Protection of Personal Health Information Policy

April 2020

Contents

1 Purpose

Using data and evidence as the foundation for all our decision making, CorHealth Ontario (CorHealth) proudly advises the Ministry of Health (MOH), Local Health Integration Networks (LHINS), hospitals, and care providers to improve the quality, efficiency, accessibility, and equity of cardiac, stroke, and vascular services for patients across Ontario.

CorHealth is subject to Ontario's health information privacy legislation, the Personal Health Information Protection Act, 2004 (PHIPA). 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)[1]. 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.

CorHealth's Protection of Personal Health Information Policy is based on this model, reflects PHIPA and its regulation, and sets out the principles CorHealth follows to protect the privacy of individuals whose personal health information (PHI) is received by CorHealth as a s. 39(1)(c) Prescribed Person under PHIPA.

CorHealth is committed to complying with PHIPA and its regulation, and fostering trust and confidence with the government, the healthcare system, and the public. This Policy is implemented throughout CorHealth to ensure all agents of CorHealth understand and apply these mandatory requirements and responsibilities in their daily work.

CorHealth 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.

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

2 Status Under PHIPA

As a Prescribed Person within the meaning of subsection 39(1) (c) of the *Personal Health Information Protection Act, 2004*, CorHealth is permitted to collect, use, and disclose personal health information, without consent, for purposes of facilitating or improving the provision of cardiac and vascular care services. In particular, CorHealth uses personal health information, in its registry of cardiac and vascular services, to monitor and manage the health status of patients who are waiting to access advanced cardiac and vascular services, and for service evaluation and planning to improve the provision of cardiac and vascular services in the province.

3 Scope

This Policy applies to CorHealth, and all its agents, in respect of CorHealth's role as a s. 39(1)(c) Prescribed Person under PHIPA, as well as to the data holdings, the CorHealth Cardiac and Vascular Registry (Registry), which CorHealth operates in this role.

CorHealth's Protection of Personal Health Information Policy complies with PHIPA. If there is a discrepancy between the Policy and PHIPA, PHIPA takes precedence.

This Policy is supported by other CorHealth privacy and security policies, standards, and procedures which are part of a comprehensive program for the protection of PHI. These policies include, but are not limited to:

- Limiting Collection of Personal Health Information;
- Information Security and Privacy Breach Management;
- Privacy Impact Assessment (PIA);
- Privacy Inquiries and Complaints; and
- Integrated Risk Management (IRM) Program.

4 Policy

4.1 Principle 1: Accountability

The principle of accountability means an organization is responsible for PHI under its control and has designated an individual or individuals to be accountable for the organization's compliance with privacy principles and the management of PHI; this includes the collection, use, disclosure, retention, transfer, and destruction of PHI.

CorHealth's Chief Executive Officer (CEO) is ultimately accountable for the protection of PHI in CorHealth's custody or control, ensuring compliance with PHIPA, and for ensuring compliance with the privacy and security policies, procedures, and practices implemented by CorHealth.

The day-to-day responsibility for ensuring PHI is collected, used, and disclosed in accordance with CorHealth's privacy policies and procedures, and in compliance with PHIPA, has been delegated to the Privacy Officer for privacy and the Chief Digital Officer (CDO) for security, who report to the CEO.

CorHealth uses contractual means to ensure PHI in its custody or control is collected, used, and disclosed in accordance with PHIPA, and is protected from theft, loss, and unauthorized use or disclosure. In particular, CorHealth requires its agents sign the Confidentiality & Non-Disclosure Agreement which clearly states their obligations with respect to protecting the confidentiality of PHI, and protecting the privacy of individuals with respect to that information. CorHealth further requires consultants, contractors, and vendors to sign agreements outlining their obligations to protect PHI.

The Privacy Officer is responsible for ensuring hospitals have signed Participation Agreements. Hospitals that provide PHI to CorHealth, pursuant to Participation Agreements, are responsible for the PHI they collect, while CorHealth is responsible for the PHI it receives from hospitals.

4.2 Principle 2: Identifying Purposes

The principle of identifying purposes means an organization must clearly identify the purposes for which PHI is collected, either at or before the time of collection.

It is the responsibility of the health information custodian (HIC) who collects PHI to inform the patient of the purposes for which the PHI will be collected, used, and disclosed.

Via front-line healthcare providers, CorHealth identifies to patients the purposes for which PHI is collected proximate to the time the PHI is collected. Each patient registered in the Registry is provided an information brochure specifying the purposes for which PHI is being collected. This information brochure is available on the CorHealth website, www.corhealthontario.ca.

