CARDIAC CARE NETWORK

# 2017 REPORT OF CARDIAC CARE NETWORK

# TO

# THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

**August 18, 2017**

CARDIAC CARE NETWORK

## Table of Contents

CARDIAC CARE NETWORK

# Introduction

The Cardiac Care Network of Ontario (CCN) serves as a system support to the Ministry of Health and Long-Term Care (MOHLTC), 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 and vascular services in Ontario. CCN'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 and vascular procedures in Ontario, as well as procedures performed on Ontario residents in certain centres outside of Ontario. In addition, CCN 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, CCN helps to plan, coordinate, implement and evaluate cardiovascular care and is responsible for the Ontario Cardiac Registry (CCN Cardiac and Vascular Registry). The CCN Cardiac and Vascular Registry is designed to improve the provision of health care. The information collected in the CCN 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, CCN uses evidence and consensus driven methods to identify best practice and strategies to effectively deliver cardiovascular services, across the continuum of care.

CCN is a prescribed person within the meaning of section 39(1)(c) of *Personal Health Information Protection Act, 2004* (PHIPA) in respect of the CCN Cardiac and Vascular Registry. Health information custodians (as defined below) are allowed to disclose personal health information (as defined below) to CCN 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), CCN reports to the Information and Privacy Commissioner of Ontario (IPC) every three years on CCN's practices and procedures for protecting the privacy of cardiac and vascular patients and maintaining the confidentiality of their personal health information. This report addresses CCN's privacy and security program, including the improvements achieved to the program since November 1, 2013. This report is being submitted to satisfy the requirements in section 13(2)(b) of the Regulation so

that CCN is continued as a prescribed person in respect of the Registry from November 1, 2017 to October 31, 2019.

In this report, the following terms have the following meanings:

- "agent", "collect", "use", "disclose", "health care", "health information custodian", and "personal health information" have the same meaning as in PHIPA;
- "mobile devices" means 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
- "Manual" means the IPC's *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

CARDIAC CARE NETWORK

# PART 1 – Privacy Documentation

The following describes CCN's policies and procedures in relation to its privacy and security program.

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

## 1.1 Privacy Policy

CCN 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 CCN's obligations in relation to personal health information as a prescribed person. The policy is available on the CCN website (www.ccn.on.ca). The following summarizes the provisions of the policy.

**Status under the Act**

CCN is an advisory body to the MOHLTC and a prescribed person within the meaning of Section 39(1)(c) of PHIPA. As a prescribed person, CCN 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. CCN is committed to complying with PHIPA and its Regulation. CCN's privacy and security policies, procedures, and practices are subject to review by the IPC every three years.

**Privacy and Security Accountability Framework**

The accountability framework for ensuring compliance with the *Act* and its regulation and for ensuring compliance with the privacy and security policies, procedures and practices implemented by the CCN is articulated in CCN's Privacy Policy. In particular, the Privacy Policy indicates that the Chief Executive Officer is ultimately accountable for ensuring compliance with the *Act* 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 identify 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 CCN is ultimately accountable for the protection of personal health information in CCN'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 Lead, Data Governance and Reporting.

CCN 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, CCN 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. CCN 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 CCN pursuant to Participation Agreements are responsible for the personal health information that they collect, while CCN is responsible for the personal health information that it receives from hospitals.

**Collection of Personal Health Information**

CCN 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 CCN collects about patients who undergo select adult cardiac and vascular care. CCN 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 CCN that provide direction as to how to make an inquiry to CCN about the Registry and CCN's collection of personal health information. A list of all data holdings containing personal health information is included in the policy.

**Use of Personal Health Information**

CCN 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, CCN commits to not collecting personal health information if other information will serve the purpose.

CCN 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 CCN. CCN requires all of its agents to sign Confidentiality Agreements that identifies their obligations with respect to protecting personal health information and the privacy of the individuals to whom it relates. CCN 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 CCN'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 CCN's use of personal health information is compliant with PHIPA and its Regulation. CCN 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.

CCN 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 CCN 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 CCN'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 CCN. 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 CCN's privacy and security program. This is further detailed in CCN'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 CCN's privacy and security program.

**Disclosure of Personal Health Information**

CCN does not disclose personal health information except to the Institute for Clinical Evaluative Sciences (ICES), with which CCN has executed a data sharing agreement, 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. CCN 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 CCN 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 CCN 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 CCN has a policy to share de-identified and/or aggregate data with 3rd party researchers, in practice CCN 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 CCN to disclose personal health information to ICES and articulates CCN'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.

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

Personal health information collected by CCN 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 CCN 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 CCN 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. CCN 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.

**Implementation of Administrative, Technical, and Physical Safeguards**

CCN's "Protection of Personal Health Information" Policy lists the administrative, physical, and technical safeguards that CCN 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 CCN are required to sign Confidentiality Agreements that set out their obligations to protect personal health information
- CCN executes Participation Agreements with hospitals that outline both parties' privacy obligations
- CCN is located in a secure location with external video monitoring and progressive grades of physical security
- CCN uses firewalls, network encryption, and intrusion detection systems to maintain the integrity of its networks

**Inquiries, Concerns, or Complaints Related to Information Practices**

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

**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 CCN. 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 also available on the CCN website. Under the "Protection of Personal Health Information" policy, information about the Registry must be publicly available on the CCN website.

## 1.2 Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices

**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 CCN. The purpose of the review is to determine whether amendments or new privacy policies, procedures and practices are required. CCN'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 CCN'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 that CCN policy reflects advancements in technology and in industry practices, and also 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 CCN's privacy policies, procedures, and practices conducted since November 1, 2013 is available in Part 5 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 CCN's agents. New and amended policies will be communicated to CCN'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 CCN agents must comply with the "Annual Review of Privacy and Security Policies and Procedures" policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 1.3 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 CCN's website:

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

Brochures and posters discussing CCN's mandate, activities, and mission to protect personal health information are located in a visible location at all CCN participating hospitals and at the CCN 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 CCN Privacy Officer whose full contact information is listed in the brochure.

The "Transparency of Privacy Policies, Procedures and Practices" policy requires CCN to place brochures in all participating hospitals that explain CCN's mandate and its collection of personal health information. These brochures are required to include, at minimum, an explanation of CCN's legal status as a Section 39(1)(c) prescribed person under PHIPA, CCN's responsibilities stemming from that status, a statement directing any questions and inquiries to CCN's Privacy Officer, a statement directing complaints and inquiries about CCN's compliance with PHIPA and its Regulation to the IPC, contact information for CCN's Privacy Officer and the IPC, some of the administrative, technical, and safeguards used by CCN to protect personal health information, the fact that CCN 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; and
- 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 CCN'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.

## 1.4 Policies and Procedures for the Collection of Personal Health Information

CCN has developed and implemented a number of 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 CCN, 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.

**Identifying Purposes for Collecting Personal Health Information Policy**

The "Identifying Purposes for Collecting Personal Health Information" policy lists the general types of personal health information that CCN 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, telephone number
- Patient telephone numbers

**Limiting Collection of Personal Health Information Policy**

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

**Notice/Consent for Collecting, Using, or Disclosing Personal Health Information Policy**

The "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information" policy provides that CCN 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 CCN'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, CCN requires all its agents to sign Confidentiality Agreements, obliging them to comply with the privacy and security policies and procedures implemented by CCN, 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 CCN. CCN executes Participation Agreements with participating hospitals that clearly set out their obligations to follow CCN 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, CCN is responsible for maintaining the integrity and the security of the personal health information that CCN receives from participating hospitals.

**Information Security and Privacy Breach Management Policy**

CCN'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 CCN at the first reasonable opportunity in the case of a confirmed or suspected breach. CCN's Privacy Officer is responsible for ensuring that all CCN agents comply with this policy.

**Policy and Procedures for Privacy and Security Auditing**

CCN 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 CCN'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 CCN only collects data necessary to fulfil its mandate under PHIPA and its Regulation.

**Review and Approval Process**

CCN only collects personal health information from participating hospitals and does not receive personal health information from any other source. CCN'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 CCN. CCN executes Participation Agreements with participating hospitals that articulate the obligations of both CCN and the hospital in question to protect personal health information.

As set out in the CCN policy "Identifying Purposes for Collecting Personal Health Information", CCN's Privacy Officer is responsible for reviewing the data elements of personal health information that CCN collects to verify that only personal health information necessary for CCN'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 CCN 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.

**Conditions or Restrictions on Approval**

In accordance with the CCN policy "Accountability for Personal Health Information", CCN executes Participation Agreements with participating hospitals prior to its collection of personal health information. These Agreements were drafted by legal consultants to CCN and with input from the IPC following its review of CCN 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 CCN 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"). CCN's Privacy Officer is responsible for ensuring that Participation Agreements have been executed prior to the collection of personal health information by CCN from hospitals.

