CorHealth Ontario (formerly Cardiac Care Network) Report to the Information and Privacy Commissioner of Ontario

Three-Year Review as a Prescribed Person under PHIPA (2020)

Contents

1 Overview

Important: In 2016, the Cardiac Care Network of Ontario (CCN) and the Ontario Stroke Network merged to form one organization, with a mandate spanning cardiac, stroke, and vascular care in the province. On June 22, 2017, after a year of transition, the new entity became CorHealth Ontario. It is recognized that the Cardiac Care Network of Ontario is the designated organization in the legislation and hereafter will be referenced as CorHealth Ontario. CorHealth Ontario has requested that the Ministry of Health update the legislation to reflect the new name of the organization.

1.1 Background

CorHealth Ontario (CorHealth) serves as a system support to the Ministry of Health (MOH), Local Health Integration Networks (LHINs), hospitals, and care providers dedicated to improving quality, efficiency, access, and equity in the delivery of the continuum of cardiac, vascular, and stroke services in Ontario. CorHealth's priority is to ensure the highest quality of cardiovascular care, based on evidence, standards, and guidelines, and actively monitors access, volumes, and outcomes of advanced cardiac, vascular, and stroke procedures in Ontario, as well as procedures performed on Ontario residents in certain centres outside of Ontario. In addition, CorHealth works collaboratively with provincial and national organizations to share ideas and resources and co-develop strategies that enhance and support the continuum of cardiovascular care, including prevention, rehabilitation, and end-of-life care.

Working with key stakeholders, CorHealth helps to plan, coordinate, implement, and evaluate cardiovascular care and is responsible for the registry of cardiac and vascular services, referred to as the CorHealth Cardiac and Vascular Registry. The CorHealth Cardiac and Vascular Registry is designed to improve the provision of health care. The information collected in the CorHealth Cardiac and Vascular Registry includes wait time information as well as specific clinical parameters required to evaluate key components of care and determine risk-adjusted outcomes. Through scientific evidence, expert panels and working groups, CorHealth uses evidence and consensus driven methods to identify best practice and strategies to effectively deliver cardiovascular services, across the continuum of care.

CorHealth is a prescribed person within the meaning of section 39(1)(c) of Personal Health Information Protection Act, 2004 (PHIPA) in respect of the CorHealth Cardiac and Vascular Registry. Health information custodians are allowed to disclose personal health information, as defined in the Definitions & Terminology section, to CorHealth without consent under section 39(1)(c) of PHIPA for the purposes of maintaining the Registry.

In accordance with the Regulations made under PHIPA (Regulation), CorHealth reports to the Information and Privacy Commissioner of Ontario (IPC) every three years on CorHealth's practices and procedures for protecting the privacy of cardiac and vascular patients and maintaining the confidentiality of their personal health information (PHI). This report addresses CorHealth's privacy and security program, including the improvements achieved to the program since November 1, 2016. This report is being submitted to satisfy the requirements in section 13(2)(b) of the Regulation so that CorHealth is continued as a prescribed person in respect of

the Registry from November 1, 2020 to October 31, 2023.

2 About this Report

2.1 Document Information

2.1.1 Contents

The Contents section of this assessment outlines the overall structure and content of this document and is hyperlinked for easy navigation.

2.1.2 Document Icons

Icons are used throughout this assessment to draw your attention to specific information:

Icon	Meaning	Indicates
	Note	Supplemental commentary
	Important	Imperative information which is key to the understanding of the statement(s)/this document

2.1.3 Definitions & Terminology

Term	Definition
Agent	Same meaning as in PHIPA
Collection	As defined in PHIPA; meaning the gathering, acquiring, receiving, or obtaining of personal health information by any means from any source
CorHealth	Short form of CorHealth Ontario
CCO	Short form of Cancer Care Ontario
Director of IT	Role responsible for managing aspects of the privacy and security program in conjunction with the Privacy Officer and as outlined in the privacy and security policies and procedures. This role is currently performed by the Senior Director, Service Delivery & Chief Digital Officer
Disclose	As defined in PHIPA; meaning to make the personal health information available or to release it to another health information custodian or person
Health Care	As defined in PHIPA
Health Information	As defined in PHIPA

Term	Definition
Custodian (HIC)	
IT Manager	Role responsible for performing aspects of privacy and security procedures including maintaining a log of access requests and data transfers. This role is currently performed by the Senior Specialist, Cloud and DevOps Services
Manual	The IPC's *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*
Mobile Devices	Any portable storage device that could be used to digitally/electronically copy, transcribe, or store information, including but not limited to cell phones, smart phones, and laptops
Personal Health Information (PHI)	As defined in PHIPA
PHIPA	Personal Health Information Protection Act, 2004
Prescribed Person	As defined in PHIPA
Privacy Officer	Role responsible for the day-to-day oversight and for ensuring that personal health information is collected, used, and disclosed in accordance with CorHealth's privacy policies and procedures, and in compliance with the Personal Health Information Protection Act, 2004. This role is currently performed by the Senior Director, Service Delivery & Chief Digital Officer
Registry	Short form for the CorHealth Cardiac and Vascular Registry
Registry of cardiac and vascular services	Formal name of the data holding in the regulation. Referred to as the CorHealth Cardiac and Vascular Registry
Use	As defined in PHIPA; meaning to view, handle or otherwise deal with personal health information, but does not include the disclosure of the information

3 Privacy Documentation (PART 1)

The following describes CorHealth's policies and procedures in relation to its privacy policy and procedures.

Note: As a general matter, in relation to all CorHealth policies, its agents are required to sign agreements stating that they understand and will uphold CorHealth's policies at the outset of their relationship with CorHealth and annually thereafter. Should an agent discover or suspect a breach of a policy, CorHealth's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach to CorHealth's Privacy Officer. Disciplinary guidelines for privacy breaches are set out in the CorHealth policy, "Policy and Procedures for Discipline and Corrective Action". If it is determined that there has been a breach of the Confidentiality & Non-Disclosure Agreement signed by agents, CorHealth may seek legal action against the agent(s) responsible.

3.1 Privacy Policy

CorHealth has developed and implemented an overarching privacy policy (the "Protection of Personal Health Information" Policy) to protect the personal health information that it receives. The policy reflects PHIPA and its Regulation, and CorHealth's obligations in relation to personal health information as a prescribed person. The policy is available on the CorHealth website (www.corhealthontario.ca). The following summarizes the provisions of the policy.

3.1.1 Status under the Act

CorHealth is an advisory body to the Ministry of Health and a prescribed person within the meaning of Section 39(1)(c) of PHIPA. As a prescribed person, CorHealth has implemented policies, practices, and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. CorHealth is committed to complying with PHIPA and its Regulation. CorHealth's privacy and security policies, procedures, and practices are subject to review by the IPC every three years.

3.1.2 Privacy and Security Accountability Framework

The accountability framework for ensuring compliance with PHIPA and its Regulation, and for ensuring compliance with the privacy and security policies, procedures, and practices implemented by CorHealth is articulated in CorHealth's Privacy Policy. In particular, the Privacy Policy indicates that the Chief Executive Officer is ultimately accountable for ensuring compliance with PHIPA and its Regulation, and for ensuring compliance with the privacy and security policies, procedures, and practices implemented.

The Privacy Policy articulates the position(s) that have been delegated day-to-day authority to manage the privacy program and the security program, and to whom these positions report. It identifies the duties and responsibilities of the position(s) that have been delegated day-to-day authority to manage the privacy program and the security program, and some of the key activities of these programs. The Privacy Policy also identifies other positions or committees that support the privacy program and/or the security program, and their role in respect of these programs.

Specifically, the Privacy Policy provides that the Chief Executive Officer of CorHealth is ultimately accountable for the protection of personal health information in CorHealth's custody or control. The day-to-day responsibility for ensuring that personal health information is collected, used, and disclosed in accordance with its privacy policies and procedures, and in compliance with the Personal Health Information Protection Act, 2004, has been delegated to the Privacy Officer, who is currently the Senior Director, Service Delivery & Chief Digital Officer.

CorHealth uses contractual means to ensure that personal health information in its custody or control is collected, used, and disclosed in accordance with the Personal Health Information Protection Act, 2004, and is protected from theft, loss, and unauthorized use or disclosure. In particular, CorHealth requires employees, consultants, volunteers, and members of the Board of Directors to sign confidentiality agreements that clearly state their obligations with respect to protecting the confidentiality of personal health information 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 personal health information.

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

3.1.3 Collection of Personal Health Information

CorHealth is permitted to collect personal health information without consent for the purposes of facilitating or improving the provision of cardiac and vascular care services. The policy describes the types of personal health information that CorHealth collects about patients who undergo select adult cardiac and vascular care. CorHealth limits the collection of personal health information to that which is necessary for the purposes it has identified and is consistent with those permitted by PHIPA and its Regulation. Brochures are made available to all patients whose personal health information is collected by CorHealth that provide direction as to how to make an inquiry to CorHealth about the Registry and CorHealth's collection of personal health information. A list of all data holdings containing personal health information is included in the policy.

3.1.4 Use of Personal Health Information

CorHealth only uses personal health information for purposes of facilitating or improving the quality and provision of cardiac and vascular care services, namely to: maintain wait lists for cardiac and vascular care services; ensure that individuals receive timely, equitable, and appropriate access to cardiac and vascular care services; provide advice on issues relating to cardiac and vascular services such as the implementation of best practices, quality indicators, performance measurement, and continuum of care strategies; assist in the management and planning of the delivery of cardiac and vascular care services in Ontario; and as permitted or required by law. As stated in the "Limiting Collection of Personal Health Information" policy, CorHealth commits to not collecting personal health information if other information will serve the purpose.

CorHealth protects personal health information by only providing access to its agents on a "need to know" basis, as is required in the performance of their employment, contractual, or other relationship with CorHealth. CorHealth requires all its agents to sign confidentiality agreements that identify their obligations with respect to protecting personal health information and the privacy of the individuals to whom it relates. CorHealth is responsible for personal health information in its custody and under its control, and personal health information that is no longer

required for the identified purposes is destroyed in a secure manner. Agents are not permitted to conduct research with either personal health information or aggregate/de-identified health information, though aggregate or de-identified health information may be provided to researchers upon request and in compliance with CorHealth's "Disclosure of Aggregate and/or De-identified Health Information to Researchers" policy. Agents are prohibited from using personal health information for the fulfilment of their job description or other contractual obligations if de-identified and/or aggregate data will suffice. The Privacy Officer is responsible for ensuring CorHealth's use of personal health information is compliant with PHIPA and its Regulation. CorHealth has developed and implemented policies ("Limiting Agent Access to and Use of Personal Health Information" and "Limiting Use, Disclosure, and Retention of Personal Health Information") to ensure that its agents use, disclose, and retain no more personal health information than is absolutely necessary for the fulfilment of their job description or other contractual obligations.

CorHealth makes a copy of participating hospitals' data available to them for their own use to track the status of patients in their care, to aid in current and strategic planning, and as permitted or required by law.

Transfers of personal health information are governed by the CorHealth policy, "Secure Transfer of Personal Health Information", which provides for the transfer of personal health information in a secure manner, in compliance with PHIPA and its Regulation, and in accordance with CorHealth's privacy and security program.

The policies, "Notice/Consent for Collecting, Using, and/or Disclosing Personal Health Information" and "Identifying Purposes for Collecting Personal Health Information", govern the collection of personal health information by CorHealth. These policies ensure that agents only collect personal health information in a manner that is compliant with PHIPA and its Regulation, and in accordance with CorHealth's privacy and security program. This is further detailed in CorHealth's Participation Agreements with hospitals. Under the policy, "Destruction of Personal Health Information", agents may only dispose of personal health information in a manner that precludes reconstruction, is compliant with PHIPA and its Regulation, and in accordance with CorHealth's privacy and security program.

3.1.5 Disclosure of Personal Health Information

CorHealth does not disclose personal health information, except to ICES, with which CorHealth has executed a data sharing agreement that meets the requirements of the Manual for Template Data Sharing Agreements, and when required by law. Personal health information is disclosed to ICES pursuant to s.13(5) of PHIPA and its Regulation, for section 45 purposes. ICES immediately de-identifies the personal health information upon receipt and before any data analysis occurs, as required by the data sharing agreement. CorHealth does not disclose personal health information to any other organization or entity. De-identified and/or aggregate data may be provided to third party researchers (Researchers), if certain privacy conditions, set out in the CorHealth policy, "Disclosure of Aggregate and/or De-identified Health Information to Researchers", are met. The de-identification of personal health information is performed according to the procedures set out in the CorHealth policy, "Aggregation and De-Identification of Record Level Data". As an added safeguard, this policy requires de-identified and/or aggregate data to be reviewed prior to its disclosure to ensure that it is not reasonably foreseeable, in the circumstances that the information could be used, either alone or with other information, to identify an individual. Although CorHealth has a policy to share de-identified and/or aggregate data with 3rd party researchers, in practice, CorHealth only shares de-identified and/or aggregate data with researchers affiliated with ICES.

The "Limiting Use, Disclosure and Retention of Personal Health Information" policy sets out the statutory authority for CorHealth to disclose personal health information to ICES and articulates CorHealth's commitment not to disclose personal health information, if other information will serve the purpose, and not to disclose more personal health information than is reasonably necessary to meet the purpose.

3.1.6 Secure Retention, Transfer, and Disposal of Records of Personal Health Information

Personal health information collected by CorHealth is currently retained for as long as is reasonably necessary for long-term analysis and statistical information. Should it be determined that certain personal health information is no longer necessary for the identified purposes, it is destroyed in a secure manner to ensure that reconstruction is not reasonably foreseeable in the circumstances. The manner in which personal health information is retained is set out in the CorHealth policy, "Secure Retention of Personal Health Information". Currently, personal health information is only stored electronically and in an identifiable format. The manner in which personal health information may be transferred is set out in the CorHealth policy, "Secure Transfer of Personal Health Information". Personal health information may only be transferred over secure and encrypted connections at industry standard encryption levels. Additionally, personal health information may be transferred to a third-party service provider on tape medium within a metal box for long-term backup. CorHealth has a policy ("Destruction of Personal Health Information") governing the secure destruction of personal health information, which addresses the manner in which personal health information in both paper and electronic format must be destroyed.

3.1.7 Implementation of Administrative, Technical, and Physical Safeguards

CorHealth's "Protection of Personal Health Information" policy lists the administrative, physical, and technical safeguards that CorHealth has implemented to protect personal health information in its custody or under its control. These include:

- Annual privacy and security training, as well as training for all new staff
- All agents of CorHealth are required to sign Confidentiality & Non-Disclosure Agreements that set out their obligations to protect personal health information
- CorHealth executes Participation Agreements with hospitals that outline both parties' privacy obligations
- CorHealth is located in a secure location, with external video monitoring and progressive grades of physical security
- CorHealth uses firewalls, network encryption, and intrusion detection systems to maintain the integrity of its networks

3.1.8 Inquiries, Concerns, or Complaints Related to Information Practices

CorHealth's "Protection of Personal Health Information" policy provides that individuals may direct inquiries, concerns, or complaints related to the CorHealth's privacy policies, procedures, and practices, and CorHealth's compliance with PHIPA and its Regulation to CorHealth's Privacy Officer and provides contact information for the Privacy Officer and CorHealth's Provincial Office. Inquiries, concerns, or complaints can be made via mail, email, or telephone. Individuals may direct complaints regarding CorHealth's compliance with PHIPA and its Regulation to the IPC. CorHealth's privacy policy and patient brochure also provide contact information for the IPC.

3.1.9 Transparency of Practices in Respect of Personal Health Information

The "Protection of Personal Health Information" policy provides the purposes for which personal health information is collected by CorHealth. It provides for an information brochure explaining those purposes, which are to be given to all patients at the time of the collection of their personal health information and is available on the CorHealth website. Under the "Protection of Personal Health Information" policy, information about the Registry must be publicly available on the CorHealth website.

3.2 Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices

3.2.1 Annual Review of Privacy and Security Policies and Procedures Policy

The policy and associated procedures have been developed and implemented for the ongoing review of the privacy policies, procedures, and practices put in place by CorHealth. The purpose of the review is to determine whether amendments or new privacy policies, procedures, and practices are required. CorHealth's policy on the review of its privacy policies has been combined with its policy on review of its security policies.

Under the policy, the Privacy Officer reviews CorHealth's privacy and security policies and practices at the beginning of each fiscal year or as otherwise directed by the IPC. The Privacy Officer is required to ensure CorHealth policy reflects advancements in technology and industry practices, and to implement initiatives set out by the IPC or changes to applicable laws, including PHIPA and its Regulation. In the event that the law is changed or the IPC issues new guidelines or orders that impact procedures, the Privacy Officer is required to review and make appropriate changes to policy as soon as is reasonably possible, before the scheduled annual review. Policy reviews are conducted with respect to recommendations made by the IPC, in privacy impact assessments, privacy and security audits, and in reports arising from investigations into any privacy or security breaches. In the review process, the Privacy Officer considers the degree to which existing policies have been successfully implemented and the level of consistency among policies, procedures, and practices and may make recommendations in these regards.

Information regarding the reviews of CorHealth's privacy policies, procedures, and practices conducted since November 1, 2016 is available in the Privacy and Security Indicators section of this document.

Under the policy, "Annual Review of Privacy and Security Policies and Procedures", the Privacy Officer is responsible for the communication of new or amended policies to the public and to CorHealth's agents. New and amended policies will be communicated to CorHealth's agents in written and/or electronic format. The Privacy Officer reviews on an annual basis the manner of communication.

The CEO is responsible for ensuring that all agents comply with the "Annual Review of Privacy and Security Policies and Procedures". The Privacy Officer undertakes the day-to-day responsibility for this task.

All CorHealth agents must comply with the "Annual Review of Privacy and Security Policies and Procedures" policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually (in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not

complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreements, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.3 Transparency of Privacy Policies, Procedures and Practices Policy

The "Transparency of Privacy Policies, Procedures and Practices" policy ensures that information regarding its activities and policies is made available to the public and other stakeholders. This policy sets out that the following information must be made publicly available on CorHealth's website:

- CorHealth's privacy and security policies and procedures
- A list of data holdings containing personal health information – currently, this consists of two data holdings, the CorHealth Cardiac Registry and the CorHealth Vascular Registry, which are both stored in accordance with the CorHealth policy, "Secure Retention of Personal Health Information"
- Documentation relating to the review of CorHealth's privacy and security policies and procedures by the IPC
- Contact information of the designated Privacy Officer at CorHealth

Brochures and posters discussing CorHealth's mandate, activities, and mission to protect personal health information are located in a visible location at all CorHealth participating hospitals and at the CorHealth head office. Additionally, brochures are provided to all patients whose personal health information has been collected by a health information custodian proximate to the time of the procedure.

All inquiries, concerns, or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with PHIPA and its Regulation may be directed to the CorHealth Privacy Officer, whose full contact information is listed in the brochure and on the CorHealth website.

The "Transparency of Privacy Policies, Procedures, and Practices" policy requires CorHealth to place brochures in all participating hospitals that explain CorHealth's mandate and its collection of personal health information. These brochures are required to include, at minimum, an explanation of CorHealth's legal status as a Section 39(1)(c) prescribed person under PHIPA, CorHealth's responsibilities stemming from that status, a statement directing any questions and inquiries to CorHealth's Privacy Officer, a statement directing complaints and inquiries about CorHealth's compliance with PHIPA and its Regulation to the IPC, contact information for CorHealth's Privacy Officer and the IPC, some of the administrative, technical, and safeguards used by CorHealth to protect personal health information, the fact that CorHealth will take all necessary precautions to protect personal health information from theft, loss, and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification, or disposal, and the following information regarding its privacy and

security policies and procedures:

- The types of personal health information collected and the persons or organizations from which this personal health information is typically collected
- The purposes for which personal health information is collected
- The purposes for which personal health information is used, and if identifiable information is not routinely used, the nature of the information that is used
- The circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to which it is typically disclosed

As stated in CorHealth's policy, "Limiting Agent Access and Use of Personal Health Information", personal health information is not routinely used and is only used in instances when de-identified or aggregate data will not suffice.

3.4 Policies and Procedures for the Collection of Personal Health Information

CorHealth has developed and implemented policies governing the collection of personal health information. These policies ("Identifying Purposes for Collecting Personal Health Information", "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information", and "Limiting Collection of Personal Health Information") identify the purposes for which personal health information will be collected by CorHealth, the nature of the personal health information that will be collected, from whom the personal health information will be collected, and the secure manner in which personal health information will be collected. The Privacy Officer is responsible for compliance with these policies.

The "Identifying Purposes for Collecting Personal Health Information" policy lists the general types of personal health information that CorHealth may collect. These include:

- Patient name, middle name, and surname
- Patient date of birth
- Patient sex
- Patient OHIP number
- Patient chart and/or medical record numbers
- Medical report numbers and/or specimen accession numbers
- Patient address, city/town, province, and postal code
- Patient telephone numbers

The "Limiting Collection of Personal Health Information" policy sets out that CorHealth will only collect personal health information within the limits set out in section 39(1)(c) of PHIPA and that CorHealth will collect personal health information by fair and lawful means.

The "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information" policy provides that CorHealth limits its collection of personal health information to that which is necessary for the purposes of facilitating or improving the provision of cardiac and vascular care services and only uses personal health information without consent for these purposes, including to maintain wait lists for treatment and to assist in the management, planning, and delivery of cardiac and vascular care services.

The policy articulates CorHealth's commitment not to collect personal health information unless the collection is permitted by PHIPA and its Regulation, not to collect personal health information if other information will serve the purpose, and not to collect more personal health information than is reasonably necessary to meet the purpose. In order to ensure that the personal health information that is collected for the identified purposes is limited to that which is necessary for

the fulfilment of those purposes, CorHealth requires all its agents to sign confidentiality agreements, obliging them to comply with the privacy and security policies and procedures implemented by CorHealth, including its policies on personal health information collection ("Identifying Purposes for Collecting Personal Health Information", "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information", and "Limiting Collection of Personal Health Information"). As mentioned, these confidentiality agreements provide that failure to comply may result in disciplinary action up to and including termination of an agent's relationship with CorHealth. CorHealth executes Participation Agreements with participating hospitals that clearly set out their obligations to follow CorHealth policies, including those on the collection of personal health information ("Identifying Purposes for Collecting Personal Health Information", "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information", and "Limiting Collection of Personal Health Information"). As stipulated in these Participation Agreements, CorHealth is responsible for maintaining the integrity and the security of the personal health information that CorHealth receives from participating hospitals.

CorHealth's policy on privacy breaches ("Information Security and Privacy Breach Management") dictates the procedure followed by its agents should they suspect that a breach of this policy has taken place and requires agents to notify CorHealth at the first reasonable opportunity in the case of a confirmed or suspected breach. CorHealth's Privacy Officer is responsible for ensuring that all CorHealth agents comply with this policy.

CorHealth audits these policies ("Identifying Purposes for Collecting Personal Health Information", "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information", and "Limiting Collection of Personal Health Information") in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"). The policy provides that CorHealth's policies on the collection of personal health information will be audited annually by the Privacy Officer and sets out the nature of the auditing, which involves the review of the data points of personal health information that are collected to ensure that CorHealth only collects data necessary to fulfil its mandate under PHIPA and its Regulation.