CorHealth uses identifiable health information to:

- Facilitate access to care and treatment;
- Facilitate continuous improvement of screening thresholds to minimize missed cases;
- Identify strategies to improve the quality and efficiency of care for patients receiving cardio-vascular treatments;
- Create reports that can be used to provide the MOHTLC, LHINs and Public Heath Units with comprehensive and timely information to support effective planning and management of health care; and
- Maintain waiting lists for treatment.

The types of PHI collected include the minimum required to fulfill the stated purposes, including but not limited to:

- Name, middle name, and surname;
- Date of birth;
- Sex;
- OHIP number;
- Chart and/or medical record numbers;
- Medical report numbers and/or specimen accession numbers; and
- Address, city/town, province, postal code, telephone number.

As set out in CorHealth's policy, Statements of Purpose for Data Holdings Containing Personal Health Information, CorHealth maintains a list of data holdings containing PHI, and the purpose for which CorHealth collects PHI, for each of its data holdings; this list, is available on the CorHealth website, www.corhealthontario.ca.

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

The principle of consent means the knowledge and consent of the individual are required when an organization collects, uses, or discloses PHI.

CorHealth acknowledges patients in its Registry are entitled to receive information to allow them to understand the purposes of the Registry. Via front-line healthcare providers, CorHealth provides notice to patients about its collection, use, and disclosure of PHI through a patient brochure. The brochure is to be provided to each patient whose PHI is collected for CorHealth's Registry, specifying the purpose for which PHI is being collected. This information brochure is available on the CorHealth website, www.corhealthontario.ca.

As a Prescribed Person within the meaning of subsection 39(1) (c) of the *Personal Health Information Protection Act, 2004*, CorHealth is permitted to collect, use, and disclose PHI, without consent, for purposes of facilitating or improving the provision of cardiac and vascular care services.

4.4 Principle 4: Limiting Collection of PHI

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

CorHealth limits the collection of PHI to that which is necessary for the purposes it has identified, and in accordance with the requirements set out in PHIPA, and its regulation. CorHealth collects PHI by fair and lawful means.

CorHealth does not collect PHI where other information will suffice, and does not collect more PHI than is reasonably necessary to meet the identified purpose.

CorHealth has established policies, procedures, and practices, as set out in the Collection of Personal Health Information policy, to ensure the amount and type of PHI collected is limited to that which is reasonably necessary for its purpose, and to ensure each collection of PHI is permitted by PHIPA, and its regulation. The Privacy Officer ensures CorHealth only collects PHI that will be used in the manner prescribed by Sections 39 (1) (c) of PHIPA, and its regulation.

The Privacy Officer conducts a Privacy Impact Assessment (PIA) prior to any new collection of PHI, to ensure the amount and type of PHI collected is justified, and falls within the category of purposes set out in section 39 (1) (c) of the Act.

CorHealth uses identifiable health information to:

- Facilitate access to care and treatment;
- Facilitate continuous improvement of screening thresholds to minimize missed cases;
- Identify strategies to improve the quality and efficiency of care for patients receiving cardio-vascular treatments;
- Create reports that can be used to provide the MOH, LHINs and Public Heath Units with comprehensive and timely information to support effective planning and management of health care; and
- Maintain waiting lists for treatment.

The types of PHI collected include the minimum required to fulfill the stated purposes, including but not limited to:

- Name, middle name, and surname;
- Date of birth;
- Sex;
- OHIP number;
- Chart and/or medical record numbers;
- Medical report numbers and/or specimen accession numbers; and
- Address, city/town, province, postal code, telephone number.

During the annual review of CorHealth's privacy and security program, the Privacy Officer will, in cooperation with clinical and/or IT staff, review the elements of PHI collected by CorHealth to ensure it is minimal in scope.

The Privacy Officer must ensure publication of a list of CorHealth data holdings on the CorHealth website, www.corhealthontario.ca, together with a mechanism to allow individuals to request more detailed information, including purposes, data elements, and data sources for each data holding of PHI.

4.5 Principle 5: Limiting Use, Disclosure, and Retention of PHI

The principle of limiting use, disclosure, and retention means an organization shall not use or disclose PHI for purposes other than those which it has identified purposes for, except with the consent of the individual or as required by law.

4.5.1 Use of PHI

CorHealth only uses PHI for the purposes of facilitating or improving the provision of cardiac and vascular care services, namely to maintain wait lists for cardiac and vascular care services and to assist in the management and planning of the delivery of cardiac and vascular care services in Ontario, and as permitted or required by law, including PHIPA.