**Secure Retention**

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

**Secure Transfer**

CCN's policy on the secure transfer of personal health information ("Secure Transfer of Personal Health Information") was developed by CCN's Privacy Officer in April 2010 following recommendations made by the IPC after its review of CCN in 2008. Under the policy, any digital transmissions of personal health information to and from CCN 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.

**Secure Return or Disposal**

Currently, CCN retains personal health information for as long as necessary for long-term statistical analysis. CCN 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 CCN'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 CCN whose employees are bonded. CCN'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 CCN agents must comply with the "Destruction of Personal Health Information" policy. Compliance with this policy will be audited by CCN's Privacy Officer on an annual basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 1.5 List of Data Holdings Containing Personal Health Information

CCN documents information relating to both of its data holdings containing personal health information. The -CCN Cardiac and Vascular Registry stores the 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. This information includes a list of data elements that the two CCN 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, CCN 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 CCN collects helps CCN to compare outcomes for patients who have undergone different variations of the same procedure. To that end, CCN 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 of this data is securely retained within the CCN Cardiac and Vascular Registry following the procedures set out in the CCN policy, "Secure Retention of Personal Health Information".

Information about the patient's condition that is collected by CCN helps CCN to display data to the participating hospitals that can be used to compare outcomes for patients with varying health conditions. To that end, CCN 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 particular procedure, this can include telemetry data, which is collected by ECG or other technology. All of this data is securely retained within the CCN Cardiac and Vascular Registry following the procedures set out in the CCN policy, "Secure Retention of Personal Health Information".

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

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

In accordance with the CCN policy "Statements of Purpose for Data Holdings Containing Personal Health Information", CCN'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 CCN hospitals that collect personal health information that is provided to CCN.

During the course of his/her annual review of CCN'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 CCN's operation as a prescribed person, it will be eliminated in accordance with CCN'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, CCN's privacy and security policies, and relevant IPC guidelines.

CCN's Privacy Officer will consult with CCN's software development and clinical teams to assess whether the statements of purpose are aligned with CCN'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 CCN hospitals as soon as is reasonably possible.

The policy is audited on an annual basis by the Privacy Officer as set out in the CCN policy "Policy and Procedures for Privacy and Security Auditing". The Privacy Officer is also responsible for ensuring compliance with the policy and its procedures.

## 1.7 Statement of Purpose for the CCN Cardiac and Vascular Registry

CCN maintains a statement of purpose for each of its data holdings within the CCN Cardiac and Vascular Registry. These statements of purpose explain the purpose and goals of the data holding, which is critical to CCN'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.

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

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

CCN 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 (when access is required in the performance of an agent's employment, contractual or other relationship with CCN). The Privacy Officer is responsible for determining which CCN agents are granted permission to access or use personal health information. Agents are required to comply with this policy and notify CCN at the first reasonable opportunity if an agent breaches or believes there may have been a breach of this policy or CCN 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 CCN, the Privacy Officer, in consultation with agent's manager, will determine whether or not to grant the agent access to the CCN system that involves personal health information. This system is the main CCN 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 CCN 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 CCN Cardiac and Vascular Registry may only use personal health information in the CCN 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 CCN 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 in order to create comprehensive reports, to help hospitals with entry, and/or to verify and correct patient information. As such, CCN does not segregate agents by level of access. All agents granted access to the CCN 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. CCN 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 CCN 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.

**Review and Approval of Access Process**

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

The decision is made upon the commencement of the agent's relationship with CCN or if an agent's responsibilities change and access to and/or use of becomes necessary. CCN agents do not request access to CCN'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 CCN's data holdings require that access to correct errors in records, conduct statistical analysis, and to assist participating hospitals. As stated in "Limiting Agent Access to and use of Personal Health Information", 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 CCN's data holdings, CCN'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 CCN policies. This documentation is retained by the Privacy Officer and by the Software Application Manager.

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

**Conditions or Restrictions on the Approval of Access**

Currently, there is only one access level for the CCN Cardiac and Vascular Registry, and CCN 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 CCN 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 CCN 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 CCN. Additionally, a breach of the Confidentiality Agreement amounts to a breach of contract, and CCN may seek legal action against the agent(s) responsible.

Currently, all agents with access to CCN's data holdings require that access for the fulfilment of their job description. CCN does not provide any agent temporary access to the CCN data holdings. Should the job description of an agent with access to CCN's data holdings change, and the agent no longer requires access to personal health information, CCN's Privacy Officer is responsible for revoking access as set out in "Limiting Access to and Use of Personal Health Information". Because of CCN'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, CCN has found no need to require its agents to provide specific notification to the Privacy Officer when they no longer require access to CCN's data holdings. This practice may evolve as CCN grows.

The "Limiting Agent Access to and Use of Personal Health Information" policy prohibits agents with access to CCN'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 CCN'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, CCN 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, CCN 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 CCN'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 CCN's data holdings on a quarterly basis to ensure that the day-to-day duties all agents involve the use of the CCN Cardiac

and Vascular Registry. If an agent no longer requires access to a CCN data holding, the Privacy Officer terminates his/her access rights.

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

CCN'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 CCN 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 (i.e. user data including draft documents, non-work related documents, settings, passwords, web history, etc. associated with it are deleted). The purge does not include the agent's email archive or documents that remain relevant to CCN operations, which are retained for an indefinite period. Because of the small number of agents who currently have user accounts (35, including all staff, managers, executives, and temporary contractors), it is reasonable to assume that an agent could not be terminated without the knowledge of the Privacy Officer. As such, CCN does not require agents whose relationships with CCN have been terminated to provide notification to the Privacy Officer of that termination. Agents who resign their position with CCN are required to give prior notice of 2-6 weeks, depending on the nature of the position and their 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 CCN's policy, "Secure Retention of Personal Health Information", CCN 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 CCN's secure server room and their tape backups.

**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 CCN'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 CCN'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.

**Secure Disposal: Destruction of Personal Health Information Policy**

In the event that the Privacy Officer determines that certain personal health information is no longer necessary for CCN's identified purposes, CCN's policy on the destruction of personal health information ("Destruction of Personal Health Information") dictates the methods of disposal. The Policy was developed by CCN'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. CCN'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.

**Tracking Access and Use of Personal Health Information**

The "Limiting Agent Access to and Use of Personal Health Information" policy requires CCN's Software Application Manager, under the supervision of CCN's Privacy Officer, to maintain a log of agents who have been granted access to either of CCN'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 CCN's data holdings was revoked or terminated if applicable, along with a brief explanation of the reasons for the revocation or termination.

**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 CCN policies to agree in writing, at the outset of their relationship with CCN and annually thereafter, that they understand and will uphold the policy. 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 CCN. If the breach constitutes a violation of an agent's Confidentiality Agreement, CCN 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 quarterly audit of agents who have been granted access to CCN'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 System Control and Audit Logs", changes made to the CCN Cardiac and Vascular Registry or the CCN 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".

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

As set out under the heading "Tracking Access and Use of Personal Health Information" (page 27 of this Report), CCN maintains a log of agents who have been granted approval to access and use CCN's data holdings. This log is maintained by the Software Application Manager under the direction of the Privacy Officer.

## 1.10 Policy and Procedures for the Use of Personal Health Information for Research

Currently, CCN does not do any research internally and does not permit third party researchers to have access to personal health information. The use of personal health information for research is expressly prohibited by CCN's "Disclosure of Aggregate and/or De-identified Personal Health Information to Researchers" policy and the "Limiting Use, Disclosure, and Retention of

Personal Health Information" policy. As such, CCN does not require a policy or procedures for the use of personal health information for research.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 1.11 Log of Approved Uses of Personal Health Information for Research

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

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

CCN does not disclose personal health information for any purposes. As such, a written policy on the disclosure of personal health information for purposes other than research is unnecessary.

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

All CCN agents must comply with the "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information" policy. Compliance with this policy is audited by CCN's Privacy Officer on a

quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

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

As mentioned in section 1.10, CCN does not disclose personal health information in any circumstances except under CCN's data sharing agreement with ICES. The rare requests for personal health information for the purposes of research are denied.

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

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

CCN 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.

**Review and Approval Process**

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

**Conditions or Restrictions on the Approval**

CCN 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.

**Secure Transfer**

CCN's policy and procedures for secure transfer of personal information are described in section 1.4.

**Secure Return or Disposal**

CCN 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.

**Documentation Related to Approved Disclosures of Personal Health Information**

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

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

As previously described, under no circumstances does CCN permit the disclosure of personal health information for research purposes. This restriction is set out in CCN's policy entitled "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, CCN may disclose de-identified and/or aggregate data to researchers.