3.4.1 Review and Approval Process

CorHealth only collects personal health information from participating hospitals and does not receive personal health information from any other source. CorHealth's policy, "Identifying Purposes for Collecting Personal Health Information", sets out that front-line health care providers will identify to patients the reasons for the collection of their personal health information by CorHealth. CorHealth executes Participation Agreements with participating hospitals that articulate the obligations of both CorHealth and the hospitals to protect personal health information.

As set out in the CorHealth policy, "Identifying Purposes for Collecting Personal Health Information", CorHealth's Privacy Officer is responsible for reviewing the data elements of personal health information that CorHealth collects to verify that only personal health information necessary for CorHealth's functions is collected. The "Identifying Purposes for Collecting Personal Health Information" policy states that this review shall be documented and communicated to staff in accordance with the procedures set out in the CorHealth policy, "Annual Review of Privacy and Security Policies and Procedures".

The policy, "Identifying Purposes for Collecting Personal Health Information" also sets out the minimum criteria that must be considered by the Privacy Officer when determining whether to approve the collection of personal health information. At a minimum, the criteria to consider are:

- The collection must be permitted by PHIPA and its Regulation and that any and all

conditions or restrictions set out in PHIPA and its Regulation have been satisfied
- No other information, namely de-identified and/or aggregate information, will serve the identified purpose
- No more personal health information is being collected than is reasonably necessary to meet the identified purpose

3.4.2 Conditions or Restrictions on Approval

In accordance with the CorHealth policy, "Accountability for Personal Health Information", CorHealth executes Participation Agreements with participating hospitals prior to its collection of personal health information. These Agreements were drafted by legal consultants to CorHealth and with input from the IPC following its review of CorHealth in 2008. The Agreements set out that all collection of personal health information must be in accordance with PHIPA and its Regulation, as well as CorHealth policies ("Identifying Purposes for Collecting Personal Health Information", "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information", and "Limiting Collection of Personal Health Information"). CorHealth's Privacy Officer is responsible for ensuring that Participation Agreements have been executed prior to the collection of personal health information by CorHealth from hospitals.

3.4.3 Secure Retention

Personal health information collected by CorHealth is retained in a secure manner consistent with the procedures of the CorHealth policy, "Secure Retention of Personal Health Information".

3.4.4 Secure Transfer

CorHealth's policy on the secure transfer of personal health information ("Secure Transfer of Personal Health Information") was developed by CorHealth's Privacy Officer in April 2010, following recommendations made by the IPC after its review of CorHealth in 2008. Under the policy, any digital transmissions of personal health information to and from CorHealth are made, at a minimum, under an industry standard encryption certificate. The digital certificate is renewed on an annual basis. Also, personal health information may be transferred to a third-party service provider on tape medium within a metal box for long-term backup. The "Secure Transfer of Personal Health Information" policy prohibits the transfer of personal health information in paper format.

3.4.5 Secure Return or Disposal

Currently, CorHealth retains personal health information for as long as necessary for long-term statistical analysis. CorHealth has developed and implemented a policy on the secure destruction of personal health information ("Destruction of Personal Health Information") that identifies the method by which personal health information in paper and electronic format is required to be securely disposed. This policy was developed by CorHealth's Privacy Officer in August 2008 and came into effect that same month. Personal health information on paper is disposed of in locked bins and on a monthly basis collected by Shred-It, a third-party provider to CorHealth whose employees are bonded. CorHealth's agreement with Shred-it, requires Shred-it to provide secure transportation of material to its facility, to shred (by cross shredding) the material within 24 hours of its arrival and to provide a certificate of destruction upon completion. If personal health information is on a hard drive, the "Destruction of Personal Health Information" policy states that the drive must be formatted 4 times and then mechanically destroyed. It is the Privacy Officer's responsibility to ensure that the records of personal health information collected are either securely returned or securely disposed of, following the retention period or date of termination.

All CorHealth agents must comply with the "Destruction of Personal Health Information" policy. Compliance with this policy will be audited by CorHealth's Privacy Officer on an annual basis (in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.5 List of Data Holdings Containing Personal Health Information

CorHealth documents information relating to both of its data holdings containing personal health information. The CorHealth Cardiac Registry and CorHealth Vascular Registry data holdings store personal health information of all patients who undergo select advanced cardiac and vascular procedures in Ontario, as well as Ontario residents who undergo those procedures in certain centres outside of Ontario. Included, is a list of data elements that the two CorHealth data holdings contain, such as the demographic and geographic information listed below:

- Patient name, middle name, and surname
- Patient date of birth
- Patient sex
- Patient OHIP number
- Patient chart and/or medical record numbers
- Medical report numbers and/or specimen accession numbers
- Patient address, city/town, province, and postal code
- Patient telephone number

Additionally, CorHealth collects hundreds of specific data points regarding the patient's condition and the procedure that prompted their personal health information to be collected. The information about the patient's procedure that CorHealth collects helps CorHealth to compare outcomes for patients who have undergone different variations of the same procedure. To that end, CorHealth collects information about what procedures are conducted, how long the patient waits for the procedure, where the procedure is conducted, which surgical techniques are used, what drugs are administered, what devices are used, what type of surgeon or physician performs the procedure, how long the procedure takes, and any adverse events that may take place during the procedure. All data is securely retained within the CorHealth Cardiac and Vascular Registry following the procedures set out in the CorHealth policy, "Secure Retention of Personal Health Information".

Information about the patient's condition that is collected by CorHealth helps CorHealth to display data to the participating hospitals that can be used to compare outcomes for patients with varying health conditions. To that end, CorHealth collects information about the condition that led to a referral for a cardiac or vascular procedure, the patient's family history, any drug

allergies the patient may have, any pre-existing conditions that may affect the procedure or the procedure's outcome, and how the patient's condition changes throughout the procedure. Depending on the procedure, this can include telemetry data, which is collected by ECG or other technology. All data is securely retained within the CorHealth Cardiac and Vascular Registry following the procedures set out in the CorHealth policy, "Secure Retention of Personal Health Information".

3.6 Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information

3.6.1 Statements of Purpose for Data Holdings Containing Personal Health Information Policy

In accordance with the CorHealth policy, "Statements of Purpose for Data Holdings Containing Personal Health Information", CorHealth's Privacy Officer is required to develop and maintain a statement of purpose for every data holding containing personal health information. The policy requires that these statements set out the purpose of the data holding, the personal health information contained in the data holding, the source of the personal health information, and the need for the personal health information in relation to the identified purpose.

The Privacy Officer is responsible for the development, finalization, and day-to-day authority in respect of statements of purpose for data holdings containing personal health information.

Statements of purpose for data holdings containing personal health information are provided to participating CorHealth hospitals that collect personal health information that is provided to CorHealth.

During the course of his/her annual review of CorHealth's privacy and security program, the Privacy Officer reviews the statements of purpose for data holdings containing personal health information in accordance with policy and assesses the relevance of each data holding with respect to any changes in strategy or operations to ensure that each data holding remains necessary. If the data holding is no longer necessary for CorHealth's operation as a prescribed person, it will be eliminated in accordance with CorHealth's policy, "Destruction of Personal Health Information". Additionally, if the purpose of a data holding containing personal health information has changed, the Privacy Officer will amend the statement of purpose, as necessary. The Privacy Officer is required by the aforementioned policy to prepare a document explaining the actions taken during the review, the date of the review, and the rationale for the actions under PHIPA and its Regulation, CorHealth's privacy and security policies, and relevant IPC guidelines.

CorHealth's Privacy Officer will consult with CorHealth's software development and clinical teams to assess whether the statements of purpose are aligned with CorHealth's identified purpose. As the Privacy Officer is responsible for all statements of purpose for data holdings containing personal health information, he/she does not have to receive approval from any person, organization, or entity for new or amended statements of purpose.

As set out in the policy, new or recently amended statements of purpose are communicated to participating CorHealth hospitals as soon as is reasonably possible.

All CorHealth agents must comply with the "Statements of Purpose for Data Holdings Containing Personal Health Information Policy". Compliance with this policy will be audited by CorHealth's Privacy Officer or his/her delegate on an annual basis. Should it be determined that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy

Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures ("breach" being defined in CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.7 Statement of Purpose for the CorHealth Cardiac and Vascular Registry

CorHealth maintains a statement of purpose for each of its data holdings within the CorHealth Cardiac and Vascular Registry. These statements of purpose explain the purpose and goals of the data holding, which is critical to CorHealth's function as a Registry, including a description of the personal health information contained within the data holdings, and a list of the sources of the personal health information.

3.8 Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information

3.8.1 Limiting Agent Access to and Use of Personal Health Information Policy

CorHealth has developed and implemented a policy, "Limiting Agent Access to and Use of Personal Health Information", that restricts access and use of personal health information on a "need to know" basis, as is required in the performance of their employment, contractual, or other relationship with CorHealth. The Privacy Officer is responsible for determining which CorHealth agents are granted permission to access or use personal health information. Agents are required to comply with this policy and notify CorHealth at the first reasonable opportunity if an agent breaches or believes there may have been a breach of this policy or CorHealth procedures.

The policy sets out the procedures for the Privacy Officer's approval of agent access and use of personal health information. Upon the commencement of an agent's relationship with CorHealth, the Privacy Officer, in consultation with agent's manager, will determine whether to grant the agent access to the CorHealth system that involves personal health information. This system is the main CorHealth application or Wait Time Information System (WTIS-CCN), into which personal health information is entered by hospitals and where it resides for the purposes of reporting and analysis. The policy sets out the narrowly defined purposes for which access to and use of personal health information may be granted, namely to aid Data Clerks and Regional Cardiac Care Coordinators at participating CorHealth hospitals to correct or verify patient information entered into the database, and to prepare advisory reports for hospitals and the Ministry of Health and Long Term Care. Under the policy, agents with access to the CorHealth Cardiac and Vascular Registry may only use personal health information in the CorHealth Cardiac and Vascular Registry if de-identified and/or aggregate data will not serve the purpose, and to use as little personal health information as possible when de-identified and/or aggregate data

will not serve the purpose.

Each CorHealth database is unitary, meaning that it is not compartmentalized. Agents who require access to and use of personal health information will have access to the entire database to create comprehensive reports, to help hospitals with data entry, and/or to verify and correct patient information. As such, CorHealth does not segregate agents by level of access. All agents granted access to the CorHealth Cardiac and Vascular Registry have full rights to modify data as required for the correction of records. However, both data holdings are separate and as such having access to the cardiac data holding does not grant one access to the vascular data holding and vice versa. CorHealth will contact the IPC should any part of this policy change.

Agents who do not need personal health information for the fulfilment of their job description or other contractual duties are required by the policy to use de-identified and/or aggregate data, the preparation of which is governed by the CorHealth policy, "Aggregation and De-identification of Record Level Data". The policy prohibits agents who use de-identified and/or aggregate data from using that data to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, attempting to identify an individual based on prior knowledge, and attempting to re-identify individual using additional information.

3.8.2 Review and Approval of Access Process

The process of granting an agent access to personal health information is governed by the CorHealth policy, "Limiting Agent Access to and Use of Personal Health Information", which provides that CorHealth's Privacy Officer is responsible for determining which CorHealth agents are granted access and the use of personal health information.

The decision is made upon the commencement of the agent's relationship with CorHealth or if an agent's responsibilities change and access to and/or use of becomes necessary. CorHealth agents do not request access to CorHealth's data holdings; the decision is made by the Privacy Officer, in consultation with the agent's manager. The Privacy Officer grants the agent access and the use of personal health information only if it is necessary for the agent's fulfilment of his/her contractual or other obligations. The only agents that are granted access to CorHealth's data holdings require that access to correct errors in records, conduct statistical analysis, and to assist participating hospitals. As stated in the "Limiting Agent Access to and use of Personal Health Information" policy, the Privacy Officer must be satisfied that the agent routinely requires access to and use of personal health information on an ongoing basis for his or her employment, contractual or other responsibilities, the identified purpose for access and use of personal health information is permitted by PHIPA and its Regulation, the identified purpose for access and use of personal health information cannot reasonably be accomplished without personal health information, de-identified and/or aggregate data will not serve the identified purpose, and no more personal health information will be accessed and used than is reasonably necessary to meet the identified purpose.

In approving agent access to CorHealth's data holdings, CorHealth's Privacy Officer is required by the "Limiting Agent Access to and Use of Personal Health Information" policy to document the date that access is granted or denied, the reasons for which access is required, and the purpose for permitting access with regard to PHIPA and its Regulation and CorHealth policies. This documentation is retained by the Privacy Officer and by the IT Manager.

If an agent's job description changes and it is no longer necessary for him/her to access one of CorHealth's data holdings, the Privacy Officer is required by the "Limiting Agent Access to and Use of Personal Health Information" policy to revoke that agent's access rights.

3.8.3 Conditions or Restrictions on the Approval of Access

Currently, there is only one access level for the CorHealth Cardiac and Vascular Registry, and CorHealth agents who are granted access to personal health information have full access rights to read, create, update, and delete records of personal health information. However, both data holdings are separate and as such, having access to the cardiac data holding does not grant one access to the vascular data holding and vice versa. All CorHealth agents sign a confidentiality agreement stating that they "may only use personal health information when necessary for the purpose of carrying out [their] relationship with CorHealth and for no other purpose". Violation of this agreement will result in disciplinary action, up to and including the termination of an agent's relationship with CorHealth. Additionally, a breach of the Confidentiality & Non-Disclosure Agreement amounts to a breach of contract, and CorHealth may seek legal action against the agent(s) responsible.

Currently, all agents with access to CorHealth's data holdings require that access for the fulfilment of their job description. CorHealth does not provide any agent temporary access to the CorHealth data holdings. Should the job description of an agent with access to CorHealth's data holdings change, and the agent no longer requires access to personal health information, CorHealth's Privacy Officer is responsible for revoking access, as set out in the "Limiting Access to and Use of Personal Health Information" policy. Because of CorHealth's small size and the CEO's practice of providing notification to all staff of agent termination and other staffing updates, it is not likely that an agent's relationship could be terminated, or an agent's job description could change without the Privacy Officer's knowledge. As such, CorHealth has found no need to require its agents to provide specific notification to the Privacy Officer when they no longer require access to CorHealth's data holdings. This practice may evolve as CorHealth grows.

The "Limiting Agent Access to and Use of Personal Health Information" policy prohibits agents with access to CorHealth's data holdings from accessing or using more personal health information than is absolutely necessary for the fulfilment of their job description. Access and use of personal health information are only permitted to the extent that they serve CorHealth's mandate as a prescribed person under PHIPA and its regulation. Additionally, agents are prohibited from accessing or using personal health information if de-identified and/or aggregate data will serve the same purpose.

Other than to ICES, CorHealth agents are forbidden to disclose personal health information for any purpose to any individual or organization as set out in the "Protection of Personal Health Information" policy. Therefore, CorHealth has not found it necessary to develop procedures for the imposition of conditions or restrictions on the disclosure of personal health information.

Under the policy, "Limiting Access to and Use of Personal Health Information", agents are granted access to CorHealth's data holdings upon commencing employment if their job description requires them to regularly access and/or use personal health information. In order to ensure that only agents who require access to personal health information have access to personal health information, the Privacy Officer audits the log of agents with access to CorHealth's data holdings annually to ensure that the day-to-day duties all agents involve the use of the CorHealth Cardiac and Vascular Registry. If an agent no longer requires access to a CorHealth data holding, the Privacy Officer terminates his/her access rights.

3.8.4 Notification and Termination of Access and Use: Domain Account Retention Policy

CorHealth's policy governing the retention of user accounts, "Domain Account Retention Policy", sets out that the Privacy Officer or a member of the IT staff designated by the Privacy Officer

will deactivate the account of a user whose relationship with CorHealth has been terminated within one day of termination/last-work date (whichever is later). This leaves the account inaccessible to anyone except for the Privacy Officer or designated IT staff. Sixty days after termination/last work date, the account is purged (e.g., user data including draft documents, non-work-related documents, settings, passwords, web history are deleted). The purge does not include the agent's email archive or documents that remain relevant to CorHealth operations, which are retained for an indefinite period. Because of the small number of agents who currently have user accounts, it is reasonable to assume that an agent could not be terminated without the knowledge of the Privacy Officer. As such, CorHealth does not require agents whose relationships with CorHealth have been terminated to provide notification to the Privacy Officer of that termination. Agents who resign their position with CorHealth are required to give prior notice of 2-6 weeks, depending on the nature of their position and specific employment contract. These procedures are consistent with the "Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship". As set out in CorHealth's policy, "Secure Retention of Personal Health Information", CorHealth agents are forbidden from retaining any personal health information on the hard drive of any device, including their work computers; all personal health information must be stored on the secure servers within CorHealth's secure server room and their tape backups.

3.8.5 Secure Retention: Secure Retention of Personal Health Information Policy

The "Secure Retention of Personal Health Information" policy states that personal health information may be stored only on the secure servers within the locked server room of CorHealth's provincial office, and their tape backups. Agents granted access to personal health information are prohibited from retaining personal health information on any other storage device, as set out in CorHealth's policy, "IT Policy: Email, Internet, and Computing Devices". Currently, personal health information is retained for as long as is reasonably necessary for long-term statistical analysis.

3.8.6 Secure Disposal: Destruction of Personal Health Information Policy

In the event the Privacy Officer determines certain personal health information is no longer necessary for CorHealth's identified purposes, CorHealth's policy on the destruction of personal health information, "Destruction of Personal Health Information", dictates the methods of disposal. The Policy was developed by CorHealth's Privacy Officer in August 2008 and came into effect that same month. As set out in the policy, agents who have been granted permission to access and use personal health information are to dispose of personal health information on paper in any of three locked bins, which are collected, on a monthly basis by Shred-it, an external company, which has bonded employees. CorHealth's agreement with Shred-it requires Shred-it to provide secure transportation of material to its facility, to shred (by cross shredding) the material within 24 hours of its arrival, and to provide a certificate of destruction upon completion. Under the policy, if personal health information is to be deleted from a hard drive, the drive must be formatted 4 times and then mechanically destroyed.

3.8.7 Tracking Access and Use of Personal Health Information

The "Limiting Agent Access to and Use of Personal Health Information" policy requires CorHealth's IT Manager, under the supervision of CorHealth's Privacy Officer, to maintain a log of agents who have been granted access to either of CorHealth's data holdings in a password-protected location on their computer or designated partition of the network drive. Information

tracked includes the names of agents granted permission to access and use personal health information, the date on which they were granted access, and the date on which access to CorHealth's data holdings was revoked or terminated, if applicable, along with a brief explanation of the reasons for the revocation or termination.

3.8.8 Compliance, Audit and Enforcement: Policy and Procedures for Privacy and Security Auditing/ Maintenance and Review of System Control and Audit Logs Policy

Agents are required under all CorHealth policies to agree in writing, at the outset of their relationship with CorHealth and annually thereafter, that they understand and will uphold the policies. Should an agent discover or suspect a breach of a policy, he or she is required to report the suspected or actual breach to the Privacy Officer at the first reasonable opportunity. Consequences of a breach are determined by the Privacy Officer, in consultation with the agent's manager and the CEO, when necessary, and may include the revocation of personal health information access rights, or depending on the circumstances, termination of an agent's relationship with CorHealth. If the breach constitutes a violation of an agent's confidentiality agreement, CorHealth may seek legal action against the agent(s) responsible.

The "Policy and Procedures for Privacy and Security Auditing" also mandates that the Privacy Officer conduct an additional annual audit of agents who have been granted access to CorHealth's data holdings. This audit requires the Privacy Officer to review the agents' work duties to ensure that each agent continues to require access to personal health information.

As set out in the policy, "Maintenance and Review of Specialized Assessments and System Control and Audit Logs", changes made to the CorHealth Cardiac and Vascular Registry or the CorHealth Vascular Registry are tracked, logged, and audited by the Database and Application Development Supervisor to ensure the integrity of the application. The audit logs include information on the user making changes, so that an unauthorized change can be quickly traced and resolved according to the procedures set out in the policy, "Information Security and Privacy Breach Management".

3.9 Log of Agents Granted Approval to Access and Use Personal Health Information

As set out under Section 3.8.7 Tracking Access and Use of Personal Health Information, CorHealth maintains a log of agents who have been granted approval to access and use CorHealth's data holdings. This log is maintained by the IT Manager under the direction of the Privacy Officer.

3.10 Policy and Procedures for the Use of Personal Health Information for Research

Currently, CorHealth does not conduct research, and does not permit disclosure of personal health information to third-party researchers , except to ICES, with which CorHealth has executed a data sharing agreement that meets the requirements of the Manual for Template Data Sharing Agreements. The use of personal health information for research is expressly prohibited by CorHealth's policies, "Disclosure of Aggregate and/or De-identified Personal Health Information to Researchers" and "Limiting Use, Disclosure, and Retention of Personal Health Information". As such, CorHealth does not require a policy or procedures for the use of personal health information for research.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.11 Log of Approved Uses of Personal Health Information for Research

No log is required as CorHealth does not permit the use of personal health information for research.

3.12 Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research

CorHealth does not disclose personal health information, except to ICES, with which CorHealth has executed a data sharing agreement that meets the requirements of the Manual for Template Data Sharing Agreements, and when required by law. f. As such, a written policy on the disclosure of personal health information for purposes other than research is unnecessary.

CorHealth's Privacy Officer audits "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information" annually as set out in the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing" to ensure that personal health information is not disclosed.

All CorHealth agents must comply with the "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information" policy. Compliance with this policy is audited by CorHealth's Privacy Officer annually in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.13 Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements

As mentioned in Section 3.10 Policy and Procedures for the Use of Personal Health Information for Research, CorHealth does not disclose personal health information in any circumstances, except under CorHealth's data sharing agreement with ICES. The rare requests for personal health information for the purposes of research are denied.

As stated in CorHealth's policy, "Policy and Procedures for Privacy and Security Auditing", CorHealth undertakes annually auditing of agents' computers to ensure that personal health information is not disclosed for any unauthorized purpose.

3.13.1 Where the Disclosure of Personal Health Information is Permitted for Research

CorHealth does not permit the disclosure of personal health information for research except under its data sharing agreement with ICES. As such, a written policy on when the disclosure of personal health information for research purposes is permitted is unnecessary.

3.13.2 Review and Approval Process

CorHealth does not require a review and approval process for the disclosure of personal health information for research purposes for the reasons set out above.

3.13.3 Conditions or Restrictions on the Approval

CorHealth does not require procedures for placing conditions or restrictions on the approval of disclosure of personal health information for research purposes for the reasons set out above.

3.13.4 Secure Transfer

CorHealth does not require procedures for secure transfer of personal information for research purposes for the reasons set out above.

3.13.5 Secure Return or Disposal

CorHealth does not require procedures for secure return or disposal of personal health information after it has been disclosed to a third-party for research purposes for the reasons set out above.

3.13.6 Documentation Related to Approved Disclosures of Personal Health Information

CorHealth does not require procedures for documenting disclosures of personal health information for research purposes for the reasons set out above.

3.13.7 Where the Disclosure of Personal Health Information is not Permitted for Research

As previously described, under no circumstances does CorHealth permit the disclosure of personal health information for research purposes, except to ICES, with which CorHealth has executed a data sharing agreement. This restriction is set out in CorHealth's policy, "Limiting Use, Disclosure, and Retention of Personal Health Information". As set out in the policy, "Disclosure of Aggregate and/or De-identified Health Information to Researchers", if certain conditions have been fulfilled, CorHealth may disclose de-identified and/or aggregate data to

researchers.

