "Use", as a noun, has a corresponding meaning. For the purposes of PHIPA, the providing of PHI between a HIC and an agent of the HIC is a Use by the HIC, and not a Disclosure by the person providing the information or a Collection by the person to whom the information is provided

6 Review Cycle

This Policy is to be reviewed at least within 3 years of its effective date or earlier if required in accordance with the *Privacy Audit and Compliance Policy*.

7 References and/or Key Implementation Documents

- PHIPA, FIPPA, CCA and *Gift of Life Act*
- Manual for the Review and Approval of Prescribed Persons and Prescribed Entities
- Manual for the Review and Approval of Prescribed Organizations
- Privacy Audit and Compliance Policy
- Privacy Incident Management Policy and Procedure
- Privacy Use and Disclosure Policy
- Confidentiality Agreement Policy
- PIA Standard
- Information Security Program Governance
- Information Security Policy
- Privacy Governance and Accountability Framework
- EHR Consent Directive Form
- EHR Consent Directive and Consent Override Policy
- EHR Retention Policy
- EHR Statement of Information Practices
- EHR Request for Access to PHI Policy and Procedure
- EHR Request for Correction to Personal Health Information Policy and Procedure
- EHR Policy for Receiving PHI

8 Policy Consultations

The following were consulted in the development of this Policy:

- General Counsel and Executive Lead, Legal Privacy and Risk
- Staff from the Privacy Office and other OH Agents, including the CPO and employees and contractors responsible for drafting, maintaining and/or reviewing the privacy policies in reference to OH's privacy requirements.
- Working Group members of the Privacy Program Advisory Committee

9 Policy Review History

Date of Review MM/YYYY	Itemize section changed and description of change (if no changes made, indicate N/A	New policy number	Date of Approval DD/MM/YYYY	Approver

10 Policy Repeal

1) Date of Repeal:
2) Reason for Repeal:
3) Date of Approval of Repeal:
4) Approver:

Appendix A: Description of OH Status under PHIPA

A Prescribed Organization

OH has the status as a 'Prescribed Organization' under s. 18.1 of O. Reg. 329/04 for the purposes of Part V.1 of PHIPA. Under s. 55.2 (1) of the PHIPA, the Prescribed Organization:

- Has the power and the duty to develop and maintain the EHR in accordance with Part V.1 of the PHIPA and the regulations in O. Reg. 329/04 made under Part V.1; and
- Has the authority to receive PHI from HICs for the purpose of developing and maintaining the EHR.

As a Prescribed Organization, OH shall perform the following functions:

- Manage and integrate PHI it receives from HICs;
- Ensure the proper functioning of the EHR by servicing the electronic systems that support the EHR;
- Ensure the accuracy and quality of the PHI that is accessible by means of the EHR by conducting data quality assurance activities on the PHI it receives from HICs; and
- Conduct analyses of the PHI that is accessible by means of the EHR in order to provide alerts and reminders to HICs for their use in the provision of health care to individuals.

In addition to carrying out the powers, duties and functions described in this Part V.1 and V, OH shall carry out any prescribed powers, duties or functions under PHIPA and O. Reg. 329/04.

For a description and list of the types of PHI received by OH for the purposes of developing and maintaining the EHR, see OH's *EHR Plain Language Description and List of EHR Repositories*.

Prescribed Entity

OH has the status as a 'Prescribed Entity' under s. 18(1) of O. Reg. 329/04 for the purposes of s. 45 of PHIPA. As a Prescribed Entity, OH may collect PHI without individuals' consent from HICs and use that information for analysis and compiling 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. Other permitted Uses and Disclosures are described in Part IV of PHIPA and its regulation.

For a list of the types of PHI that OH collects as a Prescribed Person or Prescribed Entity see OH's *Prescribed Entity and Prescribed Person Data Asset List*.

A Prescribed Person

OH also has the status as a 'Prescribed Person' under PHIPA with respect to OH's role in compiling and maintaining the Prescribed Registry - the Ontario Cancer Screening Registry

(**OCSR**) as part of Ontario's Cancer Screening Program (**CSP**)[5]. This designation grants OH the authority to Collect, Use and Disclose PHI, without consent, for the purpose of facilitating or improving the provision of healthcare under s. 39(1)(c) of PHIPA. Other permitted uses and disclosures are described in Part IV of *PHIPA* and its regulation.

For a list of the types of PHI that OH collects as a Prescribed Person or Prescribed Entity see OH's *Prescribed Entity and Prescribed Person Data Asset List*.

Information Practices implemented as a Prescribed Entity, Prescribed Person and Prescribed Organization

As a Prescribed Entity, Prescribed Person and Prescribed Organization, OH has in place practices and procedures to protect the privacy of the individuals whose PHI it receives under these designations and to maintain the confidentiality of the information. These Information Practices are designed to be compliant with the IPC's *Manual for the Review and Approval of Prescribed Organization* (which applies only to OH's role as a Prescribed Organization as that term is defined in s. 2 of the PHIPA) as well as the IPC's *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (which applies to OH's role as Prescribed Person and Prescribed Entity). These Information Practices are subject to review by the IPC every three years.

When OH engages in activities or roles that are otherwise regulated by PHIPA, it has appropriate policies and procedures in place that address the requirements of those other activities and roles.

A Researcher

OH 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 Person, OH can Collect, Use or Disclose PHI as if it were a HIC for the purposes of research.

A Health Information Network Provider (HINP)

OH provides information systems to HICs to enable them to exchange PHI with each other. In providing such services, OH is acting as a HINP and is subject to additional privacy requirements under O. Reg. 329/04.

[5] It is expected that CorHealth will transfer to OH, at which time OH will also be a Prescribed Person in respect of its registry of cardiac and vascular services.

A PHIPA Agent

An Agent under PHIPA, is a person that, with the authorization of HIC, acts for or on behalf of the HIC in respect of PHI for the purposes of the HIC, and not the Agent's own purposes, whether or not the Agent has the authority to bind the HIC, whether or not the Agent is employed by the HIC, and whether or not the Agent is being remunerated. OH may act as a PHIPA Agent, if OH is authorized to do so by the HIC for purposes, for example, of responding to access and correction requests.

An Electronic Service Provider (ESP)

OH provides information technology services to healthcare providers to enable them to Collect, Use, modify, Disclose, retain or dispose of PHI, or to exchange PHI with each other. In providing these services OH act as an ESP pursuant to PHIPA regulations. This ESP role strictly limits OH's use of PHI to only that which support health care providers.