**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 CCN 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 (Ministry of Health and Long-Term Care, etc.). 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. CCN 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 CCN must submit a letter of intent to the Research Publications Committee. A standardized template is made available to researchers on CCN's website. The "Letter of Intent to Conduct a Study for Publication" can be made available to the IPC upon request. CCN 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 CCN. A researcher must prove to the Research and Publications Committee that their research proposal has scientific value and does not compromise any CCN 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 "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.

**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 consequences for the breach of this agreement include legal action. As stated in "Disclosure of Aggregate and/or De-identified Health Information to Researchers", the Research and Publications Committee is responsible for ensuring compliance with these rules.

As set out in Disclosure of Aggregate and/or De-identified Health Information to Researchers," 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. Of the fourteen requests that CCN has received for de-identified and/or aggregate data since November 1, 2013, all have been approved. All fourteen requests were made by researchers affiliated with ICES.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 1.14 Template Research Agreement

Because CCN does not disclose personal health information in any circumstances except under its data sharing agreement with ICES, it does not require a template research agreement.

## 1.15 Log of Research Agreements

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

## 1.16 Policy and Procedures for the Execution of Data Sharing Agreements

CCN has only one data sharing agreement in place. It is with ICES. As CCN has no immediate plans to enter into other such agreements, it has not developed a policy on their execution. Should this change, CCN 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*.

## 1.17 Template Data Sharing Agreement

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

## 1.18 Log of Data Sharing Agreements

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

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

CCN has developed a policy ("Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information") that requires CCN 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 CCN's Privacy Officer and is based on the template provided by the IPC.

CCN'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, CCN's Privacy Officer must ensure that:

- The service provided by the third party in respect of personal health information is necessary to CCN's delivery of its mandate;
- Allowing the third party service provider access to and or use/of personal health information does not violate any CCN 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;
- CCN 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 CCN 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 CCN policy "Destruction of Personal Health Information". CCN's Privacy Officer is responsible

for ensuring that the procedures in these policies are followed by CCN 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, CCN'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 CCN's Chief Executive Officer after an unexpected delay of two days. CCN may seek legal action against the third party at this point.

All CCN 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 CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

CCN's Privacy Officer is responsible for developing and maintaining a log of all agreements in respect of personal health information, which CCN has executed with third party service providers.

CCN 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 CCN so rarely executes agreements with third party service providers, the Privacy Officer has determined that more frequent audits of this policy are unnecessary.

## 1.20 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", CCN 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 CCN 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 CCN and the third party under PHIPA and its regulation
- CCN'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 CCN
- 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 or not the third party is an agent of CCN
- If the third party provider is an agent of CCN, the agreement requires the third party to comply with the provisions of PHIPA and its regulation relating to CCN and to comply CCN'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 CCN, 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**

- CCN'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 CCN's Secure Transfer of Personal Health Information policy
- 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 CCN 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 CCN'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 CCN 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 CCN 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 CCN, the agreement sets out the time frame and manner in which the personal health information must be returned and the CCN agent to whom the personal health information must be returned
- An explanation of how the manner of returning personal health information to CCN has regard to the CCN 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 CCN'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 CCN, 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; the name and signature of the person who performed the secure disposal), and the particular CCN agent to whom the certificate must be provided

**Secure Disposal as a Contracted Service**

- If the third party's primary service to CCN 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 CCN 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 information (e.g. by agreement stating that the agent understands the terms of the agreement with CCN)

**Subcontracting of the Services**

- If the agreement permits the third party to subcontract, the agreement must stipulate that the third party will notify CCN in advance and that the subcontractor will be bound to obligations consistent with the third party's obligations to CCN under the agreement
- A copy of the written agreement between the third party and the subcontractor must be provided to CCN.

**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 CCN 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.

## 1.21 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", CCN'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; and
- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to the personal health information was terminated or 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.

## 1.22 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"", CCN strictly prohibits the linkage of personal health information. To date CCN has not approved any linkage of data. CCN 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 CCN.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty

(articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 1.23 Log of Approved Linkages of Records of Personal Health Information

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

## 1.24 Policy and Procedures with Respect to De-Identification and Aggregation

CCN 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 that the goal of aggregating or de-identifying personal health information is to ensure that 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*.

The "Aggregation and De-identification of Record Level Data" policy sets out that 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 that personal health information may not be used or disclosed for any purpose, except to ICES under the terms of its data sharing agreement with CCN 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 that agents do not reverse the process of aggregation and/or de-identification of personal health information so as 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 CCN 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.

CCN 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, CCN 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 CCN 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 CCN discloses, the risk of re-identifying patients is very low.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN 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 CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 1.25 Privacy Impact Assessment Policy and Procedures

CCN 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 CCN data holdings as long as the updates do not affect the storage or transfer or personal health information or rules regarding access to CCN's data holdings. The Privacy Officer is responsible for reviewing updates to the CCN 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 CCN's information practices.

CCN'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 CCN 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 CCN 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 and eliminate or reduce the privacy risks identified; and
- 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 CCN's privacy and security program may be completed in conjunction with CCN 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 1.26 Log of Privacy Impact Assessments

CCN 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; and
- 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.

## 1.27 Policy and Procedures in Respect of Privacy Audits

CCN 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 CCN conducts privacy audits to assess compliance with the privacy policies, procedures and practices implemented by CCN 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 CCN'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 CCN by the Privacy Officer as quickly as is reasonably possible. The results of audits are communicated to CCN 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 CCN 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 CCN's operating environment. Recommendations for changes in CCN'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 CCN policy, "Policy and Procedures for Privacy and Information Security Breach Management"), the agent has a duty (articulated in CCN 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 CCN policy, and may result in disciplinary action.

## 1.28 Log of Privacy Audits

As set out in the Policy and Procedures for Privacy and Security Auditing, CCN 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 CCN's shared drive.

## 1.29 Policy and Procedures for Privacy Breach and Information Security Breach Management

In response to a recommendation made by the IPC during its review of CCN in 2008, CCN developed and implemented a new policy ("Information Security and Privacy Breach Management") on the identification, reporting, containment, notification, investigation and remediation of privacy and information security breaches. This policy was developed by CCN'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 CCN's privacy policies, procedures or practices
- Contravention of Data Sharing Agreements, Research Agreements, Confidentiality and Non-Disclosure Agreements and Agreements with Third Party Service Providers

The policy defines an information security breach as an incident in which any of CCN'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 "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 CCN 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 and investigate the breach. This includes responsibility of the Privacy Officer 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.

The Privacy Officer must also take or recommend any remedial action required, provide notice where appropriate to the hospital(s) and 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 notify the CEO.

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.

Once the breach has been contained, the Privacy Officer is responsible for reviewing the steps of containment in order to ensure that they have been effective.

The Privacy Officer has developed a template for reporting the details of the breach to the CEO which includes the following information:

- Recipient (the CEO)
- Date sent to CEO
- Prepared by (CCN 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

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. As set out in the "Information Security and Privacy Breach Management" policy, CCN 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 CCN'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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). CCN has a number of information security audit practices that can identify cases in which personal health information has been compromised within the CCN network. Additionally, CCN's Privacy Officer audits the CCN shared hard drive for evidence of unauthorized personal health information on at least a quarterly basis. Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy, and may result in disciplinary action.

## 1.30 Log of Privacy Breaches

As set out in the"Information Security and Privacy Breach Management" policy, CCN 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 CCN 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; and
- The manner in which each recommendation was or is expected to be addressed.

## 1.31 Policy and Procedures for Privacy Complaints and Privacy Inquiries

In response to a recommendation made by the IPC during its review of CCN in 2008, CCN 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 CCN's commitment to remain open to the questions and concerns of the public. It was developed by CCN'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 CCN to receive and respond to complaints, inquiries, and comments made by any individual. The policy, which is publicly available on CCN's website, provides that these communications should be directed to the Privacy Officer, and provides contact information for both CCN's provincial office and the office of the IPC. The "Privacy Inquiries and Complaints"

policy provides contact information for CCN, CCN's Privacy Officer, and the IPC. Contact information for CCN'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 CCN's compliance with PHIPA and its regulation may be able to direct those complaints or inquiries to the IPC.

CCN'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 CCN's privacy and security policies, procedures and practices, is alleged, the Privacy Officer must determine whether or not 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 a 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. 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 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN 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 CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy, and may result in disciplinary action.

## 1.32 Log of Privacy Complaints

As mentioned above, the Privacy Officer is responsible for maintaining and updating CCN'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 or not 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; and
- 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, CCN has not received any privacy complaints.

## 1.33 Policy and Procedures for Privacy Inquiries

CCN 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.