3.13.8 Review and Approval Process

The policy, "Disclosure of Aggregate and/or De-identified Health Information to Researchers" sets out the procedures for the review and approval process for researchers requesting access to de-identified and/or aggregate data. Requests for de-identified and/or aggregate data are reviewed by the Research and Publications Committee, a body composed of medical researchers and hospital administrators who ensure that agreements are in place requiring researchers to use data received from CorHealth in a secure and ethical manner. Researchers who request de-identified and/or aggregate data must be affiliated with an established research institution, a national or provincial association representing cardiovascular services, or a funder or related organization (e.g., MOH). In addition, researchers using data for PhD theses, research supported by a grant, or research to be submitted to a peer-reviewed journal may be eligible to receive de-identified and/or aggregate data. Researchers who do not fall under any of these categories may still be granted access to data, if the researcher can provide a compelling argument to the Research Publications Committee. CorHealth has only ever provided de-identified and/or aggregate data to researchers affiliated with ICES.

Researchers interested in a topic requiring de-identified and/or aggregate data from CorHealth must submit a letter of intent to the Research Publications Committee. A standardized template is made available to researchers through CorHealth's website. The "Letter of Intent to Conduct a Study for Publication" can be made available to the IPC upon request. CorHealth systems allow researchers to search for other letters of intent to find other researchers interested in similar topics, thus facilitating co-authorship. The "Letter of Intent to Conduct a Study for Publication" requires the researcher to identify what data elements are necessary for their study and to summarize their research plan. Researchers are required to provide a certificate of approval from a research ethics board upon request from CorHealth. A researcher must prove to the Research and Publications Committee that their research proposal has scientific value and does not compromise any CorHealth privacy policy, practice, or procedure. If the Research and Publications Committee finds the proposal to be without scientific merit or ethical integrity, the proposal will be denied.

Personal health information will be aggregated or de-identified according to the procedures set out in the policy, "Aggregation and De-Identification of Record Level Data".

As set out in the "Aggregation and De-Identification of Record Level Data" policy, before the de-identified and/or aggregate data is disclosed to a researcher, the Privacy Officer must review it to ensure that the data cannot be used, alone, or with other information to identify any individuals.

The "Disclosure of Aggregate and/or De-identified Health Information to Researchers" policy requires the Chair of the Research and Publications Committee to retain all documentation relating to the review and approval of researchers' requests for aggregate and/or de-identified personal health information.

3.13.9 Conditions or Restrictions on Research Approval

If the researcher is granted access to de-identified and/or aggregate data that includes any demographic or geographic patient information, the researcher is required by the policy, "Disclosure of Aggregate and/or De-identified Health Information to Researchers" to sign a confidentiality agreement stating that he/she will preserve the confidentiality of the data and prevent disclosure. Additionally, the policy prohibits the researcher from using the de-identified and/or aggregate data, either alone or with other information, to identify an individual. This

includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge. The consequence for the breach of this agreement includes legal action. As stated in "Disclosure of Aggregate and/or De-identified Health Information to Researchers" policy, the Research and Publications Committee is responsible for ensuring compliance with these rules.

As set out in the "Disclosure of Aggregate and/or De-identified Health Information to Researchers" policy, the Chair of the Research and Publications Committee keeps a log, in electronic format, of official requests, approvals, and denials of access to de-identified and/or aggregate data.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.14 Template Research Agreement

Because CorHealth does not disclose personal health information in any circumstances except under its data sharing agreement with ICES, which meets the requirements of the Manual for Template Data Sharing Agreements, it does not require a template research agreement.

3.15 Log of Research Agreements

CorHealth has no need for a log of research agreements for the reasons set out above.

3.16 Policy and Procedures for the Execution of Data Sharing Agreements

CorHealth has only one data sharing agreement in place. It is with ICES. As CorHealth has no immediate plans to enter into other such agreements, it has not developed a policy on their execution. Should this change, CorHealth will develop a new policy and procedure that includes all of the requirements set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

3.17 Template Data Sharing Agreement

For the reasons set out above, CorHealth has determined that having a template for data sharing agreements is unnecessary.

3.18 Log of Data Sharing Agreements

For the reasons set out above, CorHealth does not need a log of data sharing agreements.

3.19 Policy and Procedures for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information

CorHealth has developed the policy, "Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" that requires CorHealth to enter into written agreements with third-party service providers prior to allowing their access to personal health information. The template agreement for this purpose has been developed by CorHealth's Privacy Officer and is based on the template provided by the IPC.

CorHealth's Privacy Officer is responsible for ensuring that agreements are executed with third-party service providers prior to their access to personal health information.

Prior to the execution of agreements with third-party service providers allowing them access to personal health information, CorHealth's Privacy Officer must ensure that:

- The service provided by the third party in respect of personal health information is necessary to CorHealth's delivery of its mandate
- Allowing the third-party service provider access to and or use/of personal health information does not violate any CorHealth privacy or security policies
- Allowing the third-party service provider access to and or use/of personal health information does not violate any privacy legislation, IPC orders, IPC guidelines, or industry best practices
- The service provided by the third party cannot be conducted without personal health information
- CorHealth is not providing any more personal health information than is necessary for the provision of the service

If these requirements have been satisfied, the Privacy Officer may go forward with the execution of an agreement in respect of personal health information with the third-party service provider.

The transfer of personal health information to the third-party provider must be compliant with the CorHealth policy, "Secure Transfer of Personal Health Information". Additionally, any destruction of personal health information following the termination of an agreement must be compliant with the CorHealth policy, "Destruction of Personal Health Information". CorHealth's Privacy Officer is responsible for ensuring that the procedures in these policies are followed by CorHealth staff and the contracted third parties.

In the event that a third-party service provider fails to provide a certificate of destruction of personal health information following the termination of an agreement, CorHealth's Privacy Officer is required by the policy to contact the third party after an unexpected delay of one day and to provide notification to CorHealth's Chief Executive Officer after an unexpected delay of two days. CorHealth may seek legal action against the third party at this point.

All CorHealth agents must comply with this policy. Enforcement is monitored by the Privacy Officer and consequences for breach include termination of the contract, legal action, or disciplinary measures, as relevant. Should a CorHealth agent suspect a breach, the agent has a duty to report this breach to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

CorHealth's Privacy Officer is responsible for developing and maintaining a log of all agreements

in respect of personal health information, which CorHealth has executed with third-party service providers.

CorHealth reviews the policy annually, in accordance with its policy for the annual review of its privacy and security program, "Annual Review of Privacy and Security Policies and Procedures". Because CorHealth so rarely executes agreements with third-party service providers, the Privacy Officer has determined that more frequent audits of this policy are unnecessary.

3.20 Template Agreement for All Third-Party Service Providers

As required by "Policy and Procedures for the Execution of Agreements with Third-Party Service Providers in Respect of Personal Health Information", CorHealth has developed a template for agreements with third-party service providers that are permitted to use and/or access personal health information including those that are contracted to retain, transfer, or dispose of records of personal health information and those that are contracted to provide services for the purpose of enabling CorHealth to use electronic means to collect, use, modify, disclose, retain, or dispose of personal health information. The template agreement includes the following:

- General Provisions:
    - A description of the role of CorHealth and the third party under PHIPA and its regulation
    - CorHealth's duties and responsibilities under PHIPA and its regulation
    - If the third-party service provider is being permitted access to and/or use of personal health information, the agreement states that the third-party service provider is an agent of CorHealth
    - If the agreement is executed with an electronic service provider, the agreement states that the third-party electronic service provider is required to indicate whether the third party is an agent of CorHealth
    - If the third-party service provider is an agent of CorHealth, the agreement requires the third party to comply with the provisions of PHIPA and its regulation relating to CorHealth, and to comply CorHealth's privacy and security policies and procedures in providing services pursuant to the agreement
    - The definition of personal health information in PHIPA and its regulation
    - A description of the nature of the personal health information being provided to the third-party service provider
    - A stipulation that the third party must perform its services in a professional manner according to industry standards and practices and employ properly trained agents to provide the identified services
- Obligations with Respect to Access and Use:
    - A list of the purposes for which the third party is permitted to access and/or use personal health information
    - Any conditions, limitations, or restrictions on the third party's permission for access to and/or use of personal health information
    - The authority under PHIPA and its regulation for each permitted access to and use of personal health information
    - A stipulation that the third party may not access or use personal health information for any other purpose than those set out in the agreement
    - If the agreement is with an electronic service provider that is not an agent of CorHealth, that the third party is prohibited from accessing or using personal health information, except as necessary in fulfilling the terms of the agreement

  - A statement prohibiting the third party from accessing or using personal health information if other information will suffice
  - A statement prohibiting the third party from accessing or using any more personal health information than is reasonably necessary to fulfill the terms of the agreement

- Obligations with Respect to Disclosure:
  - CorHealth's template agreement for third-party service providers in respect to personal health information prohibits the disclosure of personal health information, except as required by law

- Secure Transfer:
  - A stipulation that personal health information must be transferred by the third party in a secure manner where it is necessary to transfer personal health information
  - A description of the manner in which personal health information is permitted to be transferred by the third party and the procedures for this manner of transfer with reference to CorHealth's policy, "Secure Transfer of Personal Health Information"
  - A list of the conditions under which personal health information is permitted to be transferred by the third party
  - Indications of to whom personal health information is permitted to be transferred by the third party
  - A stipulation that third parties, whose primary service is the storage or disposal of personal health information, must provide CorHealth with documentation stating the date, time, and mode of transfer of personal health information, and confirming the receipt of personal health information by the third party
  - A stipulation that the third party must maintain an inventory of documentation relating to the transfer of personal health information

- Secure Retention:
  - A stipulation that personal health information must be retained by the third party in a secure manner where it is necessary to retain personal health information
  - A description of the manner, including information on different media (such as paper and electronic), in which personal health information is permitted to be retained by the third party and the procedures for this manner of retention with reference to CorHealth's "Secure Retention of Personal Health Information" policy
  - A stipulation that third parties whose primary service is the storage of personal health information on behalf of CorHealth must maintain an inventory of the records of personal health information being stored and a method of tracking the records

- Secure Return or Disposal Following Termination of the Agreement:
  - An indication of whether records of personal health information will be returned to CorHealth or disposed of in a secure manner by the third party following the termination of the agreement
  - If the personal health information is to be returned to CorHealth, the agreement sets out the time frame and manner in which the personal health information must be returned and the CorHealth agent to whom the personal health information must be returned

  - An explanation of how the manner of returning personal health information to CorHealth has regard to the CorHealth policy, "Secure Transfer of Personal Health Information"
  - If the personal health information is to be disposed of by the third party, the agreement sets out the precise manner in which records of personal health information must be disposed of and an explanation of how this manner fits a definition of "secure disposal" that is consistent with PHIPA and its regulation
  - A stipulation that records of personal health information must be disposed of in a manner consistent with CorHealth's policy, "Destruction of Personal Health Information", created in accordance with PHIPA and its regulation, IPC orders, and IPC factsheets, guidelines, and best practices, including IPC Order HO-001 and HO-006, the IPC fact sheet "Fact Sheet 10: Secure Destruction of Personal Health Information"
  - A statement setting out the time frame within which that the records of personal health information must be disposed of by the third party
  - A statement setting out the time frame within which a certificate of destruction must be provided to CorHealth, the required content of the certificate (at minimum, the certificate must identify the records of personal health information securely disposed of, the date, time and method of secure disposal employed, and the name and signature of the person who performed the secure disposal), and the particular CorHealth agent to whom the certificate must be provided

- Secure Disposal as a Contracted Service:
  - If the third party's primary service to CorHealth is the destruction of records of personal health information, the agreement sets out the time frame within which the records must be securely disposed of, the precise methods by which records in paper or electronic format must be disposed of (including descriptions for personal health information on different media), the conditions under which records of personal health information must be disposed of, and the agent of the third party responsible for ensuring that personal health information is disposed of securely
  - A stipulation that CorHealth shall be permitted to witness the destruction of personal health information subject to reasonable terms and conditions
- Implementation of Safeguards:
  - A stipulation that the third party must take reasonable steps to protect the personal health information accessed and used in the course of providing the services set out in this agreement against theft, loss, unauthorized use or disclosure, and unauthorized copying, modification, and disposal.
  - A list of the aforementioned safeguards
- Training of Agents of the Third-Party Service Provider:
  - A stipulation that the third party must provide training to its agents on the importance of protecting the privacy of individuals whose personal health information is accessed and used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations
  - A stipulation that the third party must ensure that its agents who will have access to personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access

  - The method in which the third-party service provider ensures its agents are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the personal health information (e.g., by agreement stating that the agent understands the terms of the agreement with CorHealth)

- Subcontracting of the Services:
  - If the agreement permits the third party to subcontract, the agreement must stipulate that the third party will notify CorHealth in advance and that the subcontractor will be bound to obligations consistent with the third party's obligations to CorHealth under the agreement
  - A copy of the written agreement between the third party and the subcontractor must be provided to CorHealth
- Notification:
  - A stipulation that the third party must notify the Privacy Officer in writing at first reasonable opportunity if it identifies or suspects a breach of the agreement or if the personal health information to which it has permission to access and/or use has been stolen, lost, or accessed by unauthorized persons
  - A stipulation that in such an event, the third party must take all reasonable steps to contain and mitigate the breach of contract or of personal health information
- Consequences of Breach and Monitoring Compliance:
  - The consequences of a breach of the agreement
  - An indication that CorHealth has the right to monitor the third party`s compliance with the agreement
  - The manner in which compliance will be audited and the notification of auditing that will be provided to the third party

3.21 Log of Agreements with Third Privacy Service Providers

As set out in "Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information", CorHealth's Privacy Officer has developed and maintains a log of third-party service providers that are permitted access to and/or use of personal health information. In this log, the Privacy Officer records the following information:

- The name of the third-party service provider
- The nature of the services provided by the third-party service provider that require access to and use of personal health information
- The date that the agreement with the third-party service provider was executed
- The date that the records of personal health information or access to the records of personal health information, if any, was provided
- The nature of the personal health information provided or to which access was provided
- The date of termination of the agreement with the third-party service provider
- Whether the records of personal health information, if any, will be securely returned or will be securely disposed of following the date of termination of the agreement
- The date the records of personal health information were securely returned, the date a certificate of destruction was provided, the date that access to the personal health information was terminated, the date by which the personal health information must be returned or disposed of, or access terminated.

The Privacy Officer retains this log in an access-restricted location on the shared company drive.

3.22 Policy and Procedures for the Linkage of Records of Personal Health Information

As stated in the policy, "Limiting Use, Disclosure, and Retention of Personal Health Information", CorHealth strictly prohibits the linkage of personal health information. To date CorHealth has not approved any linkage of data. CorHealth has a data sharing agreement with ICES, but under that agreement the only linkage is made after ICES de-identifies data sent to it by CorHealth.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually (in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.23 Log of Approved Linkages of Records of Personal Health Information

Because CorHealth does not allow the linkage of records of personal health information, a log of approved linkages is unnecessary.

3.24 Policy and Procedures with Respect to De-Identification and Aggregation

CorHealth has developed a policy and a set of procedures for the de-identification and aggregation of personal health information ("Aggregation and De-identification of Record Level Data"). The policy defines the aggregation of personal health information as the process by which anonymous data sets are created through the collation of patient records. This policy provides definitions of both aggregate information and de-identified information. De-identified information is defined in the policy as the result of the process by which data elements that could be used to identify an individual are removed from personal health information, leaving only the minimum information needed for a particular purpose. The "Aggregation and De-identification of Record Level Data" policy sets out the goal of aggregating or de-identifying personal health information is to ensure data provided to researchers is not, and cannot reasonably be modified into "identifying information", as set out in Section 4(2) of PHIPA. These definitions are consistent with those set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

The "Aggregation and De-identification of Record Level Data" policy sets out the de-identification of data is to be performed when the recipient of the data has not been permitted by the Privacy Officer to access personal health information. Additionally, the policy sets out personal health information may not be used or disclosed for any purpose, except to ICES under the terms of its

data sharing agreement with CorHealth, if de-identified and/or aggregate data will serve the same purpose. Researchers are required by the "Aggregation and De-identification of Record Level Data" policy to execute non-disclosure agreements compelling them to protect the information to which they have been granted access. The policy also outlines the procedures that have been implemented to ensure agents do not reverse the process of aggregation and/or de-identification of personal health information to re-identify it. A breach of any of the procedures of the "Aggregation and De-identification of Record Level Data" policy constitutes a breach of contract, and CorHealth may take legal action against any researcher who does this.

In de-identifying data, the "Aggregation and De-identification of Record Level Data" policy dictates that fields that can be used to identify a person are collapsed and aggregated or removed from data. The Privacy Officer is responsible for ensuring data is de-identified before it is sent out. Complete de-identification of record level data requires removing the following fields from each record:

- Patient health insurance number
- Patient name, middle name, and surname
- Patient date of birth
- Patient sex
- Patient chart and/or medical record numbers
- Medical report numbers and/or specimen accession numbers
- Patient address, city/town, province, and postal code, telephone number
- Patient telephone numbers

The same fields, if not removed, must be collapsed and aggregated so that individual records cannot be differentiated.

CorHealth recognizes that some studies, such as geographic or demographic studies, require information such as the first three characters of the patient's postal code, the patient's province of residence, or the patient's date of birth. For these studies, CorHealth will de-identify the record-level data, eliminating all but the minimum level of demographic or geographic detail required for the study.

De-identified and/or aggregate data may only be used or disclosed if the cell of personal health information contains the patient data of five or more individuals. This policy applies to all research agreements and any future data sharing agreements into which CorHealth may enter.

Agents are prohibited from using de-identified and/or aggregate data to identify a patient. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge. Due to the nature of de-identified and/or aggregate data that CorHealth discloses, the risk of re-identifying patients is very low.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". The Privacy Officer or a designate will review aggregate/de-identified personal health information that has been provided to researchers to ensure that the above procedures have been followed. Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.25 Privacy Impact Assessment Policy and Procedures

CorHealth has developed a policy for the ordering and conducting of Privacy Impact Assessments, "Privacy Impact Assessments". The policy states that privacy impact assessments must be conducted on existing and proposed data holdings involving personal health information, and whenever the implementation of a new or a change to an existing information system, technology or program involving personal health information is contemplated.

Privacy impact assessments must be conducted on proposed new data holdings involving personal health information or changes to existing information systems, technologies, or programs involving personal health information at the conceptual design stage and reviewed and amended, if necessary, during the detailed design and implementation stage.

For existing data holdings containing personal health information, privacy impact assessments must be conducted every three years at minimum. The assessments should be conducted in advance of the three-year review by the Information and Privacy Commissioner of Ontario. The Privacy Officer is responsible for establishing a three-year timetable and ensuring that the timetable is adhered to.

Privacy impact assessments are not required to be conducted on updates to user portals for the CorHealth data holdings, as long as the updates do not affect the storage or transfer or personal health information or rules regarding access to CorHealth's data holdings. The Privacy Officer is responsible for reviewing updates to the CorHealth Cardiac and Vascular Registry to ensure that these aspects are not affected by the updates.

Completed privacy impact assessments shall be reviewed by the Privacy Officer or a designate annually, as part of the Annual Review of the privacy and security program. Reviews of privacy impact assessments shall ensure that they continue to be accurate and continue to be consistent with CorHealth's information practices.

CorHealth's Privacy Officer is responsible for identifying when privacy impact assessments are required. This determination shall be made on the basis of the three-year timetable, ongoing monitoring of new CorHealth projects relating to data holdings containing personal health information and information systems relating to personal health information, and orders and advice from the Information and Privacy Commissioner of Ontario. The Privacy Officer is also responsible for ensuring that privacy impact assessments are conducted, completed, and reviewed in accordance with the policies and procedures. The Privacy Officer is furthermore the day-to-day authority for the management of the privacy and security program in respect of privacy impact assessments.

At a minimum, privacy impact assessments conducted by CorHealth are required to describe the following aspects of the data holding/information system in question:

- The data holding, information system, technology, or program at issue
- The nature and type of personal health information collected, used, or disclosed, or that is proposed to be collected, used, or disclosed
- The sources of the personal health information

- The purposes for which the personal health information is collected, used, or disclosed, or is proposed to be collected, used, or disclosed
- The reason that the personal health information is required for the purposes identified
- The flows of the personal health information
- The statutory authority for each collection, use and disclosure of personal health information identified
- The limitations imposed on the collection, use and disclosure of the personal health information
- Whether or not the personal health information is or will be linked to other information
- The retention period for the records of personal health information
- The secure manner in which the records of personal health information are or will be retained, transferred, and disposed of
- The functionality for logging access, use, modification, and disclosure of the personal health information, and the functionality to audit logs for unauthorized use or disclosure
- The risks to the privacy of individuals whose personal health information is or will be part of the data holding, information system, technology, or program, and an assessment of the risks
- Recommendations to address, eliminate, or reduce the privacy risks identified
- The administrative, technical, and physical safeguards implemented or proposed to be implemented to protect the personal health information

The Privacy Officer is responsible for addressing the recommendations arising from privacy impact assessments. Amendments to CorHealth's privacy and security program may be completed in conjunction with CorHealth information technology, administrative, and data management staff when necessary. Recommendations arising from privacy impact assessments must be addressed within reasonable timeframes established by the Privacy Officer. The Privacy Officer is furthermore responsible for ensuring that recommendations have been implemented.

The implementation of recommendations shall be reviewed by the Privacy Officer along with the privacy impact assessments annually, as part of the Annual Review of the privacy and security program to ensure that all recommendations have been implemented or are being implemented as stipulated by the Privacy Officer.

The Privacy Officer shall maintain a log of privacy impact assessments that have been completed, that have been undertaken but not completed, and have not been undertaken.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually (in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.26 Log of Privacy Impact Assessments

CorHealth maintains a log of privacy impact assessments that have been completed, and of privacy impact assessments that have been undertaken but that have not been completed. The log describes the:

- A description of the data holding, information system, technology, or program involving personal health information at issue
- The date that the privacy impact assessment was completed or is expected to be completed
- The agent(s) responsible for completing or ensuring the completion of the privacy impact assessment
- The recommendations arising from the privacy impact assessment
- The agent(s) responsible for addressing each recommendation
- The date that each recommendation was or is expected to be addressed
- The manner in which each recommendation was or is expected to be addressed

A separate section of the consolidated log of recommendations details the data holdings involving personal health information for which privacy impact assessments not been undertaken. For each such data holding, information system, technology, or program, the log sets out the reasons that a privacy impact assessment will not be undertaken and the agent(s) responsible for making this determination. Alternately, the log sets out the date that privacy impact assessments are expected to be completed for such data holdings, and the agent(s) responsible for completing or ensuring the completion of the privacy impact assessments.

3.27 Policy and Procedures in Respect of Privacy Audits

CorHealth has developed and implemented a policy, "Policy and Procedures for Privacy and Security Auditing", that sets out the requirements for privacy and security auditing. This policy states that CorHealth conducts privacy audits to assess compliance with the privacy policies, procedures, and practices implemented by CorHealth, and audits of the agents permitted to access and use personal health information pursuant to the policy, "Limiting Agent Access to and Use of Personal Health Information". For each audit that is conducted, the policy sets out the purposes of the privacy and security audit, the nature and scope of the privacy audit, the agent responsible for the privacy audit, and the frequency and circumstances in which each privacy audit is required to be conducted. The Privacy Officer is responsible for the development and implementation of an auditing schedule.

Agents who are the subjects of privacy and security audits will be notified in writing at least one day in advance of the scheduled audit by the Privacy Officer and of the process for the audit.