CorHealth permits its agents to access and use PHI only when access is required for the purpose of their employment, contractual, or other relationship with CorHealth. CorHealth agents are not permitted to use any identifiable PHI if de-identified or aggregate information will suffice. CorHealth distinguishes between the use of PHI and the use of de-identified and/or aggregate information, and between the use of PHI for purposes of subsection 39(1) (c) and those used for research.

CorHealth remains accountable for PHI used by its agents. The CorHealth policy, Limiting Agent Access to and Use of Personal Health Information Policy, sets out further procedures for ensuring there are limits and restrictions on agent access and use of PHI.

4.5.2 Disclosure of PHI

CorHealth limits disclosure of PHI to other prescribed registries and prescribed entities, and when permitted or required by law. Disclosures are made only as permitted by PHIPA, and section 18(4) of its regulation, data sharing agreements, and verified through a PIA. Excluding these identified purposes, CorHealth prohibits the disclosure of PHI.

The Privacy Officer reviews all de-identified and/or aggregate information prior to its disclosure to ensure it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual, and to ensure CorHealth only discloses PHI when other information will not serve the purpose, and discloses no more PHI than is reasonably necessary to meet the identified purpose. The CorHealth policies, Aggregation and De-identification of Record Level Data and Disclosure of Aggregate and/or De-identified Personal Health Information to Researchers, sets out further procedures for ensuring limits and restrictions on the disclosure of PHI.

4.5.3 Secure Retention, Transfer, and Destruction of PHI

PHI is retained by CorHealth only as long as is necessary to fulfill the identified purposes of the data holding and in accordance with PHIPA. Generally, given CorHealth's role as a Prescribed Person, PHI will be retained long-term to support retrospective analysis for the purposes for which it was collected.

CorHealth provides the following general restrictions on retention:

- Retention of de-identified or aggregate information only if it will serve the purpose;
- De-identification to the fullest extent possible;
- Agents are prohibited from retaining more PHI than is reasonably necessary for the identified purpose;
- Use of encryption and complex passwords in accordance with CorHealth's Password Policy, and responsibility of assigned IT staff for encryption;
- Password-protected screen savers and responsibility for enabling them;
- Shortest possible retention periods; and
- Second layer of encryption and different complex password at the file level.

PHI is retained in a secure location until the identified purpose for that data no longer exists, and then securely destroyed according to the procedures set out in CorHealth's policies, Secure Retention of Personal Health Information and Destruction of Personal Health Information.

CorHealth protects PHI in transit. Protections include an encrypted file transfer system for inbound and outbound electronic file transfers, and a requirement to remove direct personal identifiers before transferring the information.

All PHI, when no longer required for the identified purposes, must be destroyed in a secure manner in compliance with CorHealth's procedures for secure destruction of PHI. These procedures are set out in CorHealth's policy, Destruction of Personal Health Information.

4.6 Principle 6: Accuracy of PHI

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

The accuracy of PHI is the responsibility of the HIC who collects it. Any corrections or changes to PHI must be completed by the HIC.

Data quality checks are performed monthly to ensure data is accurate and up to date.

CorHealth, where possible, provides mechanisms to HICs to support the accurate entry of PHI into the Registry, such as data input validation controls. CorHealth maintains, through its information security practices, mechanisms to protect the integrity of PHI. CorHealth ensures the integrity of PHI sent by HICs is maintained and protected at rest and in transit. Integrity means the PHI has not been altered inadvertently or improperly and can be relied upon for the purposes for which it was collected.

4.7 Principle 7: Safeguards for PHI

The principle of safeguards means PHI shall be protected by security safeguards appropriate to the sensitivity of the information held. PHI shall be protected against loss or theft, unauthorized access, disclosure, copying, use or modification, regardless of what format it is stored in.

CorHealth protects PHI through administrative, physical, and technical safeguards.

4.7.1 Administrative Safeguards

CorHealth uses the Confidentiality & Non-Disclosure Agreement to ensure agents of CorHealth understand their responsibility to protect PHI, and to create a culture of privacy at CorHealth. All agents and contracted third-party service providers are required to comply with CorHealth's privacy and security policies, including, mandatory annual privacy and security training.

The Privacy Officer is responsible for ensuring data accessed by agents and third-party service providers is in compliance with CorHealth's privacy and security policies, and access to PHI is audited on a regular basis.