# PART 2 – Security Documentation

## 2.1 Information Security Policy

The "Protection of Personal Health Information" policy sets out that CCN must have a credible program to continually assess and respond to threats and risks to the data holdings containing personal health information in CCN'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 CCN's custody against theft, loss and unauthorized use or disclosure and to ensure that the records of PHI 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. CCN's security policy requires the security program to employ physical, technical, and administrative safeguards that are consistent with established industry standards and practices in order to maintain the integrity of personal health information. The Privacy Officer is responsible for implementing, monitoring, and reviewing CCN's security program.

CCN's security program includes:

- A framework for the governance of CCN's security program;
- Policies and procedures for the administration of training to CCN 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 control;
- 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; and
- 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, CCN 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 and support procedures and technical vulnerability management. CCN has an information technology team that the Privacy Officer can call on regarding the software or operating environment used by CCN and the protection of personal health information in CCN's custody.

As required by the policy "Protection of Personal Health Information", CCN has ordered both organization-wide and appropriate project specific threat risk assessments, to be conducted by third-party experts in order to identify and minimize vulnerabilities and increase overall security. The last such assessment was conducted in 2013 by Cygnos IT Security. The recommendations made in that assessment were incorporated into CCN's information security policies by the Supervisor Database/Application Development.

CCN has a number of 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 CCN information;
- The encryption of all personal health information being transferred to, from, or within the CCN network;
- Password protection on the workstations of all CCN staff;
- A system-wide rule for password-protected screensavers to be activated after one minute 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 CCN's network; and
- The use of network intrusion detection software to identify any unauthorized access to the CCN network.

The policies associated with CCN'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, "Privacy 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 CCN agents must comply with the "Information Security" policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). The Privacy Officer or a designate will, on a quarterly basis, review the logs described above. Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy, and may result in disciplinary action.

## 2.2 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 CCN. The purpose of the review is to determine whether amendments or new security policies, procedures and practices are required.

As mentioned above, CCN'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 CCN policy reflects advancements in technology and in industry practices,

and also 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, CCN'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 Part 5 of this document.

Under the "Annual Review of Privacy and Security Policies and Procedures" policy, CCN's Privacy Officer is responsible for the communication of new or amended policies to the public and to CCN 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 CCN agents comply with "Annual Review of Privacy and Security Policies and Procedures". The Privacy Officer undertakes the day-to-day responsibility for this task.

CCN 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 on a quarterly basis.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Director of Communications and Corporate Services or her/his designate on a quarterly basis (in compliance with the CCN 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 the Director of Communications and

Corporate Services determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy, and may result in disciplinary action.

## 2.3 Policy and Procedures for Ensuring Physical Security of Personal Health Information

CCN has developed a policy ("Physical Security") addressing the physical safeguards to protect personal health information against loss, theft and unauthorized use or disclosure, unauthorized copying, modification or disposal. CCN'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 one database server) requires that individuals successfully pass through multiple levels of security.

**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 CCN 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, CCN's IT services provider, have access to the server room to perform

maintenance. This privilege is given to these agents conditional on a continued need in order to fulfil the agent's job description or contractual duties. Under CCN'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.

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

To protect the physical security of its provincial office, CCN 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 CCN's Privacy Officer immediately.

In the event that 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 CCN 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 CCN office, and a description of these measures. These forms are retained in a repository by the Privacy Officer.

**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 CCN provincial office and the secure server room. CCN's policy that sets out the procedures for the termination of employment ("Termination of Employment") states that the Privacy Officer must collect all CCN property (keys, identification tags, passwords, among other items) from individuals whose employment has been terminated. Because of the limited number of people employed by CCN (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 CCN are required to give prior notice of 2-6 weeks, depending on the nature of the position and their specific employment contract.

**Notification When Access is No Longer Required**

Currently, the only CCN agents with access to the locked server room, where personal health information is stored, are managers, 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, CCN does not require a policy requiring agents to provide notification when access is no longer required.

**Audits of Agents with Access to the Premises**

Because of the small number of people who have relationships with CCN, 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, CCN 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 CCN's Suite quarterly in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing").

**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 CCN 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.

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

CCN has developed a policy ("Physical Security") on access to the CCN provincial office premises by visitors. This policy defines "visitor" as any individual who is not party to a contractual or other written agreement with CCN and who is present at the CCN premises with the specific intent of visiting a member of the CCN staff. Because CCN 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 CCN agent that the visitor requests. That agent must accompany the visitor at all times.

CCN's new office (move completed Spring 2013) 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 CCN agent. There is a locked door accessible only by key card

separating the main board room from the rest of the CCN's office and with the exception of the main boardroom, access to CCN's offices are locked to visitors at all times.

Visitors to the CCN office must sign in at the front office. CCN'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 CCN agent who they are visiting)

Because CCN 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. In the event that 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.4 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 CCN 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.

## 2.5 Policy and Procedures for Secure Retention of Records of Personal Health Information

CCN's policy "Secure Retention of Personal Health Information" sets out that all personal health information is to be stored on CCN's secure network, which is comprised of one database server in the locked server room in CCN's provincial office. CCN agents are prohibited from retaining personal health information on paper. Furthermore, CCN 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 CCN'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 CCN'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.

CCN 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.

CCN 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;
- CCN 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, network encryption and intrusion detection systems; and
- A credible program for continuous assessment and verification of the effectiveness of the security program in order 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 CCN database is secure in the event of a disaster affecting the database held at CCN's provincial office. Currently, long-term tape backup storage services are provided by Recall.

Tape backups are required to be provided to representatives from the third party service provider on a daily basis 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 CCN 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.

CCN'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 CCN 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.6 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 CCN's secure network.

Mobile Devices are defined as but are not restricted 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.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.7 Policy and Procedures for the Secure Transfer of Personal Health Information

CCN 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, CCN's Privacy Officer is responsible for ensuring that these transfers are made in a secure manner.

CCN only permits the transfer of personal health information via secure connection and at least industry standard encryption. These transmissions are primarily made to CCN by Cancer Care Ontario, who receives personal health information from Data Clerks and Regional Cardiac Care Coordinators at CCN hospitals. Additionally, CCN 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. CCN prohibits the transfer of personal health information using other media, including paper.

CCN'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 CCN shared server for later review and auditing.

Third party service providers who store CCN database tape backups are required to provide CCN 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 CCN. CCN's Data 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 and best practices issued by the IPC and existing privacy and security standards and best practices. In accordance with "Review of Privacy and Security Policies and Procedures", CCN'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. In the event that 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.8 Policy and Procedures for Secure Disposal of Personal Health Information

CCN has developed and implemented a 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 CCN policy "Secure Retention of Personal Health Information" forbids the retention of personal health information on any medium other than the secure CCN server or its tape backups. CCN 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, CCN has a third party agreement with

Shred-It. For the secure disposal of electronic personal health information, CCN provides its own destruction. It is highly uncommon for CCN 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 or not 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 CCN 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.
- In the event that Shred-It fails to provide CCN 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. In the event that 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 CCN'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 CCN's policy on secure retention of personal health information ("Secure Retention of Personal Health Information"), CCN 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 CCN 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 CCN policy, "Secure Transfer of Personal Health Information".

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.9 Policy and Procedures Relating to Passwords

CCN has developed a policy ("Password Policy") governing the passwords used by agents to access their accounts on the CCN 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 the 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 workstation, preventing the user from accessing the desktop. This lock can be removed only by a CCN system administrator. The mandatory system-wide password-protected screen saver is triggered, after 10 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, CCN 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 on a quarterly basis.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN 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, on a quarterly basis, audit the CCN shared hard drive for evidence of unauthorized personal health information. Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.10 Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs

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

The "Maintenance and Review of 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 CCN office that is used by CCN agents authorized to access and use personal health information and by authorized staff at participating CCN 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. The CCN Cardiac and Vascular

Registry application is hosted by Cancer Care Ontario, whose staff members log the username, time of login, and changes made to both databases. Neither software logs geographic information because of the limited number (nineteen participating hospitals and the provincial office) of sites from which CCN network can be accessed through the firewall.

The replication of CCN data on Cancer Care Ontario servers is monitored in real time, with automatic alerts for problems or inconsistencies. This provides assurance that CCN data completely resides at Cancer Care Ontario.

CCN'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; and
- Monitoring system logs on Windows Servers to identify any repetitive warning and error logs.

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

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

- 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 other CCN registries
- CCN 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 mutable only 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 reviewer 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 "Maintenance and Review of System Control and Audit Logs" policy states that CCN'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 CCN'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 CCN policy, "Information Security and Privacy Breach Management"), the procedures set out in the CCN policy "Information Security and Privacy Breach Management" will be followed.