For each type of privacy audit, the "Policy and Procedures for Privacy and Security Auditing" sets out the process to be followed in conducting the audit. Also included, is a discussion of the documentation that must be completed, provided, and/or executed in undertaking each privacy audit. The Privacy Officer is responsible for completing, providing, and/or executing the documentation. The documentation is a template that includes the following information at a minimum:

- Type of Privacy Audit
- Date Privacy Audit Completed
- Person responsible for completing Audit
- Recommendations arising from Audit
- Person responsible for addressing each recommendation

- Date each recommendation was addressed or expected to be addressed
- Manner that each recommendation was or is expected to be addressed

The Privacy Officer and the Director of IT have authority to manage the privacy and security program. The Privacy Officer is responsible for addressing recommendations arising from privacy audits, including the establishment of timelines to address the recommendations, and the monitoring of implementation of the recommendations. The Privacy Officer also identifies the nature of documentation that will be completed, provided, and/or executed at the conclusion of each privacy audit.

Any deficiencies in CorHealth's privacy and security program that are identified as a result of a privacy or security audit are communicated in writing to the Chief Executive Officer of CorHealth by the Privacy Officer, as quickly as is reasonably possible. The results of audits are communicated to CorHealth agents within about one week of the conclusion of the privacy or security audit in most circumstances.

A log of all privacy and security audits is maintained on the main CorHealth shared drive by the Privacy Officer. The Privacy Officer and the Director of IT ensure that the recommendations are implemented within one week of the final review of privacy and security audits unless the recommendation relates to CorHealth's operating environment. Recommendations for changes in CorHealth's operating environment will be implemented in accordance with a timeline set out by the Privacy Officer upon receipt of the recommendation.

Should an agent suspect a breach of the "Policy and Procedures for Privacy and Security Auditing" (breach being defined in the CorHealth policy, "Policy and Procedures for Privacy and Information Security Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Policy and Procedures for Privacy and Information Security Breach Management") to report his/her suspicions to the Privacy Officer as soon as possible. Failure to report a breach or suspected breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.28 Log of Privacy Audits

As set out in the Policy and Procedures for Privacy and Security Auditing, CorHealth maintains a log of privacy audits that is updated every time an audit is conducted. The log includes the following information:

- Type of Privacy Audit
- Date Privacy Audit Completed
- Person responsible for completing Audit
- Recommendations arising from Audit
- Person responsible for addressing each recommendation
- Date each recommendation was addressed or expected to be addressed
- Manner that each recommendation was or is expected to be addressed

The log must be completed by the Privacy Officer and retained by the Privacy Officer on CorHealth's shared drive.

3.29 Policy and Procedures for Privacy Breach and Information Security Breach Management

In response to a recommendation made by the IPC during its review of CorHealth in 2008, CorHealth developed and implemented a new policy, "Information Security and Privacy Breach

Management", for the identification, reporting, containment, notification, investigation, and remediation of privacy and information security breaches. This policy was developed by CorHealth's Privacy Officer in December 2009 and was implemented on April 1, 2010. The policy states that the same set of procedures are to be followed in the event of both privacy and information security breaches.

The "Information Security and Privacy Breach Management" policy defines a privacy breach as an incident in which at least one of the following criteria is met:

- Personal health information is lost, stolen, disclosed to those unauthorized, or subject to unauthorized copying, modification, or disposal
- Personal health information is used for unauthorized purposes
- The collection, use and disclosure of personal health information is not in compliance with PHIPA or its regulation
- Contravention of CorHealth's privacy policies, procedures, or practices
- Contravention of Data Sharing Agreements, Research Agreements, Confidentiality & Non-Disclosure Agreements, and Agreements with Third-Party Service Providers

The policy defines an information security breach as an incident in which any of CorHealth's security policies, procedures, and practices are contravened.

Upon discovering or suspecting a breach, agents must immediately notify the Privacy Officer in oral or written format, as set out in the "Information Security and Privacy Breach Management" policy. The nature of the information that must be provided upon notification and the contact information for the Privacy Officer are set out in the policy. This is a positive duty on CorHealth agents. The Privacy Officer is responsible for determining whether or not the suspected breach has in fact occurred, whether the breach constitutes a privacy breach or information security breach, and whether or not personal health information has been compromised. If the Privacy Officer determines that personal health information has been compromised, he/she is required by the "Information Security and Privacy Breach Management" policy to notify the CEO immediately.

The Privacy Officer is responsible for ensuring that the proper steps are taken, given the particular circumstances of the breach, to immediately contain, investigate, and document the breach. Documentation of the steps required to contain the breach are required to be included on the template for reporting the details of the breach and include a description of the step taken, the date and time, and the agent performing the step. The Privacy Officer is also responsible to ensure that no other personal health information has been compromised, to ensure that no further personal health information can be accessed via the same means, and that no copies of breached personal health information have been made. If the Privacy Officer finds that copies of personal health information have been made, he/she is responsible for retrieving and disposing of all copies in a secure manner and to obtain written confirmation that copies have been disposed of in a secure manner, including the time, date, and method of the disposal.

Once the breach has been contained, the Privacy Officer is responsible for reviewing the steps of containment to ensure that they have been effective. Documentation of the steps of the containment are required to be included on the template for reporting the details of the breach and include a description of the step taken, the date and time, and the agent performing the step.

The Privacy Officer is responsible for consulting with privacy and information security authorities at affected hospitals to ascertain risk and determine what action may be necessary. Written notice should be given to the affected health information custodian, or other organization at the

first reasonable opportunity. The Privacy Officer is required to contact affected hospitals and the health information custodians that provided the personal health information in order to have the health information custodians notify the individuals to whom the personal health information relates, when required pursuant to subsection 12(2) of PHIPA, as opposed to notifying these individuals directly. Additionally, the "Information Security and Privacy Breach Management" policy requires the relevant health information custodian to be advised of the extent of the privacy or information security breach, the nature of the personal health information at issue, the measures implemented to contain the privacy or information security breach, and further actions that will be undertaken with respect to the privacy or information security breach, including investigation and remediation.

The Privacy Officer must also take or recommend any remedial action required, and provide notice, where appropriate, to the hospital(s), the IPC (with reference to Guides such as the IPC's "What to do When Faced With a Privacy Breach: Guidelines for the Health Sector"), and the CEO, at first reasonable opportunity. Notice should include a description of the privacy or security breach, the measures implemented, and any further actions that will be undertaken.

The Privacy Officer is responsible for the investigation of the breach, including determining the nature, scope, and documentation of the investigation. According to the "Information Security and Privacy Breach Management" policy, the Privacy Officer's investigation may include interviews with agents or other individuals associated with the breach. Documentation of the steps of the investigation are required to be included on the template for reporting the details of the breach and include a description of the step taken and associated findings, the date and time, and the agent performing the step. The Privacy Officer is responsible for the findings of the investigation, including the recommendations arising from the investigation and the status of their implementation. Documentation of the recommendations, the date of implementation, and the agent responsible for implementation are required to be included on the template for reporting the details of the breach.

The Privacy Officer has developed a template for documenting and reporting the details of the breach to the CEO, at first reasonable opportunity, which includes the following information:

- Recipient (the CEO)
- Date sent to CEO
- Prepared by (CorHealth Privacy Officer)
- Tracking Number
- Incident classification:
    - Privacy breach
    - Information security breach
    - Near miss
    - Privacy practices not followed
- Resolution closure (indication y/n)
- Name, organization, and contact information of the individual reporting the suspected breach
- Date the suspected breach occurred
- Location of the suspected breach
- Names and roles of the individuals involved
- Type of information used/disclosed inappropriately
- Description of immediate steps to contain the incident
- Timeline of events
- Recommendations to prevent reoccurrence of breach

- Comments on resolution
- Date of resolution

As set out in the "Information Security and Privacy Breach Management" policy, CorHealth maintains a log of privacy breaches. The Privacy Officer is responsible for maintaining the log of privacy breaches.

Recommendations made in these reports are compiled with other recommendations in CorHealth's consolidated log of recommendations. The consolidated log of recommendations is maintained by the Privacy Officer. The policy sets out the manner and format in which the findings of the investigation of the privacy breach are communicated. The Privacy Officer is responsible for setting a timeline for the completion of the recommendations made as the result of the investigation of a privacy or information security breach and the implementation of those recommendations.

The policy addresses whether the process to be followed in identifying, reporting, containing, notifying, investigating, and remediating a privacy breach is different where the breach is both a privacy breach or suspected privacy breach, as well as an information security breach or suspected information security breach.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". CorHealth has information security audit practices that can identify cases in which personal health information has been compromised within the CorHealth network. Additionally, CorHealth's Privacy Officer audits the CorHealth shared hard drive for evidence of unauthorized personal health information on at least an annual basis. Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.30 Log of Privacy Breaches

As set out in the "Information Security and Privacy Breach Management" policy, CorHealth maintains a log of privacy breaches. The Privacy Officer is responsible for maintaining the log of privacy breaches. The following information is recorded using a template developed by the Privacy Officer:

- The date of the privacy breach
- The date that the privacy breach was identified or suspected
- Whether the privacy breach was internal or external
- The nature of the personal health information that was the subject matter of the privacy breach and the nature and extent of the privacy breach
- The date that the privacy breach was contained and the nature of the containment

measures
- The date that the health information custodian or other organization that disclosed the personal health information to CorHealth was notified
- The date that the investigation of the privacy breach was completed
- The agent(s) responsible for conducting the investigation
- The recommendations arising from the investigation
- The agent(s) responsible for addressing each recommendation
- The date each recommendation was or is expected to be addressed
- The manner in which each recommendation was or is expected to be addressed

3.31 Policy and Procedures for Privacy Complaints and Privacy Inquiries

In response to a recommendation made by the IPC during its review of CorHealth in 2008, CorHealth revised its policy on receiving, documenting, tracking, investigating, remediating, and responding to privacy inquiries and complaints made by individuals. The policy, "Privacy Inquiries and Complaints", articulates CorHealth's commitment to remain open to the questions and concerns of the public. It was developed by CorHealth's Privacy Officer in July 2008 and took effect in November 2008.

Under the "Privacy Inquiries and Complaints" policy, "Complaints" are defined as "concerns or complaints relating to the privacy policies, procedures, and practices implemented by the prescribed person, and related to the compliance of the prescribed person with PHIPA and its regulation". The policy defines "Inquiries" as "inquiries relating to the privacy policies, procedures, and practices implemented by the prescribed person, and related to the compliance of the prescribed person with PHIPA and its regulation".

The policy requires CorHealth to receive and respond to complaints, inquiries, and comments made by any individual. The policy, which is publicly available on CorHealth's website, provides that these communications should be directed to the Privacy Officer, and provides contact information for CorHealth's provincial office, CorHealth's Privacy Officer, and the office of the IPC. Contact information for CorHealth's Privacy Officer is also included in brochures given to participating hospitals.

The "Privacy Inquiries and Complaints" policy states that individuals who have complaints or inquiries relating to CorHealth's compliance with PHIPA and its regulation may be able to direct those complaints or inquiries to the IPC.

CorHealth's policy on privacy inquiries and complaints sets out that the Privacy Officer is responsible for receiving communications from the public relating to privacy and lists the documentation that must be completed, provided, and/or executed by the individual making a complaint or inquiry, the content required, and the nature of the information that will be requested from the individual.

All privacy complaints will be investigated. If a breach of CorHealth's privacy and security policies, procedures, and practices is alleged, the Privacy Officer must determine whether there has been a breach of the privacy and security policies, procedures, and practices. If a privacy breach has been identified it will be dealt with according the policy, "Information Security and Privacy Breach Management". The policy sets out the processes and the time frame within which the Privacy Officer must make their determinations in regard to investigation of a complaint or inquiry, in addressing the recommendations, if any, arising from these processes, in communicating the findings, the documentation that must be completed, provided, and/or executed, and the required content of the documentation.

The Privacy Officer is responsible for providing a letter to the individual who made the complaint, acknowledging receipt of the complaint, advising that an investigation will be undertaken, explaining the investigation procedure, setting out the time frame for completing the investigation, and identifying the nature of the documentation that will be provided to the individual following the investigation.

The individual who made the privacy complaint will be notified in writing of the nature and findings of the investigation and of the measures taken, if any, in response to the complaint. The individual will be advised that he or she may make a complaint to the IPC and provided contact information for the IPC.

All inquiries and complaints will be responded to, in writing, even if it is determined that the inquiry or complaint is without validity (i.e., the inquiry or complaint does not pertain to CorHealth's privacy and security program and practices). In such cases, the Privacy Officer will provide a letter to the individual, who made the complaint, acknowledging receipt of the complaint, providing a response, advising that an investigation will not be undertaken, advising that the individual may make a complaint to the IPC, and providing contact information for the IPC. The Privacy Officer will also provide any other affected organizations, such as health information custodians, with a letter outlining the complaint at the first reasonable opportunity.

As set out the in policy, "Privacy Inquiries and Complaints", all complaints and inquiries will be tracked using the "Privacy Complaints Template". The Privacy Officer will maintain a log of privacy inquiries and complaints which indicates whether or not recommendations arising from the investigation of privacy complaints are addressed within the specified timelines, where documentation relating to the receipt, investigation, notification, and remediation of privacy complaints will be retained, and the agent responsible for retaining this documentation.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Audits of this policy involve the Privacy Officer's review of completed and ongoing investigations of legitimate complaints. Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report their suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

3.32 Log of Privacy Complaints

As mentioned above, the Privacy Officer is responsible for maintaining and updating CorHealth's log of privacy complaints. The log includes the following information:

- The date that the privacy complaint was received and the nature of the privacy complaint
- The determination as to whether the privacy complaint will be investigated and the date that the determination was made

- The date that the individual making the complaint was advised that the complaint will not be investigated and was provided a response to the complaint
- The date that the individual making the complaint was advised that the complaint will be investigated
- The agent(s) responsible for conducting the investigation
- The dates that the investigation was commenced and completed
- The recommendations arising from the investigation
- The agent(s) responsible for addressing each recommendation
- The date each recommendation was or is expected to be addressed
- The manner in which each recommendation was or is expected to be addressed
- The date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint

To date, CorHealth has not received any privacy complaints.

3.33 Policy and Procedures for Privacy Inquiries

CorHealth has consolidated its policies on privacy complaints and privacy inquiries. The Privacy Officer follows the same procedures when responding to a public inquiry, as he/she does when responding to a complaint from the public, with some additional procedures being followed for privacy complaints as noted.

4 Security Documentation (PART 2)

The following describes CorHealth's policies and procedures in relation to its security policy and procedures.

Note: As a general matter, in relation to all CorHealth policies, its agents are required to sign agreements stating that they understand and will uphold CorHealth's policies at the outset of their relationship with CorHealth and annually thereafter. Should an agent discover or suspect a breach of a policy, CorHealth's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach to CorHealth's Privacy Officer. Disciplinary guidelines for privacy breaches are set out in the CorHealth policy, "Policy and Procedures for Discipline and Corrective Action". If it is determined that there has been a breach of the Confidentiality & Non-Disclosure Agreement signed by agents, CorHealth may seek legal action against the agent(s) responsible.

4.1 Information Security Policy

The "Protection of Personal Health Information" policy sets out that CorHealth must have a credible program to continually assess and respond to threats and risks to the data holdings containing personal health information in CorHealth's custody, and to assess and verify the effectiveness of its security program. This comprehensive security program is designed to protect personal health information in CorHealth's custody against theft, loss, and unauthorized use or disclosure, and to ensure that the records of personal health information are protected against unauthorized copying, modification, or disposal. This policy establishes and documents a methodology for identifying, assessing, and remediating threats and risks, and for prioritizing all threats and risks identified for remedial action. This program is directed by the Privacy Officer, who is responsible for reviewing and amending all security policies. The Privacy Officer is also responsible for overseeing security training and communicating any changes to policies. CorHealth's security policy requires the security program to employ physical, technical, and administrative safeguards that are consistent with established industry standards and practices to maintain the integrity of personal health information. The Privacy Officer is responsible for implementing, monitoring, and reviewing CorHealth's security program.

CorHealth's security program includes:

- A framework for the governance of CorHealth's security program
- Policies and procedures for the administration of training to CorHealth agents
- Policies and procedures for the ongoing review of the security policies, procedures and practices implemented
- Policies and procedures for ensuring the physical security of the premises
- Policies and procedures for the secure retention, transfer, and disposal of records of personal health information, including policies and procedures related to mobile devices, remote access, and security of data at rest
- Policies and procedures to establish user access controls, including user access management, network access controls, operating system access controls, and application, and information access controls
- The maintenance and review of system control and audit logs and security audits

- Policies and procedures for network security management and practices for patch management and change management
- Policies and procedures related to the acceptable use of information technology
- Provisions for back-up and recovery
- Policies and procedures for information security breach management
- Policies and procedures to establish protection against malicious and mobile code

Being a small organization with limited staff, and only two data holdings containing personal health information, CorHealth has not found it necessary to develop formal policies for information systems acquisition, development, and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development, supports procedures, technical vulnerability management, and threat risk assessments. CorHealth has an information technology team, that the Privacy Officer can call on regarding the software or operating environment used by CorHealth and the protection of personal health information in CorHealth's custody. Additionally, CorHealth has not found it necessary to develop formal policies for business requirements or user responsibilities, for the reasons stated above. However, while there are no formal policies related to business requirements and user responsibilities, it is CorHealth's practice to utilize industry best practices.

As required by the policy, "Protection of Personal Health Information", CorHealth has ordered both organization-wide and appropriate project specific threat risk assessments to be conducted by third-party experts, to identify and minimize vulnerabilities, and increase overall security. The last such assessment was conducted in 2017.

CorHealth has technical measures in place to protect its network infrastructure and maintain the integrity of the personal health information in its custody. These include:

- An authenticated, secure network for transferring and accessing all CorHealth information
- The encryption of all personal health information 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 activity
- 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
- The implementation of firewalls to block unauthorized intrusions to CorHealth's network and the use of network intrusion detection software to identify any unauthorized access to the CorHealth network.

The policies associated with CorHealth's security program are subject to regular audits as set out in the policy, "Policy and Procedures for Privacy and Security Auditing". For each policy, "Policy and Procedures for Privacy and Security Auditing" sets out the frequency and nature of the audit, while identifying the agent responsible for carrying out the audit.

All CorHealth agents must comply with the "Information Security" policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". The Privacy Officer or a designate will, annually, review the logs described above. Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and depending on the

circumstances may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.2 Policy and Procedures for Ongoing Review of Security Policies, Procedures, and Practices

A policy and associated procedures ("Annual Review of Privacy and Security Policies and Procedures") have been developed and implemented for the ongoing review of the security policies, procedures and practices put in place by CorHealth. The purpose of the review is to determine whether amendments or new security policies, procedures, and practices are required.

As mentioned above, CorHealth's policy on the review of its security policies has been combined with its policy on review of its privacy policies. The "Annual Review of Privacy and Security Policies and Procedures" requires the Privacy Officer to review privacy and security policies and practices at the beginning of each fiscal year or as otherwise directed by the IPC. The Privacy Officer is required to ensure that CorHealth policy reflects advancements in technology and in industry practices, and to implement initiatives set out by the IPC or changes to relevant laws (i.e. PHIPA and its Regulation). In the event that the law is changed or the IPC issues new orders, guidelines, factsheets, or best practices, the Privacy Officer is required to review and make appropriate changes to policy as soon as is reasonably possible, before the scheduled annual review. Policy reviews are made with respect to recommendations made by the IPC, in privacy impact assessments, privacy and security audits, and in reports arising from complaints, or privacy or information security breaches. In the review process, CorHealth's Privacy Officer also considers the degree to which existing policies have been successfully implemented and the level of consistency among policies and may make recommendations in these regards.

During the reviews of the security policies, procedures, and practices that have occurred since the last 3-year review by the IPC, the Privacy Officer has made only a small number of amendments that are detailed in Section 7 Privacy and Security Indicators (PART 5) of this document.

Under the "Annual Review of Privacy and Security Policies and Procedures" policy, CorHealth's Privacy Officer is responsible for the communication of new or amended policies to the public and to CorHealth agents in written and/or electronic format. The Privacy Officer reviews on an annual basis the manner of communication. The policy also identifies the agents responsible and the procedure that must be followed in obtaining approval of any amended or newly developed security policies, procedures, and practices.

The CEO is ultimately responsible for ensuring that all CorHealth agents comply with "Annual Review of Privacy and Security Policies and Procedures". The Privacy Officer undertakes the day-to-day responsibility for this task.

CorHealth audits the "Annual Review of Privacy and Security Policies and Procedures" in accordance with the procedures set out in its privacy and security audit policy, "Policy and

Procedures for Privacy and Security Auditing". The Privacy Officer is responsible for auditing to ensure compliance with the policy and its procedures annually.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer or her/his designate annually (in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing"). The auditor shall review the completed "Form for Formal Review of Privacy and Security Policies and Procedures" to ensure that the review has been properly conducted and that the recommendations have been properly logged. Should it be determined that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.3 Policy and Procedures for Ensuring Physical Security of Personal Health Information

CorHealth has developed the policy, "Physical Security", addressing the physical safeguards to protect personal health information against loss, theft, unauthorized use or disclosure, and unauthorized copying, modification, or disposal. CorHealth's safeguards include:

- Tracked card access which divides the facility into varying levels of security with each successive level being more secure and restricted to fewer individuals
- Access to the server room (where personal health information is retained on database servers) requires that individuals successfully pass through multiple levels of security

4.3.1 Policy, Procedures and Practices with Respect to Access by Agents

As set out in the policy, "Physical Security", the Privacy Officer is responsible for granting, reviewing, and terminating access by agents to the CorHealth provincial office premises and to the secure server room, where personal health information is stored. The secure server room is the only area in the building where records of personal health information are permanently retained. Access is granted to agents if it is absolutely necessary for the fulfillment of their contractual, employment, or other obligations. Currently, only management, IT staff, and employees of Interface Technologies, CorHealth's IT service provider, have access to the server room to perform maintenance. This privilege is given to these agents, conditional on a continued need, to fulfil the agent's job description or contractual duties. Under CorHealth's service agreement with Interface Technologies, agents of Interface Technologies are forbidden from accessing or using personal health information. The Privacy Officer's responsibilities include the procurement of badges and security authorization from the building's security team. An indication as to whether or not an agent has been granted access to the secure server room, in addition to a brief explanation of the purpose for access, must be provided by the Privacy Officer in the log of agents with access to the provincial office.

The "Physical Security" policy sets out that the Privacy Officer is responsible for providing access cards to agents and for logging that information in the log of agents with access to the provincial office.

The Privacy Officer is responsible for maintaining a log of agents granted access to the premises and to the secure server room, including the name of the agent, the level and nature of the access granted, the locations within the premises to which access is granted, the date that the access was granted, the date(s) that identification cards, access cards and/or keys were provided to the agent, the identification numbers on the identification cards, access cards and/or keys, if any, the date of the next audit of access, and the date that the identification cards, access cards and/or keys were returned to the prescribed person or prescribed entity, if applicable.

4.3.2 Theft, Loss and Misplacement of Identification Cards, Access Cards and Keys

To protect the physical security of its provincial office, CorHealth requires its agents to use access cards to gain entry to the premises. Additionally, certain filing cabinets and storage rooms are locked with conventional keys. It should be noted that in accordance with the policy, "Secure Retention of Personal Health Information", no personal health information is stored within these filing cabinets and storage rooms. The theft, loss, or misplacement of keys and access cards is governed by the "Physical Security" policy. This policy sets out that keys and access cards provided to agents are the responsibility of the agent, and that any loss of keys or access cards must be reported in oral or written format to CorHealth's Privacy Officer immediately.