The Privacy Officer ensures there are processes in place to safeguard PHI, including:

- Appropriate privacy and security policies and procedures;
- Annual privacy and security training;
- Requiring CorHealth agents sign Confidentiality & Non-Disclosure Agreements which clearly state their obligations with respect to protecting the privacy of individuals with respect to PHI;
- Requiring Privacy Impact Assessments prior to any new collection of PHI;
- Requiring Participation Agreements to be executed prior to the collection of PHI; and
- Requiring Data Sharing Agreements to be executed prior to the disclosure of PHI.

CorHealth also has a comprehensive Integrated Risk Management (IRM) program to ensure privacy and security risks are identified, assessed, mitigated, monitored, and responsibly managed. The IRM program includes the use of a corporate risk register.

4.7.2 Physical Safeguards

CorHealth provides a secure physical environment for the equipment on which PHI is stored, and for the agents who use PHI. Physical safeguards include:

- CorHealth is located in a locked facility with external video monitoring;
- Tracked card access divides the facility into multiple levels of security with each successive level being more secure and restricted to fewer individuals; and
- Access to the server room requires individuals successfully pass through multiple levels of security.

4.7.3 Technical Safeguards

CorHealth adopts industry standards to ensure PHI in its custody, and the technical systems utilized by CorHealth, are secure. CorHealth's security policies and procedures specify the manner in which CorHealth protects PHI. Technical safeguards include:

- The use of firewalls, network encryption, and intrusion detection systems;
- An authenticated, secure network for transferring and accessing all CorHealth information;
- The encryption of all PHI being transferred to or from the CorHealth network;
- Workstations are encrypted and password protected for all CorHealth staff;
- A system-wide rule for password-protected screensavers to be activated after five minutes of user inactivity;
- Zoning network principles including a segregated public Wi-Fi network, Operation Zone, and Restricted Zone for servers and infrastructure;
- Self-updating anti-virus and anti-spam software installed on all staff workstations; and
- The implementation of firewalls to block unauthorized intrusions to CorHealth's network.

4.8 Principle 8: Openness about the Management of PHI

The principle of openness means an organization shall make its policies and procedures relating to the management of PHI readily available.

CorHealth makes available information about its policies and procedures relating to the management of PHI, including general information related to CorHealth's privacy practices, descriptions of CorHealth's data holdings of PHI, a patient brochure, which specifies the purpose for which PHI is collected, and contact information for the Privacy Officer. This information is available on the CorHealth website, www.corhealthontario.ca.

4.9 Principle 9: Individual Access to and Amendment of PHI

The principle of individual access means upon an individual's request, an individual shall be informed of the existence, use, and disclosure of their PHI, and shall be given access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Upon written request, an individual is informed of the existence, use, and disclosure of their PHI in the Registry. Contact information for making a request is available on the CorHealth website, www.corhealthontario.ca.

In particular, upon request, CorHealth informs an individual if it holds PHI about the individual, and seeks to indicate the source of this PHI. In addition, CorHealth provides, to the extent possible, an account of the use that has been made, or is being made, of this PHI, and an account of the third parties to which the PHI has been disclosed, if any.

The accuracy of PHI is the responsibility of the HIC who collects it. Any corrections or changes to PHI must be completed by the HIC. If CorHealth receives a correction request, it shall direct the individual to the appropriate HIC(s) to respond to the request.

4.10 Principle 10: Complaints or Inquiries About CorHealth's Handling of PHI

The principle of challenging compliance means an individual shall be able to address a complaint or inquiry related to an organization's compliance with PHIPA, and its regulation, and the organization shall have procedures in place to receive and respond to such complaint's or inquiries.

Any person may submit an inquiry, concern, or complaint regarding CorHealth's information practices, its privacy policies and procedures, its compliance with PHIPA, or the purposes for which PHI is collected to CorHealth's Privacy Officer; they can do so by contacting:

> Privacy Officer c/o CorHealth Ontario
> 4100 Yonge Street, Suite 502
> Toronto, ON M2P 2B5
> Phone: 416-514-7472
> Email: service@corhealthontario.ca

PHI should not be submitted with the description of an inquiry, concern, complaint, or any other feedback. CorHealth may, however, request this level of detail during its investigation. In doing so, CorHealth obtains the appropriate consent as required.

The Information and Privacy Commissioner of Ontario has jurisdiction over CorHealth's compliance with PHIPA. A person may also submit a concern or complaint to the IPC; they can do so by contacting:

> Information and Privacy Commissioner of Ontario
> 2 Bloor Street East, Suite 1400
> Toronto, ON M4W 1A8
> Toronto Area: 416-326-3333
> Long distance: 1-800-387-0073
> TDD/TTY: 416-325-7539
> Fax: 416-325-9195
> Email: info@ipc.on.ca

5 Glossary

The following terminology and acronyms are associated with this policy.