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

CCN audits the "Maintenance and Review of 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 CCN's Privacy Officer is responsible with auditing for compliance with this policy on a quarterly basis.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.11 Policy and Procedures for Patch Management

CCN 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, CCN's contracted third party IT service provider, is responsible for monitoring the availability of patches on behalf of CCN. 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 also responsible for analyzing the patch and making the determination as to whether it should be implemented. The policy states that Interface Technologies must take into account 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 crucial or for security by Interface Technologies are downloaded automatically, while service packs, non-crucial 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.12 Policy and Procedures Related to Change Management

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

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

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

To further ensure the security and persistence of CCN networks in the event of a disaster, CCN is required to have tape backups of its servers performed daily through an external vendor, which stores the tapes at an off-site location. CCN 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 CCN's custody is protected and safe. According to the agreement with Recall, CCN 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 CCN for CCN to write over and reuse. Every time the tape backups are given to Recall, CCN's Data Manager is required to log that a backup of the database was given to Recall, along with the time and date, and the representative of Recall is required to provide CCN with a form saying that the backup was received. These forms are retained in a filing cabinet by CCN's Data 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 CCN
- 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 CCN evidence of its compliance with privacy legislation and its privacy and security program
- Providing notice to CCN should Recall receive a complaint from an individual whose personal health information is under CCN's custody. Recall will provide all information necessary, unless it is unlawful to do so, for CCN's resolution of the complaint at CCN's discretion. Recall will implement any changes with respect to CCN's orders arising from the complaint at CCN's expense
- Recall will notify CCN 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 CCN
- Upon the termination or expiry of the agreement, Recall will return all personal health information to CCN. If instructed by CCN, Recall may instead destroy or make anonymous all personal health information in its care and provide a sworn statement to CCN that it has done so.

CCN's Template Agreement for All Third Party Service Providers was introduced after the execution of CCN'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 CCN wish to renew its contract with Recall, CCN 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, CCN's Data Manager is able to determine the efficacy of this method of backing-up the CCN database on regular and frequent basis. As such, CCN 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 in the event that errors are identified.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.14 Policy and Procedures on the Acceptable Use of Technology

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

agents. If the download is approved, agents are required to save the file locally first so that in the event that 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 CCN agent. However, the 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 CCN Code of Conduct or any other CCN 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 CCN to risk of malicious code and may degrade the performance of CCN network systems.
- Agents are not to host or post CCN information on blogs, chat-rooms, 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 CCN 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:

- CCN email addresses will be issued to conduct CCN business. At no time may email accounts other than CCN be used to conduct CCN 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 of 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 CCN information to or from their own personal email account. Likewise, agents are to never send CCN confidential information to a non-CCN 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 CCN 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.
- CCN email addresses are not to be added to mailing lists unless required as part of your assigned job duties. Doing so may lead to CCN email systems receiving excessive unwanted mass email (spam.)
- Another user's email account may not be accessed without written, formal authorization from the CCN 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 CCN's critical functions.
- CCN 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 CCN Code of Conduct or any other CCN policies or procedures.
- All messages sent by email using CCN email systems are the property of CCN. CCN 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.15 Policy and Procedures In Respect of Security Audits

CCN 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 CCN conducts privacy and security audits to assess compliance with the privacy and security policies, procedures and practices implemented by CCN. 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", CCN will perform audits of its privacy program at least quarterly 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.

CCN's security auditing program includes the maintenance, review, and auditing of system control logs. This component of CCN's security program is governed by the policy, "Maintenance and Review of System Control and Audit Logs".

Due to the stability of CCN's operations, CCN has not developed procedures for threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing, or ethical hacks. Rather, CCN orders these types of specialized security audits when circumstances dictate, such as a major change in its 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". CCN last ordered a threat and risk assessment in 2013. The recommendations made in this assessment have been incorporated into CCN's information security policies by the Supervisor Database/Application Development.

Should CCN determine in the future that more frequent or regular threat and risk assessments or other types of specialized security auditing are necessary, CCN's Privacy Officer will prepare a policy and associated procedures for issues relating to these types of security auditing that is compliant with the expectations set out in pages 99-100 of the *Manual*.

As set out in "Policy and Procedures for Privacy and Security Auditing", CCN 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, "Policy and Procedures for Privacy and Security Auditing" sets out 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 Privacy 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

As set out in the "Policy and Procedures for Privacy and Security Auditing", 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 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 CCN'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 CCN by the Privacy Officer as quickly as is reasonably possible. The results of audits are communicated to CCN 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 CCN 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 CCN's operating environment. Recommendations for changes in CCN's operating environment will be implemented in accordance with a timeline set out by the Privacy Officer upon reception of the recommendation.

Should a CCN agent suspect a breach of "Policy and Procedures for Privacy and Security Auditing" or its procedures ("breach" being defined in CCN policy, "Policy and Procedures for Privacy and Information Security Breach Management"), the agent has a duty (articulated in CCN 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 CCN policy, and may result in disciplinary action.

## 2.16 Log of Security Audits

The "Policy and Procedures for Privacy and Security Auditing" sets out that CCN 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.

CCN 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 CCN's Privacy Officer. Recommendations made by security audits will be recorded in greater detail in CCN's consolidated log of recommendations.

## 2.17 Policy and Procedures for Information Security Breach Management

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

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 2.18 Log of Information Security Breaches

CCN 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; and
- The manner in which each recommendation was or is expected to be addressed.

# PART 3 – Human Resources Documentation

## 3.1 Policy and Procedures for Privacy Training and Awareness

CCN has developed and implemented a policy ("Privacy and Security Training") that requires CCN agents to complete initial and ongoing privacy and security training and identifies the procedures to be followed for privacy training. CCN conducts its privacy and security training through an online module that was prepared by a professional privacy consultant. CCN requires all staff to complete privacy training both upon commencement of employment and annually at the start of every fiscal year in April. 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.

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

Thus, while not all CCN employees have access to personal health information, all CCN staff members are required to complete 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, are required to take our 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 CCN who have completed 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 orientation online program and ongoing privacy and security training includes the description of CCN 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 and procedures and practices implemented by CCN 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 CCN manages the privacy program.

The "Privacy and Security Training" policy requires the training program to include advising agents of administrative, physical and technical safeguards implemented by CCN 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 CCN. The "Privacy and Security Training" policy requires the 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 is mandatory. All new employees are required to sign a Confidentiality Agreement as well as complete the online privacy and security training program. The results of this program are automatically tracked online. As a further component of the privacy and security onboarding program, each new employee is required to sign a Confidentiality Agreement with CCN compelling the agent to protect personal health information. All of these contracts are kept in a safe locked location and are accessible only by the Privacy Officer. Additionally, all Confidentiality Agreements are signed, scanned and retained on the CCN company drive accessible as required by the Privacy Officer. The online privacy and security training results 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 CCN to foster a culture of privacy and to 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 CCN's Privacy Officer communicates with agents in relation to privacy and security, the method and nature of the communication.

The CCN Privacy Officer discusses CCN's privacy and security program, and any issues that have arisen, at each monthly staff meeting. 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 CCN 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 on a quarterly basis in accordance with the policy, "Policy and Procedures for Privacy and Security Auditing". Additionally, CCN's CEO provides updates to staff, the Board of Directors, and other interested stakeholders at each Annual General Meeting.

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 3.2 Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training

As set out in the "Privacy and Security Training" policy, CCN maintains a log of attendance for privacy orientation via its online web privacy training. The system identifies the agent, the date and time they completed the privacy training and the score they obtained. CCN employees take this online privacy training every other year on an ongoing basis and the results are obtainable by the Privacy Officer whenever they are required.

## 3.3 Policy and Procedures for Security Training and Awareness

See Section 3.1. The Privacy and Security Training and Awareness Policy and Procedures are combined.

## 3.4 Log of Attendance at Initial Security Orientation and Ongoing Security Training

See Section 3.2. The Log of Attendance for the initial security orientation and ongoing security training is the same as that used for the privacy orientation and ongoing privacy training.

## 3.5 Policy and Procedures for the Execution of Confidentiality Agreements by Agents

CCN 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 CCN agents are required to execute Confidentiality Agreements with CCN 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 CCN must include all of the conditions set out in the template provided by the IPC.

The "Execution of Confidentiality and Non-Disclosure Agreements" policy sets out that CCN's Privacy Officer is responsible for ensuring that the Confidentiality Agreements have been executed with all CCN 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 at the end of each April.

The Privacy Officer must provide notification regarding the necessity of their executing Confidentiality Agreements with CCN in written format to new CCN agents within two days of the outset of their employment or other contractual relationship. As CCN 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 CCN 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 CCN grows.