If an agent loses an access card, the Privacy Officer will notify building security, who will deactivate the missing card and provide the agent a new card at their own expense. Temporary replacement access cards will not be issued. In the event of a missing key, the Privacy Officer is required to consult with administrative and operations staff. If the contents of the room or filing cabinet that could be accessed with the key are sensitive enough to affect the services provided by CorHealth or the organization's reputation, the locks will be replaced. In either case, the Privacy Officer is required to complete a form that documents the date that the access card or key was lost, the contents of the location that could be accessed using the access card or key, the measures taken to protect the integrity of the CorHealth office, and a description of these measures. These forms are retained in a repository by the Privacy Officer.

4.3.3 Termination of the Employment, Contractual or Other Relationship

As stated above, the Privacy Officer is responsible for the granting and termination of access by agents to the CorHealth provincial office and the secure server room. CorHealth's policy that sets out the procedures for the termination of employment ("Termination of Employment") states that the Privacy Officer must collect all CorHealth property (keys, identification tags, passwords, among other items) from individuals whose employment has been terminated. Because of the limited number of people employed by CorHealth (currently 50 people including management, executive, and temporary contractors) and the CEO's practice of providing notification to all staff of agent termination and other staffing updates, it is unlikely that an agent could end his/her employment without the knowledge of the Privacy Officer. Agents who resign their position with CorHealth are required to give prior notice of 2-6 weeks, depending on the nature of their position and specific employment contract.

4.3.4 Notification When Access is No Longer Required

Currently, the only CorHealth agents with access to the locked server room, where personal

health information is stored, are management, IT staff, and employees of Interface Technologies. All groups require access for the fulfilment of their job description or contractual obligations, and those requirements are unlikely to change for any group. Because it is not likely that an agent with access to the server room would see their job description or contractual obligations change radically, CorHealth does not require a policy requiring agents to provide notification when access is no longer required.

4.3.5 Audits of Agents with Access to the Premises

Because of the small number of people who have relationships with CorHealth, it is not reasonably conceivable that the even smaller number of agents with access to the secure server room could maintain that access despite their relationship having been terminated. As such, CorHealth does not conduct audits of the roll of agents with access to the secure server room and it does not have a written policy for that purpose. The Privacy Officer reviews building records related to access into CorHealth's suites annually, in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing").

4.3.6 Tracking and Retention of Documentation Related to Access to the Premises

The Privacy Officer is required by the "Physical Security" policy to maintain a log of agents granted access to the CorHealth provincial office and to the secure server room that houses personal health information, the name of the agent granted approval to access the premises, the level and nature of the access granted, the locations within the premises to which access is granted, the date that the access was granted/identification cards, access cards and/or keys were provided to the agent, the identification numbers on the identification cards, access cards and/or keys, if any, and the date that the identification cards, access cards and/or keys were returned to Privacy Officer, if applicable. Building security provides written reports as needed, or if there is suspicious activity.

4.3.7 Policy, Procedures and Practices with Respect to Access by Visitors

CorHealth has developed a policy, "Physical Security", for access to the CorHealth provincial office premises by visitors. This policy defines "visitor" as any individual who is not party to a contractual or other written agreement with CorHealth and who is present at the CorHealth premises with the specific intent of visiting a member of the CorHealth staff. Because CorHealth is not a public access office, its doors are locked at all times. Visitors must announce themselves by ringing the bell outside of the office door. If the individual is not recognized or expected by the front receptionist, the individual is not admitted to the premises. Upon reception of a visitor, the receptionist is required to notify the CorHealth agent that the visitor requests. That agent must accompany the visitor at all times.

CorHealth's office is laid out such that some visitors who come for meetings do not have to cross the door locked by a key card. Visitors expected for meetings in the main boardroom, who are signed in by the receptionist, may enter the main boardroom without accompaniment by a CorHealth agent. There is a locked door accessible only by key card separating the main board room from the rest of CorHealth's office, and with the exception of the main boardroom, access to CorHealth's offices are locked to visitors at all times.

Visitors to the CorHealth office must sign in at the front office. CorHealth's receptionist is required to provide the visitor with a name badge and to record in a log the following:

- Name of visitor

- Time received
- Time of departure
- Purpose of visit (name of CorHealth agent who they are visiting)

Because CorHealth only distributes simple name badges to visitors, it has not found it necessary to develop procedures for circumstances in which visitors do not return the identification provided to them by the receptionist. Badges are simple paper name tags and do not allow access to any of the secure areas of the office. If proper documentation required for a visit has not been completed, the Privacy Officer is required to meet with the receptionist to emphasize the importance of the appropriate documentation.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.4 Log of Agents with Access to the Premises of the Prescribed Person

As stated above, the Privacy Officer is required by the "Physical Security" policy to maintain a log of agents granted access to the CorHealth provincial office and to the secure server room that houses personal health information. The log records the name of the agent granted approval to access the premises, the level and nature of the access granted, the locations within the premises to which access is granted, the date that the access was granted, the date(s) that identification cards, access cards and/or keys were provided to the agent, the identification numbers on the identification cards, access cards and/or keys, if any, the date of the next audit of access, and the date that the identification cards, access cards and/or keys were returned, if applicable.

4.5 Policy and Procedures for Secure Retention of Records of Personal Health Information

CorHealth's policy, "Secure Retention of Personal Health Information" sets out that all personal health information is to be stored on CorHealth's secure network, which is comprised of database servers in the locked server room in CorHealth's provincial office. CorHealth agents are prohibited from retaining personal health information on paper. Furthermore, CorHealth is only accessible by security pass which ensures another layer of protection. In the event that the "Secure Retention of Personal Health Information" policy is breached and an agent possesses personal health information in paper format, the personal health information on paper is disposed of in locked bins and on a monthly basis collected by Shred-It, an external company

whose employees are bonded. The Privacy Officer is responsible for ensuring that all agents follow this policy and all personal health information in CorHealth's custody is retained in a secure manner. Breaches of the "Secure Retention of Personal Health Information" policy are to be resolved following the procedures set out in the "Information Security and Privacy Breach Management" policy.

Personal health information in CorHealth's custody is only retained as long as is reasonably necessary, which currently means for as long as is reasonably necessary for long-term statistical analysis.

CorHealth does not use or disclose personal health information for research purposes except to ICES under a data sharing agreement, and as such does not require procedures for that purpose.

Personal health information that is subject to data sharing pursuant to a data sharing agreement is to be retained according to the provisions in the agreement. It is forbidden for either party to a data sharing agreement to retain personal health information for any period longer than what is set out in the agreement.

CorHealth employs a number of safeguards, set out in the policy, "Protection of Personal Health Information", to ensure that the records of personal health information in its custody are protected against theft, loss and unauthorized use or disclosure and to ensure that personal health information is protected against unauthorized copying, modification or disposal. These safeguards include:

- The development and implementation of privacy and security policies and procedures
- Annual privacy and security training
- Privacy training for all new staff
- Requiring employees, consultants, volunteers, and members of the Board of Directors to sign confidentiality agreements that clearly describe their obligations with respect to protecting the privacy of individuals with respect to that information
- Requiring consultants, contractors, and vendors to sign agreements outlining their obligations to protect personal health information
- Requiring Participation Agreements to be executed prior to the collection of personal health information from participating hospitals
- CorHealth is located in a locked facility with external video monitoring
- Tracked card access which divides the facility into varying levels of security with each successive level being more secure and restricted to fewer individuals
- Access to the server room requires that individuals successfully pass through multiple levels of security
- The use of firewalls, and network and workstation encryption and network intrusion detection software; and
- A credible program for continuous assessment and verification of the effectiveness of the security program to deal with threats and risks to data holdings containing personal health information

Personal health information is transferred to a third-party service provider for long-term tape backup. Long-term tape backup storage ensures that the CorHealth database is secure in the event of a disaster affecting the database held at CorHealth's provincial office. Currently, long-term tape backup storage services are provided by Recall.

Tape backups, which are taken daily, are required to be provided to representatives from the third-party service provider twice weekly by the Director of IT. The backups must be provided to the representative in a locked metal box. The same locked metal box will be provided back to the Director of IT upon request. These procedures are compliant with the CorHealth policy,

"Secure Transfer of Personal Health Information".

The Director of IT is required by the "Secure Retention of Personal Health Information" policy to document the date, time, and mode of transfer and to maintain a repository of written confirmations received from the third-party service provider upon receipt of personal health information.

CorHealth's Director of IT maintains a detailed inventory of personal health information being transferred to the third-party service provider and received from the third-party service provider.

Personal health information may only be transferred to a third-party service provider if it has executed a contract with CorHealth modelled on the "Template Agreement for All Third-Party Service Providers" that was developed by the IPC. The Privacy Officer is responsible for ensuring that such a contract is executed prior to transferring the records of personal health information for secure retention.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.6 Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices

The "IT Policy: Email, Internet, and Computing Devices" expressly forbids the retention of personal health information on mobile devices. Personal health information can only be stored electronically on CorHealth's secure network.

Mobile Devices are defined as but are not limited to:

- Laptops
- Personal Digital Assistants (PDAs)
- Tablets
- Smart phones
- Mobile phones
- Blackberries
- Any portable storage device that could be used to digitally/electronically copy, transcribe, or store files.

The policy additionally prohibits agents who are working remotely from accessing personal health information, when outside of the CorHealth network.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by

CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.7 Policy and Procedures for the Secure Transfer of Personal Health Information

CorHealth has developed a policy and associated procedures for the secure transfer of personal health information ("Secure Transfer of Personal Health Information"). This policy sets out that all transmissions of personal health information must be done in a secure manner and provides all the means by which personal health information may be transferred. Any other method of transferring personal health information is prohibited. According to the policy, CorHealth's Privacy Officer is responsible for ensuring that these transfers are made in a secure manner.

CorHealth only permits the transfer of personal health information via secure connection and at least industry standard encryption. These transmissions were primarily made to CorHealth by Cancer Care Ontario, who received personal health information from Data Clerks and Regional Cardiac Care Coordinators at CorHealth hospitals. However, in July 2017, CorHealth repatriated the Wait Time Information System (WTIS-CCN), into which personal health information is entered by hospitals and where it resides for the purposes of reporting and analysis. Since repatriation, CorHealth receives personal health information directly from Data Clerks and Regional Cardiac Care Coordinators at CorHealth hospitals. Additionally, CorHealth provides personal health information to ICES as per its data sharing agreement via SFTP. Finally, personal health information may be transferred to a third-party service provider on tape storage within a locked metal box for long-term backup. CorHealth prohibits the transfer of personal health information using other media, including paper.

CorHealth's IT staff members are required by the "Secure Transfer of Personal Health Information" policy to ensure that SFTP transmission metadata is logged. Currently, this is done automatically by the database server software. These logs must be retained on the CorHealth shared server for later review and auditing.

Third-party service providers who store CorHealth database tape backups are required to provide CorHealth with forms confirming that the data was transferred when the metal box is given to the provider's representative and when the metal box is returned to CorHealth. CorHealth's IT Manager is responsible for maintaining a repository of these forms.

Passwords for encrypted files are provided to service providers under a separate cover.

The "Secure Transfer of Personal Health Information" policy was developed with respect to orders, guidelines, fact sheets, best practices issued by the IPC, and existing privacy and security standards and best practices. In accordance with the policy, "Review of Privacy and Security

Policies and Procedures", CorHealth's Privacy Officer reviews the "Secure Transfer of Personal Health Information" policy and all policies on an annual basis, keeping abreast of evolving privacy and security standards and best practices. If the IPC issues new orders, guidelines, fact sheets, or best practices, or the Government of Ontario introduces new legislation or amends existing legislation, the Privacy Officer is responsible for making required amendments as soon as is reasonably possible.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.8 Policy and Procedures for Secure Disposal of Personal Health Information

CorHealth has developed and implemented the policy, "Destruction of Personal Health Information", governing the secure disposal of personal health information. Here, "destruction" is used synonymously with "disposal". This policy provides that "when personal health information is no longer required it must be destroyed" and defines destruction as "in a manner that prevents re-assembly, recovery, or discovery of the information by way of reasonable effort".

The "Destruction of Personal Health Information" policy lists the means by which records of personal health information may be disposed. It should be noted, that the CorHealth policy, "Secure Retention of Personal Health Information" forbids the retention of personal health information on any medium other than the secure CorHealth server or its tape backups. CorHealth has developed procedures for the disposal of personal health information on other media, as a contingency in the event that the "Secure Retention of Personal Health Information" policy is contravened. For the destruction of paper personal health information, CorHealth has a third-party agreement with Shred-It. For the secure disposal of electronic personal health information, CorHealth provides its own destruction. It is highly uncommon for CorHealth to require disposal of personal health information on any medium other than the secure servers or their tape backups.

- For records of personal health information on paper:
    - Agents who dispose of personal health information on paper are required to complete the "Form for the Transfer of Personal Health Information for Disposal", which collects information about the nature and format, including a detailed inventory related to the records transferred to Shred-It for disposal. The Privacy Officer reviews the agent's actions to determine whether a breach has occurred according to the procedures set out in the "Information Security and Privacy

Breach Management" policy
    - The Privacy Officer is responsible for maintaining a repository of these forms
    - The Privacy Officer is required to ensure that an agreement, using relevant language from the template provided by the IPC, has been executed with Shred-It prior to the transfer of personal health information for disposal to Shred-It
    - Records are disposed of in locked bins operated by Shred-It, a third-party contractor whose employees are bonded
    - Shred-It's agreement with CorHealth stipulates that Shred-It must provide secure transportation of material to its facility, to shred (by cross shredding) the material within 24 hours of its arrival and to provide a certificate of destruction upon completion
    - The Privacy Officer is responsible for maintaining a repository of certificates of destruction provided by Shred-It
    - If Shred-It fails to provide CorHealth with a certificate of destruction, the Privacy Officer will contact the Shred-It office to seek an explanation. If problems persist, the Privacy Officer may choose to terminate the contract
    - The Privacy Officer is responsible for ensuring that transfers of paper, which may include personal health information, are made in a secure manner
    - The Privacy Officer must document the mode, time, and date of the transfer of paper records to be shredded by Shred-It

- For personal health information on CD or DVD:
    - Any information printed on the CD that describes the CD's contents, author, owner, sender, and/or recipient is blacked out with permanent marker
    - Using scissors, the disk's optical (data) surface is scratched from the center outwards to the rim. Several deep scratches are made
    - Using scissors or other implements, the disk is cut or broken into several pieces
- For personal health information on magnetic tape or floppy diskette:
    - Any information printed on the magnetic tape or floppy diskette that describes the magnetic tape or floppy diskette's contents, author, owner, sender and/or recipient is blacked out with permanent marker
    - The housing of the tape or diskette is broken apart
    - The magnetic tape or the floppy diskette is removed
    - The magnetic material is bent, torn, and otherwise cut up. Shredding is acceptable
- For personal health information on flash memory cards and/or USB devices:
    - Any information printed on the device that describes the device's contents, author, owner, sender, and/or recipient is blacked out with permanent marker
    - The contents of the portable memory device are deleted
    - The memory card or USB device is broken into pieces
- For personal health information on hard disk:
    - The disk(s) is/are removed from the computer housing
    - The disk pack chassis is opened, and the platters are removed by force, if necessary
    - The platters are deformed with pliers or holes are drilled through the platters

The "Destruction of Personal Health Information" policy was developed with respect to PHIPA and its Regulation, as well as orders, fact sheets, best practices guidelines issued by the IPC, and existing privacy and security best practices. In accordance with the "Review of Privacy and

Security Policies and Procedures", the Privacy Officer reviews the "Destruction of Personal Health Information" policy and all policies on an annual basis, keeping abreast of evolving privacy and security standards and best practices. If the IPC issues new orders or guidelines, or the Government of Ontario introduces new legislation or amends existing legislation, the Privacy Officer will make required amendments as quickly as possible.

The storage of records of personal health information awaiting disposal is governed by the "Secure Retention of Personal Health Information" policy, which dictates that all personal health information must be stored on CorHealth's secure network or its tape backups, which are handled by Recall. Additional procedures in the "Destruction of Personal Health Information" policy set out that personal health information awaiting disposal must be segregated from other records and listed as such.

It should be emphasized that as set out in CorHealth's policy on secure retention of personal health information ("Secure Retention of Personal Health Information"), CorHealth does not tolerate the retention of personal health information on paper, compact disk, mobile device, or any other storage medium but its secure servers and their tape backups. The procedures for the secure disposal of personal health information on these and other formats included in the "Destruction of Personal Health Information" policy were developed for instances in which the provisions in the "Secure Retention of Personal Health Information" policy are not followed. That CorHealth has procedures for the disposal of personal health information retained on media other than its secure servers should not be taken to mean that such methods of retention are sanctioned.

All transfers of personal health information for disposal are conducted in compliance with the CorHealth policy, "Secure Transfer of Personal Health Information".

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.9 Policy and Procedures Relating to Passwords

CorHealth has developed the policy, ""Password Policy", governing the passwords used by agents to access their accounts on the CorHealth network. The "Password Policy" requires agents to not share their passwords with anyone and to take reasonable steps to protect them from being compromised. Passwords are valid for 90 days, after which the agent will be prompted to change their password. After a password expires, it cannot be used again for two full 90-day periods. Passwords must be at least eight characters long and contain characters from at least three of the following four categories:

- Uppercase characters (A through Z)
- Lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (!, #, %, $)

This policy is enforced through technical safeguards in the Windows Server operating system. These password requirements are programmed into the Windows Server administrative settings, which are only accessible to management IT staff who have been authorized by the Privacy Officer.

Three consecutive failed attempts to log into a staff workstation will trigger an automatic lock on the account, preventing the user from accessing the computer and the CorHealth network. This lock can be removed only by a CorHealth system administrator. The mandatory system-wide password-protected screen saver is triggered, after five minutes of inactivity.

The policy is in alignment with orders, guidelines, fact sheets, and best practices issued by the IPC, as well as evolving privacy and security standards and best practices. In order to ensure the policy remains in alignment, CorHealth audits the "Password Policy", in response to issuing of any orders, guidelines, fact sheets, and best practices issued by the IPC, in addition reviewing it in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), under which the Privacy Officer is responsible for auditing the policy annually.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". This policy is enforced through technical safeguards in the Windows Server operating system. Password requirements are programmed into the Windows Server administrative settings, which are only accessible to management IT staff who have been authorized by the Privacy Officer. The Privacy Officer or a designate will, annually, audit the CorHealth shared drive for evidence of unauthorized personal health information. Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.10 Policy and Procedure for Maintaining and Reviewing Specialized Assessments and System Control and Audit Logs

CorHealth has developed a policy on specialized assessments and system control and audit logs called "Maintenance and Review of Specialized Assessments and System Control and Audit Logs". This policy was created with regard to evolving industry practices, the risks and threats to the CorHealth network, the number of agents with access to personal health information, and the amount and nature of the personal health information in CorHealth's custody.

The "Maintenance and Review of Specialized Assessments and System Control and Audit Logs" policy sets out that the Privacy Officer is responsible for creating audit logs of all accesses to personal health information. Report software running from the CorHealth office that is used by CorHealth agents authorized to access and use personal health information and by authorized staff at participating CorHealth hospitals is required to automatically log the maximum amount of user information that the software allows. This means that the username, time of login, time of logout, number of login attempts, and personal health information accessed is collected and logged automatically. Prior to July 2017, the CorHealth Cardiac and Vascular Registry application (WTIS-CCN) was hosted by Cancer Care Ontario, whose staff members log the username, time of login, and changes made to both databases. Neither software logged geographic information because of the limited number (20 participating hospitals and the provincial office) of sites from which CorHealth network can be accessed through the firewall. After repatriating the WTIS-CCN, CorHealth logged this information solely.

The replication of CorHealth data between servers is monitored in real time, with automatic alerts for problems or inconsistencies.

CorHealth's contracted IT service provider, Interface Technologies, monitors system performance by:

- Reviewing available MBs performance counter, processor time counter, committed bytes in use performance counter, disk usage, and performance log
- Monitoring filtering application
- Monitoring system logs on Windows Servers to identify any repetitive warning and error logs

On a weekly basis, CorHealth's Director of IT audits the CorHealth network antivirus threat report and update logs.

The system control and audit logs track any time PHI is accessed through CorHealth's reporting tools, and include the following:

- The date and time that PHI is accessed
- The date and time of the disconnection
- The user accessing PHI
- The network name or identification of the computer through which the connection was made
- The operations or actions that create, amend, delete, or retrieve PHI and their nature, date and time, and the name of the user performing them

On a monthly basis, CorHealth's Director of IT audits the following:

- System control and audit logs
- Security logs
    - Match security changes to known, authorized configuration changes
    - Investigate unauthorized security changes discovered in security event log
    - Verify that SMTP does not relay anonymously
    - Verify that SSL is functioning for configured security channels
    - Examine fail attempt logs/access log to CorHealth registries
- CorHealth remote access logs
- Verify and filter application and system logs on the remote servers to see all errors, repetitive warnings, and respond to discovered failures and problems
- Track login failure and access time

These logs are required by the policy to be immutable and only accessible to the Privacy Officer and the Director of IT. To achieve this, the logs may be retained on a partition of the network hard drive that is inaccessible to all users except for the Privacy Officer and the Director of IT. These logs are retained for at least one year by the Director of IT.

The review of the audit logs is not required to be documented unless the reviewer identifies a problem. If this occurs, the Director of IT is required to record the error, the time or the error, the time that the error was identified, the steps taken to resolve the error, and the name of the reviewer in a Log of System Errors. This log is accessible to the Privacy Officer, who must be notified as soon as is reasonably possible, in written or oral format, by the Director of IT in the event that a problem is not easily resolvable or unauthorized access is suspected. The Privacy Officer will work with the Director of IT to develop timelines to address the error discovered, dependent on the nature of the error, and be responsible for tracking and ensuring the findings have been addressed. The "Maintenance and Review of Specialized Assessments and System Control and Audit Logs" policy states that CorHealth's Privacy Officer is responsible for ensuring that these audits are in fact conducted by the Director of IT.

If the Director of IT discovers a problem in one of these logs, he/she must as soon as possible take steps to resolve it. If the problem is not easily resolvable and changes to CorHealth's software or network infrastructure are required, the IT staff member who identified the problem will notify the Privacy Officer. The "Maintenance of System Control and Audit Logs" policy states that the Privacy Officer tracks the findings of the review of the system control and audit logs to ensure they have been addressed within identified timelines in the course of a formal privacy and security audit or review.

If in the course of completing these audits, the Director of IT suspects that there has been a breach (as defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the procedures set out in the CorHealth policy, "Information Security and Privacy Breach Management" will be followed, and the Chief Executive Officer must be notified by the Privacy Officer, in written format, as quickly as is reasonably possible.

All audits shall be logged using the Privacy and Security Audit Form. These forms shall be gathered and stored by the Privacy Officer and retained indefinitely.

Any other findings in these audits that are of relevance to CorHealth's IT staff are communicated by the Director of IT to relevant IT staff promptly in electronic format.

The Maintenance and Review of Specialized Assessments and System Control and Audit Logs also sets out the requirement to perform threat risk assessments, vulnerability assessments, penetration testing, and ethical hacks on CorHealth systems at minimum every three years, upon the introduction of new systems, when there are changes made to existing systems, technologies, or programs involving personal health information, where there is a major change to the privacy and security program, upon recommendation from the IPC, or upon a breach as defined in the "Policy and Procedures for Privacy and Information Security Breach Management", as applicable.