Term	Definition
Agent	Agent, as that term is defined in PHIPA, generally means any person who is authorized by CorHealth to perform services or activities on its behalf with respect to PHI for the purposes of CorHealth, and not the agent's own purposes, whether or not the agent has the authority to bind CorHealth, whether or not the agent is employed by CorHealth, and whether or not the agent is being paid by CorHealth. CorHealth agents could include: employees, volunteers, consultants, vendors, contractors, committee members, Board of Directors members, and any other person working on behalf of CorHealth.
Aggregate Data	Summed and/or categorized data that is analyzed and placed in a format that precludes further analysis to prevent the chance of revealing an individual's identify. Aggregate data does not include PHI.
Auditor	Person appointed to execute an audit; may be the Chief Privacy Officer and/or a delegate.
Collect	Collect, as that term is defined in PHIPA, generally means to gather, acquire, receive, or obtain PHI by any means from any source, and Collection has a corresponding meaning.
CorHealth	Short form of CorHealth Ontario.
Data Element	A category used to identify a data type.
Data Exchange	The disclosure of one or more Data Sets from CorHealth to an External Party, or the collection of one or more Data Sets by CorHealth from an External Party.
Data Holding	A full collection of data, categorized by data element, and relied upon to support specific purposes.
Data Holding List	A central, online repository which describes CorHealth Data Holdings.
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 (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 CorHealth to an External Party, or the collection of one or more Data Sets by CorHealth from an External Party.

Term	Definition
De-Identification	De-Identification, as that term is defined in PHIPA, generally 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.
Disclose	Disclose, as that term is defined in PHIPA, in relation to PHI in the custody or under the control of a HIC or a person, generally means to make the PHI 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.
External Party	(a) A person who has requested a Data Set from CorHealth for disclosure to the person; or (b) a person from which CorHealth has requested a Data Set, for collection by CorHealth.
Health Information Custodian (HIC)	Health Information Custodian (HIC), as that term is defined in PHIPA, generally means 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 homes; • Retirement homes and homes for special care; • Community access centres; • Ambulance services; and • Ministry of Health. CorHealth Ontario is not a HIC.

Term	Definition
Information and Privacy Commissioner of Ontario (IPC)	An oversight body responsible for educating the public concerning their rights under privacy legislation and ensuring that organizations fulfill their obligations under the legislation; the IPC plays a crucial role under PHIPA. 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.
Personal Health Information (PHI)	Personal Health Information (PHI), as that term is defined in PHIPA, generally means identifying information about an individual, whether oral or recorded, if the information relates to that person's health or health services provided to the individual. Identifying information includes information which identifies an individual, or for which it is reasonably foreseeable that it could be used, either alone or with other information, to identify an individual. Examples include family health history, health card number, and any information that identifies an individual and links them to a healthcare provider or substitute decision maker.
The Personal Health Information Protection Act, 2004 (PHIPA)	The Personal Health Information Protection Act, 2004, as amended from time to time. 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 amended from time to time.
PHIPA Regulation	The General Regulation under PHIPA, as amended from time to time

Term	Definition
Personal Information (PI)	Personal Information (PI), as that term is defined in PHIPA, generally 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 (PIA)	A detailed assessment undertaken to evaluate the effects of a new or significantly modified service to determine its actual and potential impact on the protection of PI/PHI included in the service. A PIA examines how PHI is collected, stored, used, and disclosed and assesses compliance with applicable privacy law and broader privacy implications. A PIA addresses technological components, business processes, flows of personal information, information management controls, and human resource processes associated with a service, and identifies ways in which privacy risks associated with these may be mitigated.
Prescribed Person	Meaning CorHealth Ontario's status under the PHIPA Regulation. As a Prescribed Person within the meaning of subsection 39(1) (c) of the *Personal Health Information Protection Act, 2004*, CorHealth Ontario is permitted to collect, use, and disclose personal health information, without consent, for purposes of facilitating or improving the provision of cardiac and vascular care services.
Registry	Short form for the CorHealth Cardiac and Vascular Registry

Term	Definition
Registry of cardiac and vascular services	Formal name of the data holding in the Regulation. Referred to as the CorHealth Cardiac and Vascular Registry.
Third-Party Service Provider	Consultants, contractors, and other service providers.
Use	Use, as that term is defined in PHIPA, in relation to PHI in the custody or under the control of a HIC or other person, generally means to handle or otherwise deal with PHI, but does not include to Disclose the information, and Use, as a noun, has a corresponding meaning.