Additionally, the Privacy Officer must provide written notification regarding the Confidentiality Agreements to all CCN 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 CCN 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 3.6 Template Confidentiality Agreements with Agents

As required by the "Execution of Confidentiality and Non-Disclosure Agreements" policy, CCN 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 CCN's status under PHIPA and its Regulation
- An explanation of CCN's duties under PHIPA and its Regulation
- A statement setting out that individuals who sign the Confidentiality Agreements are agents of CCN in respect of personal health information
- An outline of the responsibilities of CCN 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 CCN 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 CCN 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 CCN 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 CCN all CCN 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 CCN 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 CCN.

**Notification**

- A stipulation that CCN 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 CCN 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 CCN's auditing program for ensuring compliance with its privacy and security program, including the Confidentiality Agreements

## 3.7 Log of Executed Confidentiality Agreements with Agents

The CCN policy "Policies and Procedures for the Execution of Confidentiality and Non-Disclosure Agreements" sets out that CCN'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 charts CCN agents' execution of Confidentiality Agreements. The log includes the name of the agent, the date of commencement of employment, contractual or other relationship with CCN and the dates that the Confidentiality Agreements were executed.

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

CCN has developed a job description for the role of the Privacy Officer ("CCN Privacy Officer Portfolio"). The "CCN 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 CCN. The Privacy Officer is responsible for the development and implementation of a corporate privacy and security program.

The "CCN 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 CCN 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 CCN agents. The "CCN 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 CCN and its stakeholders.

The Privacy Officer must work with all stakeholders that have relationships with CCN relating to privacy or security issues. He or she must cooperate with the IPC or any other legal entity in investigations and reviews of CCN policies. Additionally, the "CCN 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 CCN privacy and security policy, the Privacy Officer is required to represent CCN's interests.

With CCN management and operations staff, CCN's Privacy Officer is responsible for the establishment of a mechanism to track CCN agents' access to personal health information. This will ensure that access to and use of personal health information is compliant with the CCN policy ("Limiting Agent Access to and Use of Personal Health Information") and government regulations. The Privacy Officer is also required to ensure that CCN 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 CCN 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 (e.g., Supervisor Database/Application Development). The Privacy Officer may be delegated additional responsibilities by the CEO.

CCN 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 CCN 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 "Privacy Inquiries and Complaints" policy
- 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

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

See Section 3.8 as the Job Description is one and the same.

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

CCN's policies "Termination of Employment" and "Termination and Cessation of Contractual Relationships" set out that agents and other employees planning to exit CCN must provide advance notice of resignation. Resignations must be submitted in writing to the CEO. CCN 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 CCN 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 [CCN 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 CCN's alone];
- in response to a force majeure under certain circumstances; or
- on the mutual agreement of the parties to terminate the agreement or a Service Schedule.

In regard to termination of employment contracts, a protocol is in place (set out in the CCN policy, "Termination of Employment"). As part of the policy "Termination of Employment", CCN Supervisors and Directors must immediately advise the CEO and Director of Communications and Corporate Services 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 CCN must be made in collaboration with CEO, Director of Communications and Corporate Services, and Manager Finance & Administrative Affairs. CCN 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 Director of Communications and Corporate Services must ensure that communications to staff are appropriate to the situation.

The Director of Communications and Corporate Services, as delegated by the Privacy Officer, will make arrangements to obtain all CCN property on last day of work as is set out in the policy.

When an employee terminates his/her relationship with CCN, 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 CCN property including, desk keys, door keys, building pass card, parking cards, cell phones and application keys are returned to the Director of Communications and Corporate Services (all passwords are required to be immediately deactivated by the Director of IT).

The Privacy Officer has a check list with all required items to be returned that is completed when an employee leaves CCN. This information is maintained by the Director of Communications and

Corporate Services. Typically there is no risk if CCN property is not securely returned because all property pass cards, CCN email and phone accounts are disabled. Employees who are leaving CCN also have an opportunity to submit CCN property to CCN via courier if they are unable to physically come to CCN'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 Director of Communications and Corporate Services and the Director of IT as delegated by the Privacy Officer of CCN).

All access and parking cards to the main building, housing the location of CCN, are collected by the Privacy Officer and, in partnership with the building personnel, the Director of Communications and Corporate Services deactivates these cards on the day of termination.

When CCN terminates an employment contract, the CEO or Director of Communications and Corporate Services 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 CCN's policies "Termination of Employment" and "Termination and Cessation of Contractual Relationships" on a quarterly basis. Should a CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy, and may result in disciplinary action.

## 3.11 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 CCN's operations or reputation.

In the event that an agent breaches a CCN privacy or security policy, or is suspected to have breached a CCN privacy or security policy, the Privacy Officer is responsible for investigating the incident. If the Privacy Officer is under suspicion, the Director of Communications and Corporate Services conducts the investigation. 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 CCN policy and/or expose personal health information
- Whether a privacy breach occurred or personal health information 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 CCN operations
- Damage to CCN'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 CCN company electronic drive.

## PART 4 – Organizational and Other Documentation

## 4.1 Privacy Governance and Accountability Framework

The Chief Executive Officer of CCN is accountable for the protection of personal health information in the custody or under the control of CCN 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 CCN'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 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 CCN employee receives the privacy and security governance and accountability framework document as a hard copy and thereafter it will be available on the CCN intranet web page that is accessible to each CCN employee. The Privacy Officer will make any changes as required and repost on the CCN intranet web page. All new third party suppliers will receive a hard copy of the privacy and security governance and accountability framework upon execution of a services agreement with CCN 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 CCN in a secure and ethical manner.

The Board of Directors provide high level oversight of CCN'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 CCN privacy program, such as, but not limited to privacy breaches, changes to CCN's privacy status or any major changes to PHIPA that affect CCN. The Board of Directors are provided annual updates on the state of the CCN privacy program at the CCN 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 CCN hospitals, our hosting services supplier for our web based wait time information system application and our supplier of network administration support.

The Annual General Meeting reports 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 CCN'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.

## 4.2 Privacy and Security Governance and Accountability Framework

See 4.1. There is a single Privacy and Security Governance and Accountability Framework.

## 4.3 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 CCN as required.

## 4.4 Corporate Risk Management Framework

CCN has developed a comprehensive and integrated "Corporate Risk Management Framework" to identify, assess, mitigate, and monitor risks, including privacy and security risks.

The "Corporate Risk Management Framework" identifies the agents responsible and the process that must be followed in identifying risks that may negatively affect the ability of CCN, 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 "Corporate Risk Management Framework" also addresses the agents responsible, the process that must be followed, and the criteria that must be considered in ranking the risks and

assessing the likelihood of the risks occurring and the potential impact if they occur. It also includes a discussion of the agents or 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 "Corporate Risk Management Framework" 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 "Corporate Risk Management Framework" sets out the process for implementing the mitigation strategies and the other agents or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies.

The "Corporate Risk Management Framework" 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 "Corporate Risk Management Framework" 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 "Corporate Risk Management Framework" 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 "Corporate Risk Management Framework" 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 "Corporate Risk Management Framework" states that the results of the corporate risk management process will be communicated to the CEO for approval and endorsement.

The "Corporate Risk Management Framework" 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 CCN's ability to protect the personal health information in its custody are mitigated. Furthermore, the "Corporate Risk Management Framework" 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.

Finally, the "Corporate Risk Management Framework" sets out the manner in which the corporate risk management framework is integrated into CCN's policies, procedures, and practices as well as the projects undertaken by CCN, and the agent(s) responsible for such integration.

## 4.5 Corporate Risk Register

CCN has not created the corporate risk register based on the "Corporate Risk Management Framework" at this time. As of April 1, 2016, CCN and the Ontario Stroke Network have merged as a single corporate entity. CCN is undergoing a corporate strategy planning exercise being led by its Board of Directors. Upon completion of the corporate strategy planning exercise, the Corporate Risk Framework will be implemented and the Corporate Risk Register will be completed.

## 4.6 Policy and Procedures for Maintaining a Consolidated Log of Recommendations

It is the CCN'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 CCN 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 quarterly, 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 CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in compliance with the CCN policy "Policy and Procedures for Privacy and Security Auditing"). Should the Privacy Officer determine that an agent of CCN 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 CCN 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 CCN agent suspect a breach of this policy or its procedures ("breach" being defined in CCN policy, "Information Security and Privacy Breach Management"), the agent has a duty (articulated in CCN 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 in itself non-compliance with CCN policy and may result in disciplinary action.

## 4.7 Consolidated Log of Recommendations

CCN has developed a policy ("Maintaining a Consolidated Log of Recommendations") compelling it to keep 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. 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.