CorHealth audits the "Maintenance and Review of Specialized Assessments and System Control and Audit Logs" policy in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing") under which CorHealth's Privacy Officer is responsible with auditing for compliance with this policy annually.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent

of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.11 Policy and Procedures for Patch Management

CorHealth has developed and implemented a policy and associated procedures for patch management ("Patch Management Policy").

The "Patch Management Policy" sets out that network administrators at Interface Technologies, CorHealth's contracted third-party IT service provider, is responsible for monitoring the availability of patches on behalf of CorHealth. The policy further states that this monitoring is conducted on a constant basis, as patches become available from software vendors. The policy also states that Interface Technologies is responsible for analyzing the patch and making the determination as to whether it should be implemented. The policy states that Interface Technologies must consider all associated patch documentation, perform risk and relevancy assessments, and consider criteria including severity, classification, and applicability in making its determination.

The "Patch Management Policy" states that patches classified as critical or for security by Interface Technologies are downloaded automatically, while service packs, non-critical hotfixes, and non-security patches will be tested in a lab environment before being promptly implemented.

Interface Technologies is responsible for documenting the rationale for each patch that is implemented or not implemented. This documentation must include a description of the patch, the date that the patch became available, the agent responsible for implementing the patch, the date of implementation, the agent responsible for testing the patch, the date of the testing of the patch, whether or not the testing was successful, the severity level and priority of the patch, the information system, technology, equipment, resource, application or program to which the patch relates, updates status, computer status, and synchronization results.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined

in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.12 Policy and Procedures Related to Change Management

As a result of its small number of employees and the way in which they work together, CorHealth does not require a policy on the management of changes to its operating environment. Where changes are identified, the Privacy Officer, in consultation with CorHealth's IT team, is responsible for establishing a timeline and process for them to be made. CorHealth has hardware not connected to the main network on which different operating environments are tested with CorHealth software. If the new operating environment provides meaningful benefits to the user experience without negatively affecting the performance of CorHealth software, it is adopted. A log of changes implemented is maintained by the Director of IT.

4.13 Policy and Procedures for Back-Up and Recovery of Personal Health Information

CorHealth has developed the policy, "Back-Up and Recovery of Personal Health Information", to govern system backup and recovery in the event of a serious problem. The retention of all backups of personal health information is governed by the policy, "Secure Retention of Personal Health Information". The transfer of all backups of personal health information is governed by the policy, "Secure Transfer of Personal Health Information". The destruction of all backups of personal health information is governed by the policy, "Secure Destruction of Personal Health Information". CorHealth's Privacy Officer is responsible for ensuring that backups of personal health information are retained, transferred, and destroyed in accordance with these policies.

As set out in the "Back-Up and Recovery of Personal Health Information" policy, CorHealth uses the Veeam Backup and Replication Enterprise system, which automatically, backs up information stored on CorHealth servers and workstations, including personal health information, in real time. If the internal CorHealth network were to fail, the Veeam system could restore all lost data. The Veeam system is located on a separate server located in the CorHealth server room. Backups are stored indefinitely. The Veeam software system maintains logs of all of its backup activities which are accessible by CorHealth's IT staff.

To further ensure the security and persistence of CorHealth networks in the event of a disaster, CorHealth is required to have tape backups of its servers performed daily through an external vendor, which stores the tapes at an off-site location. CorHealth is required by the "Back-Up and Recovery of Personal Health Information" policy to execute an agreement with this third-party vendor based on the template developed by the IPC prior to the transfer of backups of personal health information to the third party. The Privacy Officer is responsible for ensuring that this agreement has been executed.

The current agreement is with Recall and ensures that the personal health information in CorHealth's custody is protected and safe. According to the agreement with Recall, CorHealth remains the legal owner of all data and materials transferred to Recall. This transfer is made by handing off a locked metal box containing the database's tape backup to a representative of Recall twice weekly. A rotation of tapes is carried out, as the representative of Recall returns the tapes in the same locked metal boxes to CorHealth for CorHealth to write over and reuse. Every

time the tape backups are given to Recall, CorHealth's IT Manager is required to log that a backup of all servers was given to Recall, along with the time and date, and the representative of Recall is required to provide CorHealth with a form documenting that the backup was received. These forms are retained in a filing cabinet by CorHealth's IT Manager. This method of transfer is compliant with the "Secure Transfer of Personal Health Information" policy. Recall is contractually responsible for the following:

- Protecting personal health information against theft or loss, as well as unauthorized use, disclosure, access, modification, and copying
- Only using the locked box of personal health information in tape format with respect to its agreement with CorHealth
- Not using personal health information for its own benefit or for the benefit of a third party
- Not disclosing personal health information to a third party
- Remaining compliant with provincial privacy legislation
- Remaining compliant with its own privacy and security policies and retaining the employment of a dedicated Privacy Officer
- Providing to CorHealth evidence of its compliance with privacy legislation and its privacy and security program
- Providing notice to CorHealth should Recall receive a complaint from an individual whose personal health information is under CorHealth's custody. Recall will provide all information necessary, unless it is unlawful to do so, for CorHealth's resolution of the complaint at CorHealth's discretion. Recall will implement any changes with respect to CorHealth's orders arising from the complaint at CorHealth's expense
- Recall will notify CorHealth at the first reasonable opportunity should Recall suspect a breach Recall is responsible for any and all costs, fines, damages, penalties, or other liabilities owed to third parties as the result of Recall's non-compliance with the agreement with CorHealth
- Upon the termination or expiry of the agreement, Recall will return all personal health information to CorHealth. If instructed by CorHealth, Recall may instead destroy or make anonymous all personal health information in its care and provide a sworn statement to CorHealth that it has done so

CorHealth's "Template Agreement for All Third-Party Service Providers" was introduced after the execution of CorHealth's service agreement with Recall. As such, the current service agreement does not include all relevant language from the Template. Upon the expiry of the current agreement, or should the agreement come to an early end for whatever reason, and should CorHealth wish to renew its contract with Recall, CorHealth will ensure that the new agreement includes all relevant information from the "Template Agreement for All Third Party Service Providers".

As the tapes that are used in for long-term backup storage are rotated daily and exchanged with Recall twice weekly, CorHealth's IT Manager is able to determine the efficacy of this method of backing-up the CorHealth database on regular and frequent basis. As such, CorHealth has not developed procedures for the testing of this method of backup. The "Back-Up and Recovery of Personal Health Information" policy requires the Director of IT to test the Veeam Backup system on a weekly basis and provide written notification to the Privacy Officer if errors are identified.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for

determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.14 Policy and Procedures on the Acceptable Use of Technology

CorHealth has developed the policy, "IT Policy: Email, Internet, and Computing Devices", which governs the use of CorHealth-supplied technology by its agents. In order to protect the integrity of CorHealth and the CorHealth information technology network and to avoid degrading the performance of CorHealth computing and network resources, the "IT Policy: Email, Internet, and Computing Devices" policy places a number of restrictions on Internet use by CorHealth agents. These are:

- Agents are forbidden from downloading music, video, or other files from the Internet, unless authorized to do so by the Privacy Officer after submitting a written request. The Privacy Officer is required to deny the request unless the file has legitimate value to the agent's work, no file already on the CorHealth network can serve the same purpose, no smaller file is available, the source of the file is reputable and is not likely to produce malicious code, and downloading the file will not significantly degrade Internet speed for other CorHealth agents. If the download is approved, agents are required to save the file locally first so that if the file is infected with malicious code, the problem may be limited to only one workstation. No documentation is required by the policy for these procedures, and the Privacy Officer is not required to pass along notification to any other CorHealth agent. If the download is a software file, installation on a workstation requires the software to be reviewed, approved for use, and installed by a member of the IT staff. All workstations, except for IT staff workstations, are locked to ensure software cannot be installed without prior review and approval. IT staff maintains a log of all approved software installations
- Agents are to exercise discretion when downloading files and content. Such files and content must be from reputable sources and have a clear business purpose
- Agents are to never access websites which contain images, text, or other content which could be considered indecent or offensive, or that may violate the CorHealth Code of Conduct or any other CorHealth policy or procedure
- Agents are not to use the Internet to watch videos, television, sporting events, or other sources of personal entertainment. The viewing and downloading of these file types exposes CorHealth to risk of malicious code and may degrade the performance of CorHealth network systems
- Agents are not to host or post CorHealth information on blogs, chatrooms, user-groups, forums, or other forms of Internet-based communications except when approval is obtained from Corporate Communications. This includes confidential information such as source code, logos, and policies, derogatory or negative comments about CorHealth activities, employees, or clients, and direct or indirect comments regarding proprietary information

- Incidental personal use of the Internet is allowed, but it must never interfere with job responsibilities and work-related needs

The "IT Policy: Email, Internet, and Computing Devices" policy also governs email use by agents, compelling them to adhere to the following rules:

- CorHealth email addresses will be issued to conduct CorHealth business. At no time may email accounts other than CorHealth be used to conduct CorHealth business
- Before sending email, confidential information that is not needed by the recipient must be deleted. For example, delete unnecessary fields or attachments
- When replying to or forwarding an email chain, agents are to review all the emails in the chain to make sure that they are needed by the current recipient
- In all cases, agents must confirm that the recipient's email address is correctly entered in the message's "To" field before sending the message. Agents must not "Reply to All" if some recipients on the address line do not need the information
- In cases involving particularly sensitive information, agents are to request that the recipient first send an email so that the agent can reply directly to their message
- Agents are to never send or forward CorHealth information to or from their own personal email account. Likewise, agents are to never send CorHealth confidential information to a non-CorHealth email account belonging to another party so that agents may then access the information, or have it forwarded
- Agents must use appropriate language in email messages and adhere to CorHealth values and policies. Agents are to use the same rules and the same polite forms of address that they would use in other types of business communication
- Agents are to never reply to emails that they believe to be spam
- Agents are to use discretion when opening attachments to email messages. Agents are to carefully weigh the risk of introducing malicious code such as a virus before opening any attachment
- Agents are to use discretion when forwarding files and other confidential information. Recipients must have a legitimate business need for receiving the information
- CorHealth email addresses are not to be added to mailing lists unless required as part of your assigned job duties. Doing so may lead to CorHealth email systems receiving excessive unwanted mass email (spam.)
- Another user's email account may not be accessed without written, formal authorization from the CorHealth Privacy Officer. The Privacy Officer may only grant an agent access to another user's email account if access is absolutely necessary for ensuring the persistence of CorHealth's critical functions
- CorHealth email accounts are provided to improve productivity. They are not to be used to send or forward material that could be considered indecent or offensive, or that may violate the CorHealth Code of Conduct or any other CorHealth policies or procedures
- All messages sent by email using CorHealth email systems are the property of CorHealth. CorHealth reserves the right to monitor and disclose all messages sent over its email system for any purpose
- Incidental personal use of email is occasionally permitted but it must never interfere with job responsibilities and work-related needs

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may

recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.15 Policy and Procedures In Respect of Security Audits

CorHealth has developed and implemented the policy, "Policy and Procedures for Privacy and Security Auditing", that sets out the requirements for privacy and security auditing. This policy states that CorHealth conducts privacy and security audits to assess compliance with the privacy and security policies, procedures, and practices implemented by CorHealth. Each audit that is conducted includes the purposes of the privacy or security audit; the nature and scope of the privacy or security audit; the agent responsible for the privacy or security audit; and the frequency of each privacy or security audit. In accordance with the policy, "Policy and Procedures for Privacy and Security Auditing", CorHealth will perform audits of its privacy and security program at least annually but also may be conducted upon the request of the IPC or other government entity, as a result of a privacy impact assessment, or upon recommendation following a privacy or security breach.

CorHealth's security auditing program includes requirements for reviews of system control and audit logs, threat and risk assessments, specialized security reviews or assessments, vulnerability assessments, penetration testing, and ethical hacks. These components of CorHealth's security program are governed by the policy, "Maintenance and Review of Specialized Assessments, System Control and Audit Logs". This policy sets out the frequency for each of the aforementioned security audits and states that the Director of IT is responsible for ensuring that a security audit schedule is developed annually.

As set out in "Policy and Procedures for Privacy and Security Auditing", CorHealth agents who are the subjects of privacy and security audits will be notified in writing at least one day in advance of the scheduled audit by the Privacy Officer and of the process of the audit.

For each type of privacy or security audit, the "Policy and Procedures for Privacy and Security Auditing" outlines the process to be followed in conducting the audit. The Privacy Officer is responsible for completing, providing, and/or executing the documentation. The documentation referred to in the "Policy and Procedures for Privacy and Security Auditing" is a template that includes the following information at a minimum:

- Type of Audit
- Date Completed
- Person responsible for completing Audit
- Recommendations arising from Audit
- Person responsible for addressing each recommendation
- Date each recommendation was addressed or expected to be addressed
- Manner that each recommendation was or is expected to be addressed

The Privacy Officer and the Director of IT have authority to manage the privacy and security program as outlined in the "Policy and Procedures for Privacy and Security Auditing". The Privacy

Officer is responsible for addressing recommendations arising from privacy and security audits, including the establishment of timelines to address the recommendations and the monitoring of implementation of the recommendations. The Privacy Officer shall also identify the nature of documentation that will be completed, provided, and/or executed at the conclusion of each privacy audit.

Any deficiencies in CorHealth's privacy and security program that are identified as a result of a privacy or security audit are communicated in writing to the Chief Executive Officer of CorHealth by the Privacy Officer as quickly as is reasonably possible. The results of audits are communicated to CorHealth agents, by either the CEO or the Privacy Officer, within about one week of the conclusion of the privacy or security audit.

A log of all privacy and security audits is maintained by the Privacy Officer under the "Policy and Procedures for Privacy and Security Auditing" policy. This log is retained on the main CorHealth company drive. The Privacy Officer and the Director of IT ensure that any recommendations are implemented within one week of the final review of privacy and security audits, unless the recommendation relates to CorHealth's operating environment. Recommendations for changes in CorHealth's operating environment will be implemented in accordance with a timeline set out by the Privacy Officer upon reception of the recommendation.

Should a CorHealth agent suspect a breach of "Policy and Procedures for Privacy and Security Auditing" or its procedures (breach being defined in the CorHealth policy, "Policy and Procedures for Privacy and Information Security Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Policy and Procedures for Privacy and Information Security Breach Management") to report their suspicions to the Privacy Officer as soon as possible. Failure to report a breach or suspected breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.16 Log of Security Audits

The "Policy and Procedures for Privacy and Security Auditing" sets out that CorHealth will maintain a log of completed security audits. The template for recording audits collects the following information:

- Type of Security Log
- Date Security Audit Completed
- Person responsible for completing Audit
- Recommendations arising from Audit
- Person responsible for addressing each recommendation
- Date each recommendation was addressed or expected to be addressed
- Manner that each recommendation was or is expected to be addressed

CorHealth will retain all forms, even those completed without producing a recommendation. Once completed, the forms will be stored in a locked filing cabinet maintained by CorHealth's Privacy Officer. Recommendations made by security audits will be recorded in greater detail in CorHealth's consolidated log of recommendations.

4.17 Policy and Procedures for Information Security Breach Management

In managing information security breaches, CorHealth follows the same policy ("Information Security and Privacy Breach Management") that governs its management of privacy breaches.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

4.18 Log of Information Security Breaches

CorHealth maintains a log of information security breaches. The Privacy Officer is responsible for maintaining the log information security breaches. The following information is recorded using a template developed by the Privacy Officer:

- The date of the information security breach
- The date that the information security breach was identified or suspected, and reported
- Whether the information security breach was internal or external
- The nature of the personal health information, if any, that was the subject of the information security breach and the nature and extent of the breach
- The date that the information security breach was contained and the nature of the containment measures
- The date that the health information custodian or other organization that disclosed the personal health information, if any, to the prescribed person was notified
- The date that the investigation of the information security breach was completed
- The agent(s) responsible for conducting the investigation
- The recommendation arising from the investigation
- The agent(s) responsible for addressing each recommendation
- The date each recommendation was or is expected to be addressed
- The manner in which each recommendation was or is expected to be addressed

5 Human Resources Documentation (PART 3)

5.1 Policy and Procedures for Privacy Training and Awareness

CorHealth has developed and implemented the policy, "Privacy and Security Training" that requires CorHealth agents to complete initial and ongoing privacy and security training and identifies the procedures to be followed for privacy training. CorHealth conducts its privacy and security training through an online module that was originally prepared by a professional privacy consultant. CorHealth requires all staff to complete privacy training both upon commencement of employment and annually thereafter. Agents must complete the privacy and security training program prior to being given access to personal health information. The privacy and security training is updated as required with regard to any recommendations made in privacy impact assessments, privacy and security audits, the investigation of privacy and security breaches and privacy and security complaints, as well as IPC guidance, updated legislation or regulations, or privacy and security best practices.

CorHealth requires all staff to take the online privacy and security training to understand how to protect personal health information and to learn about privacy and security in general. CorHealth's privacy training program provides, at minimum, a description of the duties and responsibilities that arise as a result of CorHealth's status under PHIPA. It also includes training on the limitations placed on access and use of personal health information by agents through CorHealth policy.

While not all CorHealth employees have access to personal health information, all CorHealth staff members are required to complete initial and ongoing privacy training regardless of their level of access to personal health information. Similarly, all other agents including Regional Cardiac Care Coordinators and Data Clerks at hospitals, Interface Technologies staff, and our hosting agent, Cancer Care Ontario (prior to July 2017), are required to take initial and ongoing privacy training based on their role and usage of personal health information. This ensures that every agent has the highest level of training. A log is maintained of all agents of CorHealth who have completed initial and ongoing privacy training.

The "Privacy and Security Training" policy sets out that the Privacy Officer is responsible for ensuring that the initial and ongoing privacy and security training is prepared in accordance with any amendments that may be made to the content of the training programs. Additionally, the Privacy Officer is responsible for ensuring that the initial and ongoing privacy and security training programs are delivered as prepared.

The privacy and security initial and ongoing privacy and security training includes the description of CorHealth under PHIPA and its Regulation, a description of the nature of personal health information collected and from whom and why this information is typically collected, what limitations exist on access to personal health information, a description of the procedure that must be followed in the event that an agent is requested to disclose personal health information, an overview of the privacy and security policies, procedures, and practices implemented by CorHealth and the obligations arising from these policies, procedures, and practices, and the consequences of breach of the privacy and security policies, procedures, and practices implemented. Other components include an explanation of the privacy program including the key activities of the program and confirming that the Privacy Officer of CorHealth manages the privacy program.

The "Privacy and Security Training" policy requires the initial and ongoing training program to include advising agents of administrative, physical, and technical safeguards implemented by

CorHealth to protect personal health information against theft, loss, and unauthorized use or disclosure, copying, modification, or disposal. Furthermore, the agents learn the duties and responsibilities in implementing the administrative, technical, and physical safeguards that are put in place by CorHealth. The "Privacy and Security Training" policy requires the initial and ongoing training to include a discussion of the nature and purpose of the confidentiality agreements that agents must execute, the key provisions of the confidentiality agreements, and finally, an explanation of the "Information Security and Privacy Breach Management" policy and the duties and responsibilities imposed on agents in identifying, reporting, containing, and participating in the investigation and remediation of privacy breaches.

The privacy and security training program, consisting of initial and ongoing training, is mandatory. All new employees are required to sign a confidentiality agreement, as well as complete the online privacy and security training program. Employees are then required to complete the ongoing privacy and security training and sign the confidentiality agreement annually. The results of this program, both initial training and ongoing training, are automatically tracked online. As a further component of the privacy and security onboarding program, the confidentiality agreement compels the agent to protect personal health information. All contracts, initial and ongoing, are kept in a safe, locked location and are accessible only by the Privacy Officer and/or delegate. Additionally, all confidentiality agreements are signed, scanned, and retained on the CorHealth company drive accessible as required by the Privacy Officer. The online privacy and security training results, for both initial and ongoing training, include name, date taken and score, and are available to the Privacy Officer at any time.

The policy and procedures also identify the other mechanisms implemented by CorHealth to foster a culture of privacy and raise awareness of the privacy and security program and the privacy and security policies, procedures, and practices implemented. The policy and procedures also discuss the frequency that CorHealth's Privacy Officer communicates with agents in relation to privacy and security, the method, and nature of the communication.

The CorHealth Privacy Officer discusses CorHealth's privacy and security program, and any issues that have arisen, at staff, team, and other ad-hoc meetings. The Privacy Officer makes clear that any questions related to privacy and/or security should go directly to the Privacy Officer. Informal emails are also sent to CorHealth employees to remind them to be aware of any privacy and/or security issues and to always ask the Privacy Officer if they are not sure how to handle a privacy or security issue. The Privacy Officer conducts privacy and security audits annually in accordance with the policy, "Policy and Procedures for Privacy and Security Auditing". Additionally, CorHealth's CEO provides updates to staff, the Board of Directors, and other interested stakeholders at each Annual General Meeting, or more frequently, as required.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in

disciplinary action.

5.2 Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training

As set out in the "Privacy and Security Training" policy, CorHealth maintains a log of attendance for privacy training, both initial and ongoing training, via its online privacy training system. The system identifies the agent, the date and time they completed the privacy training, and the score they obtained. CorHealth employees take this online privacy training annually and the results are obtainable by the Privacy Officer whenever they are required.

5.3 Policy and Procedures for Security Training and Awareness

Refer to Section 5.1 Policy and Procedures for Privacy Training and Awareness. CorHealth's Privacy and Security Training and Awareness Policy and Procedures are combined.

5.4 Log of Attendance at Initial Security Orientation and Ongoing Security Training

Refer to Section 5.2 Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training. The Log of Attendance for the initial security orientation and ongoing security training is combined with that used for the privacy orientation and ongoing privacy training.

5.5 Policy and Procedures for the Execution of Confidentiality Agreements by Agents

CorHealth has developed and implemented a policy ("Execution of Confidentiality and Non-Disclosure Agreements") governing the execution of confidentiality agreements with agents. This policy sets out that all CorHealth agents are required to execute confidentiality agreements with CorHealth at the outset of their employment or other contractual relationship, and annually thereafter, at the end of each April. The "Execution of Confidentiality and Non-Disclosure Agreements" policy sets out that the confidentiality agreements used by CorHealth must include all the conditions set out in the template provided by the IPC.

The "Execution of Confidentiality and Non-Disclosure Agreements" policy sets out that CorHealth's Privacy Officer is responsible for ensuring that the confidentiality agreements have been executed with all CorHealth agents at the outset of their employment or other contractual relationship and annually thereafter. To ensure this, the Privacy Officer is required to provide agents with copies of the confidentiality agreement to sign at the outset of their employment or other contractual relationship and on an annual basis thereafter.

The Privacy Officer must provide notification regarding the necessity of their executing confidentiality agreements with CorHealth in written format to new CorHealth agents within two days of the outset of their employment or other contractual relationship. As CorHealth is a small organization, and because in practice notification of new staff is provided by the CEO in advance of their first day, it is not reasonably conceivable that an agent could commence employment or other contractual relationship with CorHealth without the knowledge of the Privacy Officer. As such the "Execution of Confidentiality and Non-Disclosure Agreements" policy does not require notification to be provided to the Privacy Officer at the outset of an agent's employment or other contractual relationship. This practice may be reviewed as CorHealth grows.