## 4.8 Business Continuity and Disaster Recovery

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

The "Contingency 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 "Contingency Plan" identifies the agents and other organizations that must be notified in the event of short and long-term business interruptions and threats to CCN's operating capabilities, as well as the agents responsible for providing this notification. The "Contingency Plan" requires that the identified agents provide notice as soon as is reasonably possible in written or electronic format. The "Contingency 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 "Contingency 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 "Contingency Plan" on a quarterly basis to ensure that the contact information remains accurate and up-to-date.

The "Contingency 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 "Contingency 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 "Contingency 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 “Contingency 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 “Contingency 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 “Contingency Plan” sets out the procedures by which decisions are made and actions are taken during business interruptions and threats to CCN’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 “Contingency Plan” also addresses the testing, maintenance, and assessment of the plan. The “Contingency 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 “Contingency 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.

CARDIAC CARE NETWORK

# PART 5: Privacy and Security Indicators

## 5.1 Part 1 – Privacy Indicators

| Privacy Indicators | CCN |
|---|---|
| **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, 2013, privacy policies and procedures were reviewed in:<br>▪<br>▪ September 10, 2014 as part of the annual review and to meet the requirements of the Information and Privacy Commissioner of Ontario in its Three-Year Review;<br>▪ March 15, 2015 following the expansion of CCN's mandate to include vascular services, its corporate reorganization, and its expansion of data collection to include Ontario patients receiving out of province procedures;<br>▪ September 25, 2016 in preparation of the 3-Year IPC review submission.<br>▪ June 22, 2016 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 of CCN's privacy and security policies were reviewed in September 2014 as part of its annual review and to meet the requirements of the Information and Privacy Commissioner of Ontario in its Three-Year Review. Amendments included:<br>▪ Creation and Implementation of a policy on privacy impact assessments ("Privacy Impact Assessments") to set out the procedures for ordering, carrying out, and documenting privacy impact assessments;<br>▪ The policies "Disclosure of Aggregate and/or De-Identified Personal Health Information to Researchers" and |

| | |
|---|---|
| | "Disclosure of Aggregate and/or De-Identified Personal Health Information to Researchers" amended to more clearly establish documentation procedures;<br>▪ The "Limiting Use, Disclosure and Retention of Personal Health Information" policy was amended to expressly prohibit data linkages;<br>▪ Policy "Termination and Cessation of Contractual Relationships" was amended to clarify the process for terminating contractual relationships.<br>▪ All of CCN's privacy and security policies were reviewed in March 2015. Amendments included:<br>▪ All policies which reference cardiac procedures were amended such that they now recognize that CCN also collects data for vascular procedures.<br>▪ All policies which reference "member hospitals" were amended to reflect CCN's corporate reorganization away from a membership-based organization. The policies now refer to "CCN hospitals," "participating hospitals," and often simply "hospitals."<br>▪ All policies which reference procedures in Ontario were amended to reflect CCN's expanded capacity to collect personal health information for the Registry from certain centres outside of Ontario where Ontario patients are treated. |
| ▪ 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 | ▪ As a result of the 2014 3-Year review, on request of the IPC, CCN developed and implemented 1 new policies:<br>▪ The "Privacy Impact Assessments" policy to set out the procedures for |

| | |
|---|---|
| policies and procedures developed and implemented. | ordering, carrying out, and documenting privacy impact assessments. |
| ▪ 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 CCN bundles together into a single package, were posted on the CCN Intranet promptly following each review period that produced amendments. This occurred on:<br>▪ May 5, 2014<br>▪ November 17, 2014<br>▪ April 1, 2016<br>▪ June 22, 2016<br>▪ CCN's Privacy Officer and/or the CEO discussed privacy and security issues at staff meetings that took place on<br>– October 17, 2014<br>– Friday 27, 2015<br>– March 17, 2016<br>– June 14, 2017 |
| ▪ 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 in April 2016. All material which referenced CCN's data collection for cardiac procedures were amended such that they now recognize that CCN also collects data for vascular procedures. |
| **Collection** | |
| ▪ The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity. | ▪ CCN 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. | ▪ CCN 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. | ▪ CCN's WTIS-CCN statement of purpose has been reviewed since November 1, 2013. It was amended to reflect the name change to the CCN Cardiac Data Holding A statement of purpose was created for the |

| | |
|---|---|
| | CCN Vascular Data Holding when it was implemented April 1, 2016 |
| ▪ 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. | ▪ CCN amended the WTIS-CCN statement of purpose to reflect the name change to the CCN Cardiac data holding. |
| **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 552 CCN agents (includes CCN staff, CCO staff and participating hospitals) with access to personal health information for purposes other than research, including 35 CCN staff members at the CCN Provincial Office. |
| ▪ The number of requests received for the use of personal health information for research since the prior review by the IPC. | ▪ CCN does not use personal health information for research. There were no requests by CCN 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 CCN 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. | ▪ CCN does not disclose personal health information for any reason to any organization or individual. No such requests have been granted. |
| ▪ The number of requests received for the disclosure of personal health information | ▪ There have been zero requests for the disclosure of personal health information for research purposes. |

| | |
|---|---|
| for research purposes since the prior review by the IPC. | |
| ▪ 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. | ▪ CCN does not disclose personal health information for any reason to any organization or individual. 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. | ▪ CCN does not disclose personal health information. No Research Agreements providing for the disclosure of personal health information have been executed with researchers. |
| ▪ 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 14 requests for the disclosure of aggregate, de-identified information since November 1, 2013. |
| ▪ The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes since the prior review by the IPC. | ▪ 14 of the 14 requests for the disclosure of aggregate, de-identified information since November 1, 2013 were granted and agreements with 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. | ▪ CCN 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. | ▪ CCN is a party to one active data sharing agreement (DSA) with the Institute for Clinical Evaluative Sciences (ICES), executed in March 2009. That DSA expired and CCN and ICES executed a new DSA in June 2016. |
| **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. | ▪ CCN is party to an agreement with Cancer Care Ontario for hosting services, 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 |

| | |
|---|---|
| | ShredIt for paper shredding services, for a total of 4 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, 2013. 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 impact assessment:<br>– The data holding, information system, technology or program,<br>– The date of completion of the privacy impact assessment,<br>– A brief description of each recommendation,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. | ▪ Zero privacy impact assessments have been undertaken since November 1, 2013. As per CCN's policy "Privacy Impact Assessments" CCN conducts a PIA, at minimum, in conjunction with the 3-Year IPC review. CCN is currently planning its next PIA. |
| ▪ 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 | ▪ There is currently one PIA which will be completed. CCN is beginning the process of planning its next PIA. The scope of the PIA |

| | |
|---|---|
| be completed and the proposed date of completion. | will be defined and a third party will be chosen to perform the PIA. It is anticipated that the PIA will be completed before CCN's privacy status expires on October 31, 2017. |
| ▪ 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 was one determination made since November 1, 2013 that a PIA was not required. The determination was made for the launch of the CCN Vascular data holding. As the CCN Vascular data holding was built on the exact same technology system as the CCN Cardiac and Vascular Registry (the Wait Times Information System at Cancer Care Ontario), and the last PIA done on the CCN Cardiac and Vascular Registry resulted in no recommendations, it was determined that a new PIA was not required. |
| ▪ The number and a list of privacy impact assessments reviewed since the prior review by the Information and Privacy Commissioner and a brief description of any amendments made. | ▪ The privacy impact assessment completed by David Flaherty for CCN in 2013 was reviewed in advance of the 3-Year IPC review. No recommendations were made in that PIA so no amendments were made to any privacy or security policies. |
| **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:<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– 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, 2013 was reviewed in:<br>▪ November 2013<br>▪ February 2014<br>▪ May 2014<br>▪ August 2014<br>▪ November 2014<br>▪ March 2015<br>▪ June 2015<br>▪ September 2015<br>▪ November 2015<br>▪ January 2016<br>▪ April 2016<br>▪ September 2016<br>These audits were completed as parts of CCN'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:<br>– A description of the nature and type of audit conducted,<br>– The date of completion of the audit,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. | ▪ Since the beginning of the current IPC review period on November 1, 2013, privacy and security audits were completed in November 2013, February 2014, May 2014, August 2014, November 2014, March 2015, June 2015, September 2015, November 2015, January 2016, April 2016, and September 2016, November 2016, March 2017, and June 2017. These audits were all conducted according to the procedures set out in the CCN policy, "Policy and Procedures for Privacy and Security Auditing".<br>▪ In the November 2013 audit, no recommendations were made.<br>▪ In the February 2014 audit, no recommendations were made.<br>▪ In the May 2014 audit, no recommendations were made.<br>▪ In the August 2014 audit, no recommendations were made.<br>▪ In the November 2014 audit, the following recommendations were made:<br>▪ The privacy-related documents on the CCN website (the privacy and security policy, the report to the IPC, and the letter of approval from the IPC) were updated with new documents (addressed November 2014)<br>▪ Two agents who were no longer with CCN but were still on the list of agents with access to personal health information were removed |