Additionally, the Privacy Officer must provide written notification regarding the confidentiality agreements to all CorHealth agents annually at the end of April.

The "Execution of Confidentiality and Non-Disclosure Agreements" policy sets out that the Privacy Officer is responsible for developing and maintaining a log of executed confidentiality agreements with agents. This log is required by the policy to be kept on the shared company drive in a partition accessible only to the Privacy Officer. Agents' execution of confidentiality agreements is required by the policy to be tracked in this log. If CorHealth agents fail to execute confidentiality agreements with repeated notification, they will be denied permission to access personal health information. If the agent fails to execute the confidentiality agreements within one week, the agent will be subject to disciplinary action as set out in the "Policy and Procedures for Discipline and Corrective Action".

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually (in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

5.6 Template Confidentiality Agreements with Agents

As required by the "Execution of Confidentiality and Non-Disclosure Agreements" policy, CorHealth has developed a template confidentiality agreement that all agents are required to execute at the outset of their employment and annually thereafter at the end of each April. At minimum, this confidentiality agreement must set out the following:

- General Provisions:
    - A description of CorHealth's status under PHIPA and its Regulation
    - An explanation of CorHealth's duties under PHIPA and its Regulation
    - A statement setting out that individuals who sign the confidentiality agreements are agents of CorHealth in respect of personal health information
    - An outline of the responsibilities of CorHealth agents in respect to the protection of personal health information
    - A stipulation that agents will comply with the provisions of PHIPA and its Regulation relating to CorHealth and with the terms of the confidentiality agreements as may be amended from time to time
    - A statement setting out that the agent acknowledges that they have read, understood, and agree to comply with the privacy and security policies, procedures and practices implemented by CorHealth as they may be amended following the execution of the confidentiality agreements
    - The definition of personal health information found in PHIPA and its Regulation

- Obligations with Respect to Collection, Use and Disclosure of Personal Health Information:
    - A list of the purposes for which CorHealth agents are permitted to collect, use, and disclose personal health information and any limitations, conditions, or restrictions imposed thereon
    - The authority under PHIPA and its Regulation of each of the identified permitted collections, uses, and disclosures of personal health information
    - A stipulation that agents are prohibited from collecting or using personal health information except as permitted by the confidentiality agreements
    - A stipulation that agents are prohibited from disclosing personal health information except as permitted by the confidentiality agreements or as required by law
    - A prohibition on collecting, using, or disclosing personal health information if other information will serve the purpose and from collecting, using, or disclosing more personal health information than is reasonably necessary to meet the purpose
- Termination of the Contractual, Employment, or Other Relationship:
    - A stipulation that all agents must return to CorHealth all CorHealth property, including records of personal health information and all access cards, keys, and identification to the Privacy Officer on or before the date of termination of the employment, contractual or other relationship in accordance with the "Termination of Employment" and "Termination or Cessation of Contractual Relationships" policies
    - A statement setting out the time frame within which CorHealth property must be returned, and the secure manner in which the property must be returned
    - The confidentiality agreement survives termination of an agent's employment or affiliation with CorHealth
- Notification:
    - A stipulation that CorHealth agents must notify the Privacy Officer at the first reasonable opportunity if they identify or suspect a breach, as defined in the "Information Security and Privacy Breach Management" policy
- Consequences of Breach and Monitoring Compliance:
    - A statement setting out the consequences of breach of the agreement as described in the CorHealth policies "Policy and Procedures for Discipline and Corrective Action" and "Information Security and Privacy Breach Management"
    - A statement setting out the scope and nature of CorHealth's auditing program for ensuring compliance with its privacy and security program, including the confidentiality agreements

5.7 Log of Executed Confidentiality Agreements with Agents

The CorHealth policy, "Policies and Procedures for the Execution of Confidentiality and Non-Disclosure Agreements" sets out that CorHealth's Privacy Officer is required to retain all executed confidentiality agreements in a locked drawer, as well as electronically. The Privacy Officer will maintain an electronic log that documents CorHealth agents' execution of confidentiality agreements. The log includes the name of the agent, the date of commencement of employment, contractual or other relationship with CorHealth, and the dates that the confidentiality agreements were executed.

5.8 Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program

CorHealth has developed a job description for the role of the Privacy Officer ("CorHealth Privacy Officer Portfolio"). The "CorHealth Privacy Officer Portfolio" sets out that the Privacy Officer reports directly to the CEO and assumes the day-to-day responsibility for privacy and security at CorHealth. The Privacy Officer is responsible for the development and implementation of a corporate privacy and security program.

The "CorHealth Privacy Officer Portfolio" sets out that the Privacy Officer must ensure that appropriate privacy, security, and confidentiality measures and processes (e.g. consent forms, audit programs) are in place by working with CorHealth management, legal counsel, key departments, and committees. The Privacy Officer is also required to perform periodic information privacy and security audits and related compliance monitoring activities, as set out in the "Policy and Procedures for Privacy and Security Auditing".

The Privacy Officer is responsible for overseeing, directing, and delivering an online corporate privacy and security educational training program for all CorHealth agents. The "CorHealth Privacy Officer Portfolio" sets out that the Privacy Officer must maintain current knowledge of government and industry standards and initiatives to achieve training objectives. In addition, the Privacy Officer is responsible for initiating, facilitating, and promoting activities to foster privacy and security awareness within CorHealth and its stakeholders.

The Privacy Officer must work with all stakeholders that have relationships with CorHealth relating to privacy or security issues. He/she must cooperate with the IPC or any other legal entity in investigations and reviews of CorHealth policies. Additionally, the "CorHealth Privacy Officer Portfolio" states that the Privacy Officer is required to participate in the development, implementation, and ongoing compliance monitoring of all stakeholder and associate agreements to ensure that privacy and security concerns, requirements, and responsibilities are addressed. If stakeholders or other external parties that make policy, inquire about CorHealth privacy and security policy, the Privacy Officer is required to represent CorHealth's interests.

With CorHealth management and operations staff, CorHealth's Privacy Officer is responsible for the establishment of a mechanism to track CorHealth agents' access to personal health information. This will ensure that access to and use of personal health information is compliant with the CorHealth policy ("Limiting Agent Access to and Use of Personal Health Information") and government regulations. The Privacy Officer is also required to ensure that CorHealth maintains a mechanism for the reception, documentation, investigation, tracking, and taking of effective action on all privacy inquiries, complaints, and breaches of personal health information by CorHealth agents. The Privacy Officer must develop the mechanisms employed to determine whether to enter into data sharing arrangements, and monitors any personnel involved in this process.

When the Privacy Officer is not available, he/she must ensure back up coverage with other staff with specific privacy and security responsibilities. The Privacy Officer may be delegated additional responsibilities by the CEO.

CorHealth requires the Privacy Officer to have a superior knowledge of privacy laws, as well as government and industry standard practices. The Privacy Officer must also have skills and experience in project management, organization, and presentation. In addition, the Privacy Officer has the following responsibilities and obligations:

- Developing, implementing, reviewing, and amending privacy and security policies, procedures, and practices

- Ensuring compliance with the privacy and security policies, procedures, and practices implemented
- Ensuring transparency of the privacy and security policies, procedures, and practices implemented
- Facilitating compliance with PHIPA and its Regulation
- Ensuring agents are aware of PHIPA and its Regulation, and their duties thereunder
- Ensuring agents are aware of the privacy and security policies, procedures and practices implemented by CorHealth and are appropriately informed of their duties and obligations thereunder
- Directing, delivering, or ensuring the delivery of the initial privacy and security orientation and the ongoing privacy training and fostering a culture of privacy and security awareness
- Conducting, reviewing, and approving privacy impact assessments
- Receiving, documenting, tracking, investigating, remediating, and responding to privacy complaints and inquiries pursuant to the policy, "Privacy Inquiries and Complaints"
- Receiving, documenting, tracking, investigating, and remediating privacy breaches, suspected privacy breaches, information security breaches, and suspected information security breaches pursuant to the "Information Security and Privacy Breach Management" policy
- Conducting privacy and security audits pursuant to the "Policy and Procedures for Privacy and Security Auditing" policy

5.9 Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program

Refer to Section 5.8 Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program as the description has been combined and is one and the same.

5.10 Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship

CorHealth's policies, "Termination of Employment" and "Termination and Cessation of Contractual Relationships" set out that agents and other employees planning to exit CorHealth must provide advance notice of resignation. Resignations must be submitted in writing to the CEO. CorHealth currently utilizes its Master Services Agreement with its contractors to outline termination protocol.

The "Termination or Cessation of Contractual Relationships" policy sets out the following circumstances under a contract may be terminated and procedures for the termination of a contract either by CorHealth or the other party:

- The failure of the other party to carry out a material duty or obligation under the agreement, which default is not cured to the satisfaction of the non-defaulting party within ten (10) days of providing notice in writing to the defaulting party detailing the nature of the default
- The bankruptcy or insolvency of the other party or if the other party seeks the protection of any law for bankrupt or insolvent debtors
- The provision to the other party of thirty (30) days' written notice of termination [CorHealth determines on a case-by-case basis whether the other party should have the right to terminate on 30 days' notice or whether the right is CorHealth's alone]
- In response to a force majeure under certain circumstances
- On the mutual agreement of the parties to terminate the agreement or a Service Schedule

Regarding termination of employment contracts, a protocol is in place as set out in the policy, "Termination of Employment". As part of the policy, "Termination of Employment", CorHealth managers and directors must immediately advise the CEO and Specialist, Human Resources of all resignations in their department as soon as this information is available. The time stamp for the resignation is the date that the resignation is submitted in writing to the CEO. The determination to discharge an employee from employment at CorHealth must be made in collaboration with the CEO, Specialist, Human Resources, and Director of Financial Services. CorHealth must ensure that all relevant policies and legislative requirements are adhered to and the discharge is completed in a humane and caring manner. The CEO and/or Specialist, Human Resources must ensure that communications to staff are appropriate to the situation.

The Specialist, Human Resources, as delegated by the Privacy Officer, will make arrangements to obtain all CorHealth property on last day of work as is set out in the policy.

When an employee terminates his/her relationship with CorHealth, a notice period of 2-6 weeks is required, with the length of that period depending on the nature of the employee's work.

All CorHealth property including, desk keys, door keys, building pass card, parking cards, cell phones, and application keys are returned to the Specialist, Human Resources (all passwords are required to be immediately deactivated by the Director of IT and/or their delegate).

The Privacy Officer has a check list with all required items to be returned that is completed when an employee leaves CorHealth. This information is maintained by the Specialist, Human Resources. Typically, there is no risk if CorHealth property is not securely returned because all property pass cards, CorHealth email, and phone accounts are disabled. Employees who are leaving CorHealth also have an opportunity to submit CorHealth property to CorHealth via courier if they are unable to physically come to CorHealth's offices.

All access to the premises, where personal health information is retained and to the information technology operational environment, are immediately terminated upon the cessation of employment, which is the last day of employment (these duties are conducted by the Specialist, Human Resources and the Director of IT as delegated by the Privacy Officer of CorHealth).

All access and parking cards to the main building, housing the location of CorHealth, are collected by the Privacy Officer and, in partnership with the building personnel, the Specialist, Human Resources and/or delegate deactivates these cards on the day of termination.

When CorHealth terminates an employment contract, the CEO, Specialist, Human Resources, or the employee's manager must provide the employee a written notice which includes the date of termination and/or cessation. On the day of termination, the same rules of the employee termination policy apply as listed above.

The Privacy Officer will be responsible for the auditing for compliance with CorHealth's policies "Termination of Employment" and "Termination and Cessation of Contractual Relationships" annually.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report their suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

5.11 Policy and Procedures for Discipline and Corrective Action

The "Policy and Procedures for Discipline and Corrective Action" sets out the procedures for discipline and corrective action in respect of personal health information. Discipline and corrective action against an agent may be taken if that agent is found to be responsible for damage to CorHealth's operations or reputation.

If an agent breaches or is suspected to have breached a CorHealth privacy or security policy, the Privacy Officer is responsible for investigating the incident. If the Privacy Officer is under suspicion, the Director of IT conducts the investigation in conjunction with the Specialist, Human Resources. The Privacy Officer's investigation may include interviews with other agents, audits of technology to which the agent under investigation had access, and audits of logs relating to the policy that may have been breached. The Privacy Officer shall record the process and findings of the investigation using the "Form for the Investigation of Agents Suspected of Responsibility for a Privacy and/or Security Breach". The results of the investigation will be communicated to the CEO in a timely manner. In determining what discipline or corrective measures may be taken, the Privacy Officer will take into consideration:

- Whether or not the agent intended to breach a CorHealth policy and/or expose personal health information
- Whether a privacy breach occurred, or if personal health information was exposed to unacceptable risk but not compromised
- The extent of the breach, for example whether the agent has compromised more than one system
- Disruption of CorHealth operations
- Damage to CorHealth's reputation

Depending on the extent and severity of the infraction, the agent may be subject to one of the following corrective actions (in increasing order of seriousness):

- Verbal warning
- Restriction or revocation of access rights to personal health information
- Suspension with pay
- Termination of employment

The Privacy Officer, in consultation with the CEO, is responsible for determining the seriousness of the corrective action. This determination is made on a case-by-case basis. Any agent found to have intentionally disclosed personal health information will be summarily fired. The Privacy Officer will complete the "Form for Discipline and Corrective Action" and submit it to the CEO. The Privacy Officer will maintain a repository of these forms in hard copy and electronic format in a secure location on the CorHealth company electronic drive.

6 Organizational and Other Documentation (PART 4)

6.1 Privacy Governance and Accountability Framework

The Chief Executive Officer of CorHealth is accountable for the protection of personal health information in the custody or under the control of CorHealth but has delegated day-to-day responsibility to the Privacy Officer. The Privacy Officer is tasked with ensuring that personal health information is collected, used, and disclosed in accordance with CorHealth's privacy policies and procedures, and in compliance with PHIPA and its regulation. A more detailed description of the Privacy Officer's duties is located in Section 5 Human Resources Documentation (PART 3) of this report. The Privacy Officer is responsible for communicating the privacy and security governance and accountability framework document to agents of the prescribed person. The Privacy Officer will ensure that each new CorHealth employee receives the privacy and security governance and accountability framework document as a hard copy and thereafter it will be available on the CorHealth intranet web page that is accessible to each CorHealth employee. The Privacy Officer will make any changes, as required, and repost on the CorHealth intranet web page. All new third-party service providers will receive a hard copy of the privacy and security governance and accountability framework upon execution of a services agreement with CorHealth and they will receive the privacy and security governance and accountability framework document directly via email or hardcopy from the Privacy Officer, if there are any changes. Requests for de-identified and/or aggregate data are reviewed by the Research and Publications Committee, a body composed of medical researchers and hospital administrators who ensure that agreements are in place requiring researchers to use data received from CorHealth in a secure and ethical manner.

The Board of Directors provide high-level oversight of CorHealth's privacy program. The Board of Directors must be made aware, at the first reasonable opportunity, of any major changes to or issues with the CorHealth privacy program, such as, but not limited to privacy breaches, changes to CorHealth's privacy status, or any major changes to PHIPA that affect CorHealth. The Board of Directors are provided annual updates on the state of the CorHealth privacy program at the CorHealth Annual General Meeting (AGM). At the operations level, the privacy and security governance and accountability framework is headed by the CEO who has delegated duties to the Privacy Officer. Unless managed by the CEO, the Privacy Officer is responsible for all communications relating to privacy and security. The main agents likely to be affected are the participating CorHealth hospitals and our supplier of network administration support.

The Annual General Meeting report provided to the Board of Directors, which are developed by the Privacy Officer, describe the initiatives undertaken by the privacy and security program, including privacy and security training and the development and implementation of privacy and security policies, procedures and practices. The report also provides the results of any audits or assessments of CorHealth's privacy and security policies, as well as any recommendations made and the status of the implementation of those recommendations. The Board of Directors also receives a report of any privacy complaints or privacy or security breaches, including the results of any investigations where applicable.

6.2 Privacy and Security Governance and Accountability Framework

Refer to Section 6.1 Privacy Governance and Accountability Framework as there is a single Privacy and Security Governance and Accountability Framework.

6.3 Terms of Reference for Committees with Roles with Respect to the Privacy and/or Security Program

As the privacy and security program is led by the Privacy Officer and there are no committees that have a role in respect of the privacy and/or security program, there are no committee terms of reference. The Privacy Officer will assign an internal staff member from Information Technology to assist with the audit functions of CorHealth, as required.

6.4 Corporate Risk Management Framework

CorHealth has implemented the Healthcare Insurance Reciprocal of Canada (HIROC) Integrated Risk Management (IRM) program, which is a comprehensive and integrated corporate risk management framework, to identify, assess, mitigate, and monitor risks, including privacy and security risks.

The IRM program utilizes the HIROC risk management framework, which allows the organization to standardize the assessment, categorization, and ranking of risks. The IRM program outlines the organizational policies and procedures for identifying, assessing, mitigating, and monitoring corporate risks, including the use of a corporate risk register, to ensure any risk which may negatively affect CorHealth's ability to maintain IT privacy and security are mitigated, and privacy and security are maintained.

The IRM program identifies the agents responsible and the process that must be followed in identifying risks that may negatively affect the ability of CorHealth, as the prescribed person, to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. This includes a discussion of the other agents or organizations that must be consulted in identifying risks, the documentation that must be completed, the agents responsible for completing the documentation, to whom the documentation must be provided, and the required content of the documentation.

The IRM program also addresses the agents responsible, the process that must be followed, and the criteria that must be considered in ranking the risks, assessing the likelihood of the risks occurring, and the potential impact if they occur. It also includes a discussion of the agents, other persons, or organizations that must be consulted in assessing and ranking the risks, the documentation that must be completed, provided, and/or executed in assessing and ranking the risks, the documentation that must be completed, provided and/or executed in setting out the rationale for the assessment and ranking of the risks, the agent responsible for completing providing and/or executing the documentation, the agent(s) to whom this documentation must be provided, and the required content of the documentation.

The IRM program also identifies the agents responsible, the process that must be followed, and the criteria that must be considered in identifying strategies to mitigate the actual or potential risks to privacy that were identified and assessed. Furthermore, the IRM program sets out the process for implementing the mitigation strategies and the other agents, other persons, or organizations that must be consulted in identifying and implementing the mitigation strategies.

The IRM program also identifies the individuals responsible for assigning other agents to implement the mitigation strategies, for establishing timelines to implement the mitigation strategies, and for monitoring and ensuring that the mitigation strategies have been implemented. Furthermore, the IRM program sets out the documentation that must be completed in identifying, implementing, monitoring, and ensuring the implementation of the mitigation strategies, as well as the agents responsible for completing the documentation, the agents to whom this documentation must be provided, and the required content of the

documentation.

The IRM program addresses the manner and format in which the results of the corporate risk management process, including the identification and assessment of risks, the strategies to mitigate actual or potential risks to privacy, and the status of the mitigation strategies, are communicated and reported. The IRM program also identifies the agents responsible for communicating and reporting the results of the corporate risk management process, the nature and format of the communication, and the individuals to whom the results will be communicated and reported. The IRM program states that the results of the corporate risk management process will be communicated to the CEO for approval and endorsement.

The IRM program requires that a corporate risk register be maintained and reviewed on an ongoing basis in order to ensure that all the risks that may negatively affect CorHealth's ability to protect the personal health information in its custody are mitigated. Furthermore, the IRM program sets out the frequency with which the corporate risk register must be reviewed, the agent responsible for review, and the process that must be followed in reviewing and amending the corporate risk register. The IRM program requires that a corporate risk report, from the Corporate Risk Register, is reviewed by CorHealth's Business Services and Audit Committee, and then presented to the Board of Directors for final approval, on a biannual basis.

Finally, the IRM program sets out the manner in which the corporate risk management framework is integrated into CorHealth's policies, procedures, and practices, as well as the projects undertaken by CorHealth and the agent(s) responsible for such integration.

6.5 Corporate Risk Register

CorHealth implemented the Corporate Risk Register in September 2017. Through the IRM program processes, outlined above, CorHealth maintains a Corporate Risk Register (online HIROC tool) that is reviewed and updated regularly.

6.6 Policy and Procedures for Maintaining a Consolidated Log of Recommendations

It is the CorHealth's policy ("Maintaining a Consolidated Log of Recommendations") to maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, privacy audits, security audits, and the investigation of privacy breaches, privacy complaints, and security breaches. This document has a consolidated and centralized log which includes recommendations made by the IPC that must be addressed by CorHealth prior to the next review of its practices and procedures.

The log is reviewed on an ongoing basis by the Privacy Officer to ensure recommendations are addressed in a timely manner or when a new recommendation is added to the log. The centralized log is reviewed at least annually, as set out in the "Policy and Procedures for Privacy and Security Auditing," and is updated each time a recommendation has been addressed in response to a PIA, audit, breach, complaint, investigation, or review by the IPC is completed.

All CorHealth agents must comply with this policy. Compliance with this policy will be audited by CorHealth's Privacy Officer annually, in compliance with the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing". Should the Privacy Officer determine that an agent of CorHealth has not complied with this policy, disciplinary measures will be taken. The Privacy Officer, in consultation with the agent's manager and the CEO, as necessary, is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may

recommend that an agent's relationship with CorHealth be terminated. If the instance of non-compliance constitutes a violation of the agent's confidentiality agreement, legal action against the agent may be pursued as per that agreement.

Should a CorHealth agent suspect a breach of this policy or its procedures (breach being defined in the CorHealth policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in the CorHealth policy, "Information Security and Privacy Breach Management") to report such suspicions to the Privacy Officer as soon as possible. Failure to report a breach constitutes non-compliance with the CorHealth policy and may result in disciplinary action.

6.7 Consolidated Log of Recommendations

CorHealth has developed a policy ("Maintaining a Consolidated Log of Recommendations") requiring that a consolidated log of recommendations arising from privacy impact assessments, privacy and security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches, and reviews by the IPC is maintained. Information included in the log includes the name and date of the document, investigation, audit and/or review from which the recommendations arose, the recommendation made, the date that the recommendations was addressed or by which it is required to be addressed, the manner in which the recommendation was addressed, and the agent responsible for addressing the recommendation. The Privacy Officer reviews each recommendation by date to ensure that they are addressed within a reasonable timeframe.

6.8 Business Continuity and Disaster Recovery

CorHealth has developed and implemented a policy and procedures, the "Business Continuity & Disaster Recovery Plan," which can be deployed in the event of short and long-term business interruptions, or in the event of threats to CorHealth's operating capabilities to ensure the continued availability of CorHealth's information technology environment. The Plan can be put into action in circumstances including natural, human, environmental, and technical interruptions and threats.

The "Business Continuity & Disaster Recovery Plan" provides information including the notification of the interruption or threat, documentation of the interruption or threat, assessment of the severity of the interruption or threat, the procedures for the activation of the Plan, and the recovery of personal health information.

The "Business Continuity & Disaster Recovery Plan" identifies the agents and other organizations that must be notified in the event of short and long-term business interruptions and threats to CorHealth's operating capabilities, as well as the agents responsible for providing this notification. The "Business Continuity & Disaster Recovery Plan" requires that the identified agents provide notice as soon as is reasonably possible in written or electronic format. The "Business Continuity & Disaster Recovery Plan" also sets out the types of notifications that must be separately documented, as well as the other documentation that must be completed, provided, or executed.

In the main document and in an appendix, the "Business Continuity & Disaster Recovery Plan" provides contact information for all agents, service providers, stakeholders, and other persons or organizations that must be notified in the event of business interruptions and threats. The policy, "Policies and Procedures for Privacy and Security Auditing" states that the Privacy Officer or a designate must review the "Business Continuity & Disaster Recovery Plan" annually to

ensure that the contact information remains accurate and up to date.

The "Business Continuity & Disaster Recovery Plan" outlines a Disaster Recovery and Assessment Team, as well as the agents on the team, which is responsible for assessing the severity of the interruption or threat, conducting the initial impact assessment, assessing the impact on technical and physical infrastructure, and preparing a detailed damage assessment. The "Business Continuity & Disaster Recovery Plan" furthermore identifies the process for completing these assessments, the criteria pursuant to which the assessment is made, the other agents that must be consulted in making the assessment, the documentation that must be completed and its content, and the agents to whom the results of the assessment must be communicated.

The "Business Continuity & Disaster Recovery Plan" also identifies the agents responsible for resumption and recovery, the procedures that must be followed in resumption and recovery activities for each particular application or piece of hardware, the prioritization of resumption and recovery activities, the criteria pursuant to which the prioritization is made, and recovery time objectives for critical applications. The "Business Continuity & Disaster Recovery Plan" also identifies the agents that should be consulted with respect to resumption and recovery activities, the documentation that needs to be completed as well as the content of the documentation and the agents responsible for completing it, the agents to whom the documentation must be provided, and the agents to whom the results of these activities must be communicated.

The "Business Continuity & Disaster Recovery Plan" requires that an inventory be developed and maintained of all critical applications and business functions, and of all hardware and software, software licenses, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings for database systems, and network settings for firewalls, routers, domain name servers, email servers, and other network infrastructure. The plan also identifies the agents responsible for developing and maintaining the inventory, the other agents and organizations that must be consulted in developing the inventory, and the criteria upon which the determination of critical applications and business functions must be made.

The "Business Continuity & Disaster Recovery Plan" sets out the procedures by which decisions are made and actions are taken during business interruptions and threats to CorHealth's operating capabilities, and that such decisions and actions are documented and communicated, as required. This includes a discussion of the agents who are responsible for documentation and communication as well as the agents to whom the communications will be made.

The "Business Continuity & Disaster Recovery Plan" also addresses the testing, maintenance, and assessment of the plan. The "Business Continuity & Disaster Recovery Plan" sets out the frequency with which testing must take place; the agent responsible for testing the plan; the agent responsible for maintaining, assessing and amending the plan as a result of the testing; the procedure to be followed for testing, maintaining, assessing, and amending the plan; and the agents responsible for approving the plan and any amendments thereto.

Finally, the "Business Continuity & Disaster Recovery Plan" addresses the procedures that must be followed in communicating in the plan and any amendments thereto to all agents. This includes the format and nature of the plan, as well as the agents responsible for communication.

7 Privacy and Security Indicators (PART 5)

7.1 PART 1 – Privacy Indicators

Privacy Indicators	CorHealth
General Privacy Policies, Procedures and Practices	
The dates that the privacy policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the IPC.	Since November 1, 2016, the privacy policies and procedures were reviewed: • From May 17, 2017 to July 7, 2107, as part of the response to the IPC's first review of CorHealth's 2017 IPC 3-year review report • From August 25, 2018 to May 13, 2019, as part of the initiative to review and revise CorHealth's privacy program • From August 12, 2019 to October 25, 2019, in preparation of the 3-Year IPC review submission
Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	All CorHealth's privacy and security policies were reviewed between May and July 2017, in order to address feedback from the IPC's review of the first draft of CorHealth's 2017 3-year report as part of the triannual review process. Amendments included: • The "Privacy and Security Training" policy was amended to ensure CorHealth staff receive privacy training when hired initially and on an annual basis moving forward. Previously the policy had a requirement for training every two years From August 25, 2018 to May 13, 2019 and August 2, 2019 to October 25, 2019, CorHealth's privacy and security policies were reviewed and the following amendments were made: • All policies were updated to reflect the corporate reorganization and organizational name change from the Cardiac Care Network (CCN) to CorHealth Ontario (CorHealth) and were rebranded to use the CorHealth Ontario branding • Due to the corporate reorganization, all policies were updated, where applicable, to reflect the change to role names

	• The "Policy and Procedures for Privacy and Security Auditing" was amended to change the timeframe for performing audits from each quarter to annual. Additionally, all policies' enforcement was updated to reflect the change • The "Secure Transfer of Personal Health Information" policy was amended to remove references to Cancer Care Ontario as the agent responsible for providing hosting services until July 2017. As of July 2017, CorHealth repatriated the WTIS-CCN. • The "Maintenance and Review of Specialized Assessments and System Control and Audit Logs" policy was amended to remove references to Cancer Care Ontario as the agent responsible for providing hosting services until July 2017. As of July 2017, CorHealth repatriated the WTIS-CCN.
Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	No new privacy policies or procedures were developed and implemented as a result of the 2017 3-Year review.
The date that each amended, and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.	Amended privacy and security policies, which CorHealth bundles together into a single package, were posted on the CorHealth Intranet promptly following each review period that produced amendments. This occurred on: • July 5, 2017 • June 4, 2020 CorHealth's Privacy Officer and/or the CEO discussed privacy and security at staff meetings that took place on: • July 5, 2017 • July 26, 2018 • September 5, 2018 • October 25, 2018 • March 18/19/20 & 25, 2019 • April 11, 2019 • May 1, 2019 • September 5, 2019

	• October 23, 2019
Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	The communication materials available to the public and other stakeholders were amended to reflect the corporate reorganization, organization name change and branding, and PIA recommendation on March 3, 2020.
Collection	
The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.	CorHealth currently maintains two data holdings, a cardiac data holding and a vascular data holding.
The number of statements of purpose developed for data holdings containing personal health information.	CorHealth has developed two statements of purpose: one for its cardiac data holding and one for its vascular data holding.
The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the IPC.	CorHealth's Statements of Purpose are reviewed annually, as part of CorHealth's regular privacy and security auditing. Since November 1, 2016, the statements of purposes were reviewed at least annually, with the most recent review completed in October 2019, in preparation for the 3 Year IPC Report.
Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made.	CorHealth amended the statements of purpose to reflect the organizational name change and branding in October 2019.
Use	
The number of agents granted approval to access and use personal health information for purposes other than research.	Currently, there are a total of 563 CorHealth agents (includes CorHealth staff and participating hospitals) with access to personal health information for purposes other than research, including 34 CorHealth staff members at the CorHealth Provincial Office.
The number of requests received for the use of personal health information for research since the prior review by the IPC.	CorHealth does not use personal health information for research. There were no requests by CorHealth agents to use personal health information for research.

The number of requests for the use of personal health information for research purposes that were granted and that were denied since the prior review by the IPC.	There were no requests by CorHealth agents to use personal health information for research.
Disclosure	
The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the IPC.	There have been zero requests for the disclosure of personal health information for purposes other than research.
The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied since the prior review by the IPC.	CorHealth does not disclose personal health information for any reason to any organization or individual, except to ICES, with which CorHealth has executed a data sharing agreement, and when required by law. No such requests have been granted.
The number of requests received for the disclosure of personal health information for research purposes since the prior review by the IPC.	There have been zero requests for the disclosure of personal health information for research purposes.
The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied since the prior review by the IPC.	CorHealth does not disclose personal health information for any reason to any organization or individual, except to ICES, with which CorHealth has executed a data sharing agreement, and when required by law. No such requests have been granted.
The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the IPC.	CorHealth does not disclose personal health information for any reason to any organization or individual, except to ICES, with which CorHealth has executed a data sharing agreement, and when required by law. No such requests have been granted.
The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes since the prior review by the IPC.	There have been 45 requests for the disclosure of aggregate, de-identified information since November 1, 2016.
The number of acknowledgements or agreements executed by persons to whom	43 of the 45 requests for the disclosure of aggregate, de-identified information since November 1, 2016 were granted, and therefore 43 agreements with

de-identified and/or aggregate information was disclosed for both research and other purposes since the prior review by the IPC.	researchers were executed.
Data Sharing Agreements	
The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the IPC.	CorHealth is not party to any data sharing agreements executed for the collection of personal health information.
The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity since the prior review by the IPC.	CorHealth is a party to one active data sharing agreement (DSA) with the Institute for Clinical Evaluative Sciences (ICES), originally executed in June 2016, and amended in May 2017, September 2017, August 2018, and June 2019.
Agreements with Third Party Service Providers	
The number of agreements executed with third party service providers with access to personal health information since the prior review by the IPC.	CorHealth was party to an agreement with Cancer Care Ontario for hosting services. That agreement was terminated in July 2017 and CorHealth now provides their own hosting. CorHealth also has an agreement with Interface Technologies Inc. for network management and backup (IT) services, an agreement with ReCall for data backup services, and an agreement with Shred-it for paper shredding services, for a total of 3 Third Party Agreements.
Data Linkage	
The number and a list of data linkages approved since the prior review by the IPC.	No data linkages have been approved or implemented since November 1, 2016. Data linkages with ICES are linked using aggregate and/or de-identified health information and not personal health information.
Privacy Impact Assessments	
The number and a list of privacy impact assessments completed since the prior review by the IPC and for each privacy	One privacy impact assessment (PIA) was undertaken since November 1, 2016. The PIA was conducted on the CorHealth Cardiac and Vascular Registry and completed in July 2017. There was one recommendation from the assessment, which was that CorHealth should amend its Patient Brochure, posters, notices,

impact assessment: • The data holding, information system, technology, or program, • The date of completion of the privacy impact assessment, • A brief description of each recommendation, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	online information, and any other form of communication with patients to include information about CorHealth collecting Enterprise Master Patient Index (EMPI) data from the Ministry of Health (MOH). CorHealth updated its patient communications material to include information about collecting EMPI data from the MOH. The revised communication material was made available on CorHealth's website on March 3, 2020.
The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion.	There are no privacy impact assessments in progress.
The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion.	There are no privacy impact assessments that were not undertaken.
The number of determinations made since the prior review by the IPC that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.	There were no determinations made since the prior review by the IPC.
The number and a list of privacy impact assessments reviewed since the prior review by the Information and Privacy	Both the privacy impact assessment completed in 2013 and the PIA described above were reviewed in advance of the 3-Year IPC review. No recommendations were made that would require amendments to the privacy or security policies.

Commissioner and a brief description of any amendments made.	
Privacy Audit Program	
The dates of audits of agents granted approval to access and use personal health information since the prior review by the IPC and for each audit conducted: • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	The log of agents granted approval to access personal health information since November 1, 2016 was reviewed in: • November 2016 • March 2017 • June 2017 • September 2017 • December 2017 • March 2018 • June 2018 • September 2018 • January 2019 • April 2019 • September 2019 These audits were completed as parts of CorHealth's regular privacy and security auditing. The audits did not reveal information that necessitated recommendations.
The number and a list of all other privacy audits completed since the prior review by the IPC and for each audit: • A description of the nature and type of audit conducted, • The date of completion of the audit, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is	Since the beginning of the current IPC review period on November 1, 2016, privacy and security audits were completed in: • November 2016, no recommendations were made • March 2017, no recommendations were made • June 2017, no recommendations were made • September 2017, no recommendations were made • December 2017, no recommendations were made • March 2018, no recommendations were made • June 2018, no recommendations were made • September 2018, no recommendations were made • January 2019, no recommendations were made • April 2019, the following recommendations were made: o An updated privacy training module will be administered to all

proposed to be addressed.	CorHealth agents upon its completion (module was completed and made available to agents September 2019). o The 2017 PIA recommendation that CorHealth should amend its Patient Brochure, posters, notices, online information, and any other form of communication with patients to include information about CorHealth collecting Enterprise Master Patient Index (EMPI) data from the Ministry of Health was added to the consolidated log or recommendations. • September 2019, the following recommendation was made o Two agents who were no longer with CorHealth but were still on the list of agents with the f access to personal health information were removed from the list (addressed October 2019). These audits were all conducted according to the procedures set out in the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing".
Privacy Breaches	
The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity since the prior review by the IPC.	No notifications of privacy breaches have been received since November 1, 2016.
With respect to each privacy breach or suspected privacy breach: • The date that the notification was received, • The extent of the privacy breach or suspected privacy breach, • Whether it was internal or external, • The nature and extent of personal health information at issue, • The date that senior management was notified, • The containment measures	No notifications of privacy breaches have been received since November 1, 2016.

implemented, • The date(s) that the containment measures were implemented, • The date(s) that notification was provided to the health information custodians or any other organizations, • The date that the investigation was commenced, • The date that the investigation was completed, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	
Privacy Complaints	
The number of privacy complaints received since the prior review by the IPC.	There have been no privacy complaints made to CorHealth since November 1, 2016.
Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC and with respect to each privacy complaint investigated: • The date that the privacy complaint was received, • The nature of the privacy complaint, • The date that the investigation was commenced, • The date of the letter to the individual who made the privacy complaint in	There have been no privacy complaints made to CorHealth since November 1, 2016.

relation to the commencement of the investigation, • The date that the investigation was completed, • Brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, • The manner in which each recommendation was addressed or is proposed to be addressed, and • The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.	
Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC and with respect to each privacy complaint not investigated: • The date that the privacy complaint was received, • The nature of the privacy complaint, and • The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.	There have been no privacy complaints made to CorHealth since November 1, 2016.

7.2 PART 2 – Security Indicators

Security Indicators	CorHealth
General Security Policies and Procedures	
The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the IPC.	Since November 1, 2016, the privacy policies and procedures were reviewed: • From May 17, 2017 to July 7, 2107, as part of the response to the IPC's first review of CorHealth's 2017 IPC 3-year review report • From August 25, 2018 to May 13, 2019, as part of the initiative to review and revise CorHealth's privacy program • From August 12, 2019 to October 25, 2019, in preparation of the 3-Year IPC review submission
Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	All CorHealth's privacy and security policies were reviewed between May and July 2017, in order to address feedback from the IPC's review of the first draft of CorHealth's 2017 3-year report, as part of the triannual review process. Amendments included: • The "Privacy and Security Training" policy was amended to ensure CorHealth staff receive privacy training when hired initially and on an annual basis moving forward. Previously the policy had a requirement for training every two years From August 25, 2018 to May 13, 2019 and August 2, 2019 to October 25, 2019, CorHealth's privacy and security policies were reviewed and the following amendments were made: • All policies were updated to reflect the corporate reorganization and organizational name change from the Cardiac Care Network (CCN) to CorHealth Ontario (CorHealth) and were rebranded to use the CorHealth Ontario branding • Due to the corporate reorganization, all policies were updated, where applicable, to reflect the change to role names • The "Policy and Procedures for Privacy and Security Auditing" was amended to change the timeframe for performing audits from each quarter to annual. Additionally, all policies' enforcement was updated to reflect the change

	• The "Secure Transfer of Personal Health Information" policy was amended to remove references to Cancer Care Ontario as the agent responsible for providing hosting services until July 2017. As of July 2017, CorHealth repatriated the WTIS-CCN. • The "Maintenance and Review of Specialized Assessments and System Control and Audit Logs" policy was amended to remove references to Cancer Care Ontario as the agent responsible for providing hosting services until July 2017. As of July 2017, CorHealth repatriated the WTIS-CCN.
Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	No new Security policies or procedures have been developed or implemented since November 1, 2016
The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.	Amended privacy and security policies, which CorHealth bundles together into a single package, were posted on the CorHealth Intranet promptly following each review period that produced amendments. This occurred on: • July 5, 2017 • June 4, 2020 CorHealth's Privacy Officer and/or the CEO discussed privacy and security at staff meetings that took place on: • July 5, 2017 • July 26, 2018 • September 5, 2018 • October 25, 2018 • March 18/19/20 & 25, 2019 • April 11, 2019 • May 1, 2019 • September 5, 2019 • October 23, 2019
Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so,	The communication materials available to the public and other stakeholders were amended to reflect the corporate reorganization, organization name change and branding, and PIA recommendation in March 2020. The materials

a brief description of the amendments.	are available on CorHealth's public website.
Physical Security	
The dates of audits of agents granted approved to access the premises and locations within the premises where records of personal health information are retained since the prior review by the Information and Privacy Commissioner and for each audit: • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	The log of agents granted approval to access personal health information since November 1, 2016 was reviewed in: • November 2016 • March 2017 • June 2017 • September 2017 • December 2017 • March 2018 • June 2018 • September 2018 • January 2019 • April 2019 • October 2019 These audits were completed as parts of CorHealth's regular privacy and security auditing. The audits did not reveal information that necessitated recommendations.
Security Audit Program	
The dates of the review of system control and audit logs since the prior review by the IPC and a general description of the findings, if any, arising from the review of system control and audit logs.	The primary component of CorHealth's "Maintenance and Review of Specialized Assessments and System Control and Audit Logs" policy sets out that software that provides for real-time monitoring of CorHealth data replication automatically alerts CorHealth IT staff if a technical or security issue with the data duplication arises. There is thus no need to review these system control logs.

The number and a list of security audits completed since the prior review by the IPC and for each audit: • A description of the nature and type of audit conducted, • The date of completion of the audit, • A brief description of each recommendation made, • The date that each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is expected to be addressed.	Since the beginning of the current IPC review period on November 1, 2016, privacy and security audits were completed in: • November 2016, no recommendations were made • March 2017, no recommendations were made • June 2017, no recommendations were made • September 2017, no recommendations were made • December 2017, no recommendations were made • March 2018, no recommendations were made • June 2018, no recommendations were made • September 2018, no recommendations were made • January 2019, no recommendations were made • April 2019, the following recommendations were made: o An updated privacy training module will be administered to all CorHealth agents upon its completion (module was completed and made available to agents September 2019). o The 2017 PIA recommendation that CorHealth should amend its Patient Brochure, posters, notices, online information, and any other form of communication with patients to include information about CorHealth collecting Enterprise Master Patient Index (EMPI) data from the Ministry of Health was added to the consolidated log or recommendations. • September 2019, the following recommendation was made: o Two agents who were no longer with CorHealth but were still on the list of agents with access to personal health information were removed from the list (addressed October 2019). A new offboarding process was recently implemented that will help to ensure that an agent's access is disabled on their termination date. These audits were all conducted according to the procedures set out in the CorHealth policy, "Policy and Procedures for Privacy and Security Auditing".
Information Security Breaches	
The number of notifications of information security breaches or suspected information	There have been no information security breaches or suspected information security breaches since November 1, 2016.

security breaches received by the prescribed person or prescribed entity since the prior review by the IPC.	
With respect to each information security breach or suspected information security breach: • The date that the notification was received, • The extent of the information security breach or suspected information security breach, • The nature and extent of personal health information at issue, • The date that senior management was notified, • The containment measures implemented, • The date(s) that the containment measures were implemented, • The date(s) that notification was provided to the health information custodians or any other organizations, • The date that the investigation was commenced, • The date that the investigation was completed, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is	There have been no information security breaches or suspected information security breaches since November 1, 2016.

proposed to be addressed.	

7.3 PART 3 – Human Resources Indicators

Human Resources Indicators	CorHealth
Privacy Training and Awareness	
The number of agents who have received and who have not received initial privacy orientation since the prior review by the IPC.	In total, 563 CorHealth agents, including applicable staff of health information custodians, committee members, and CorHealth staff have completed initial privacy training. Zero agents of CorHealth have not received initial privacy training.
The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation.	All CorHealth agents have received initial privacy orientation.
The number of agents who have attended and who have not attended ongoing privacy training each year since the prior review by the IPC.	Since the prior review by the IPC, CorHealth's privacy and security policies were updated to require ongoing training on an annual basis. Since 2018, all CorHealth agents completed annual privacy and security training.
The dates and number of communications to agents by the prescribed person or prescribed entity in relation to privacy since the prior review by the IPC and a brief description of each communication.	Amended privacy and security policies, which CorHealth bundles together into a single package, were posted on the CorHealth Intranet promptly following each review period that produced amendments. This occurred on: • July 5, 2017 • June 4, 2020 CorHealth's Privacy Officer and/or the CEO discussed privacy and security at staff meetings that took place on: • July 5, 2017 • July 26, 2018 • September 5, 2018 • October 25, 2018 • March 18/19/20 & 25, 2019

	• April 11, 2019 • May 1, 2019 • September 5, 2019 • October 23, 2019
Security Training and Awareness	
The number of agents who have received and who have not received initial security orientation since the prior review by the IPC.	In total, 563 CorHealth agents, including applicable staff of health information custodians, committee members, and CorHealth staff have completed initial security training. Zero agents of CorHealth have not received initial security training.
The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation.	All CorHealth agents have attended initial security training.
The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the IPC.	Since the prior review by the IPC, CorHealth's privacy and security policies were updated to require ongoing training on an annual basis. Since 2018, all CorHealth agents completed annual privacy and security training.
The dates and number of communications to agents by the prescribed person or prescribed entity to agents in relation to information security since the prior review by the IPC.	Amended privacy and security policies, which CorHealth bundles together into a single package, were posted on the CorHealth Intranet promptly following each review period that produced amendments. This occurred on: • July 5, 2017 • June 4, 2020 CorHealth's Privacy Officer and/or the CEO discussed privacy and security at staff meetings that took place on: • July 5, 2017 • July 26, 2018 • September 5, 2018 • October 25, 2018 • March 18/19/20 & 25, 2019 • April 11, 2019 • May 1, 2019

	• September 5, 2019 • October 23, 2019
Confidentiality Agreements	
The number of agents who have executed and who have not executed confidentiality agreements each year since the prior review by the IPC.	In total, 117 agents have executed confidentiality agreements (called Non-Disclosure Agreements throughout this report) since November 1, 2016. This includes 60 agents who no longer have relationships with CorHealth. • In 2017, 52 confidentiality agreements were executed; 2 contract employees did not execute confidentiality agreements • In 2018, 63 confidentiality agreements were executed; 8 contract employees did not execute confidentiality agreements • 2019, 54 confidentiality agreements were executed; 0 employees did not execute confidentiality agreements; 3 employees are currently on leave and will sign upon their return For 2019, a new process was implemented to ensure all agents executed confidentiality agreements annually.
The date of commencement of the employment, contractual or other relationship for agents that have yet to execute the confidentiality agreement and the date by which the confidentiality agreement must be executed.	All CorHealth agents have signed confidentiality agreements with CorHealth.
Termination or Cessation	
The number of notifications received from agents since the prior review by the IPC related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.	Since November 1, 2016: • 16 contract employees had their contracts end • 17 employees resigned • 2 employees retired • 25 employees were terminated

7.4 PART 4 – Organizational Indicators

Organizational Indicators	CorHealth
Risk Management	
The dates that the corporate risk register was reviewed by the prescribed person or prescribed entity since the prior review by the IPC.	CorHealth implemented the corporate risk register since the last review by the IPC. The risk register was reviewed by CorHealth in April 2019 and most recently reviewed this month, October 2019.
Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.	No amendments were made to the corporate risk register as a result of the review.
Business Continuity and Disaster Recover	
The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC.	CorHealth revised the Business Continuity & Disaster Recovery Plan Policy and Procedure in the Spring of 2020 and subsequently successfully tested the policy and procedure on July 17, 2020.
Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.	No amendments have been made to the Business Continuity & Disaster Recovery Plan Policy as a result of the testing. However, the following amendments have been made to the Business Continuity & Disaster Recovery Plan Procedure as a result of the testing: • Addition of hyperlinks to commonly used communication templates • Updated CorHealth call tree • Updated time estimates for process steps • Addition of step to identify delegation of process tasks