| | |
|---|---|
| | from the list (addressed November 2014).<br>▪ In the March 2015 audit, the following recommendations were made:<br>▪ The consolidated log of recommendations was updated with the recommendations from the Q4 privacy audit (addressed March 2015).<br>▪ An updated privacy training module will be administered to all CCN agents upon its completion (module was completed and made available to agents November 2015).<br>▪ Two agents who were no longer with CCN but were still on the list of agents with access to personal health information were removed from the list (addressed March 2015).<br>▪ In the June 2015 audit, no recommendations were made.<br>▪ In the September 2015 audit, no recommendations were made.<br>▪ In the November 2015 audit, no recommendations were made.<br>▪ In the January 2016 audit, no recommendations were made.<br>▪ In the April 2016 audit, the following recommendations were made:<br>▪ The policy "Secure Transfer of Personal Health Information" was amended to include language that PHI would be transferred over secure encrypted connections however not just solely |

| | |
|---|---|
| | Secure File Transfer Protocol (addressed April 2016).<br>▪ In the September 2016 audit, no recommendations were made.<br>▪ In the November 2016 audit, no recommendations were made.<br>▪ In the March 2017 audit, no recommendations were made.<br>▪ In the June 2017 audit no recommendations were made. |
| **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, 2013. |
| ▪ With respect to each privacy breach or suspected privacy breach:<br>– The date that the notification was received,<br>– The extent of the privacy breach or suspected privacy breach,<br>– Whether it was internal or external,<br>– The nature and extent of personal health information at issue,<br>– The date that senior management was notified,<br>– The containment measures implemented,<br>– The date(s) that the containment measures were implemented,<br>– The date(s) that notification was provided to the health information custodians or any other organizations,<br>– The date that the investigation was commenced,<br>– The date that the investigation was completed, | ▪ No notifications of privacy breaches have been received since November 1, 2013. |

| | |
|---|---|
| – A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– 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 CCN since November 1, 2013. |
| ▪ 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:<br>– The date that the privacy complaint was received,<br>– The nature of the privacy complaint,<br>▪ The date that the investigation was commenced,<br>▪ The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation,<br>▪ The date that the investigation was completed,<br>– Brief description of each recommendation made,<br>▪ The date each recommendation was addressed or is proposed to be addressed,<br>▪ The manner in which each recommendation was addressed or is proposed to be addressed, and<br>▪ 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. | ▪ There have been no privacy complaints made to CCN since November 1, 2013. |

| | |
|---|---|
| ▪ 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:<br>– The date that the privacy complaint was received,<br>– The nature of the privacy complaint, and<br>– 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 CCN since November 1, 2013. |

## 5.2 Part 2 – Security Indicators

| Security Indicators | CCN |
|---|---|
| **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, 2013, security policies and procedures were reviewed in:<br>▪ September 10, 2014 as part of the annual review and to meet the requirements of the Information and Privacy Commissioner of Ontario in its Three-Year Review;<br>▪ March 15, 2015 following the expansion of CCN's mandate to include vascular services, its corporate reorganization, and its expansion of data collection to include Ontario patients receiving out of province procedures;<br>▪ September 25, 2016 in preparation of capturing of vascular data;<br>▪ June 22, 2016 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 | ▪<br>▪ Many of CCN's policies were reviewed in September 2014 as part of the 2014 annual review and to meet the |

| | |
|---|---|
| and, for each policy and procedure amended, a brief description of the amendments made. | requirements of the Information and Privacy Commissioner of Ontario in its Three-Year Review.<br>▪ Creation and implementation of a patch management policy (Patch Management Policy)All of CCN's privacy and security policies were reviewed in Fall-Winter 2014-5. Amendments included:<br>▪ All policies which reference cardiac procedures were amended such that they now recognize that CCN also collects data for vascular procedures.<br>▪ All policies which reference "member hospitals" were amended to reflect CCN's corporate reorganization away from a membership-based organization. The policies now refer to "CCN hospitals," "CCN-associated hospitals," and often simply "hospitals."<br>▪ All policies which reference procedures in Ontario were amended to reflect CCN's expanded capacity to collect personal health information for the Registry from certain centres outside of Ontario where Ontario patients are treated.<br>▪ As part of the Q1 2016/17 quarterly Privacy and Security audit the policy "Secure Transfer of Personal Health Information" was amended to include language that PHI would be transferred over secure encrypted connections however not just solely Secure File Transfer Protocol. |
| ▪ 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. | ▪ As a result of the 2014 annual review and to meet the requirements of the Information and Privacy Commissioner of Ontario in its Three-Year Review, one new policy was developed and implemented: |

| | |
|---|---|
| | ▪ "Patch Management Policy" was developed and implemented in order to describe the means by which CCN ensures that the latest patches and updates are being applied to the servers, computers, firewalls and routers in the network in order to make sure our servers, computers, firewalls and routers remain secure, and are not vulnerable to attacks. |
| ▪ 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 CCN bundles together into a single package, were posted on the CCN Intranet promptly following each review period that produced amendments. This occurred on:<br>▪ May 5, 2014<br>▪ November 17, 2014<br>▪ April 1, 2016<br>▪ June 22, 2016<br>▪ CCN's Privacy Officer and/or the CEO discussed privacy and security issues at staff meetings that took place on<br>– October 17, 2014<br>– February, 2015<br>– March 17, 2016<br>– June 14, 2017 |
| ▪ 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 in April 2016. All material which referenced CCN's data collection for cardiac procedures were amended such that they now recognize that CCN also collects data for vascular procedures. |
| **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 | ▪ The log of agents granted approval to access the premises since November 1, 2013 was reviewed in:<br>▪ November 2013<br>▪ February 2014<br>▪ May 2014 |

| | |
|---|---|
| Information and Privacy Commissioner and for each audit:<br>– A brief description of each recommendation made,<br>▪ The date each recommendation was addressed or is proposed to be addressed, and<br>▪ The manner in which each recommendation was addressed or is proposed to be addressed. | ▪ August 2014<br>▪ November 2014<br>▪ March 2015<br>▪ June 2015<br>▪ September 2015<br>▪ November 2015<br>▪ January 2016<br>▪ April 2016<br>▪ September 2016<br>▪ November 2016<br>▪ March 2017<br>▪ June 2017<br>▪ These audits were completed as parts of CCN'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 CCN's "Maintenance and Review of System Control and Audit Logs" policy sets out that software that provides for real-time monitoring of CCN data replication resides on servers at Cancer Care Ontario. The software automatically alerts CCN IT staff if a technical or security issue with the data duplication arises. There is thus no need to review these system control logs<br>▪ CCN's IT staff, under the direction of the Privacy Officer and the Director of IT, have carried out the majority of recommendations made by Cygnos IT Security in its 2013 TRA. |
| ▪ The number and a list of security audits completed since the prior review by the IPC and for each audit:<br>▪ A description of the nature and type of audit conducted,<br>▪ The date of completion of the audit,<br>▪ A brief description of each recommendation made, | ▪ Since the beginning of the current IPC review period on November 1, 2013, privacy and security audits were completed in November 2013, February 2014, May 2014, August 2014, November 2014, March 2015, June 2015, September 2015, November 2015, January 2016, April 2016, and September 2016, November 2016, March 2017, and June 2017. These audits |

| | |
|---|---|
| ▪ The date that each recommendation was addressed or is proposed to be addressed, and<br>▪ The manner in which each recommendation was addressed or is expected to be addressed. | were all conducted according to the procedures set out in the CCN policy, "Policy and Procedures for Privacy and Security Auditing".<br>▪ In the November 2013 audit, no recommendations were made.<br>▪ In the February 2014 audit, no recommendations were made.<br>▪ In the May 2014 audit, no recommendations were made.<br>▪ In the August 2014 audit, no recommendations were made.<br>▪ In the November 2014 audit, the following recommendations were made:<br>  ▪ The privacy-related documents on the CCN website (the privacy and security policy, the report to the IPC, and the letter of approval from the IPC) were updated with new documents (addressed November 2014)<br>  ▪ Two agents who were no longer with CCN but were still on the list of agents with access to personal health information were removed from the list (addressed November 2014).<br>▪ In the March 2015 audit, the following recommendations were made:<br>  ▪ The consolidated log of recommendations was updated with the recommendations from the Q4 privacy audit (addressed March 2015)<br>  ▪ An updated privacy training module will be administered to all CCN agents upon its |

| | |
|---|---|
| | completion (module was completed and made available to agents November 2015).<br>▪ Two agents who were no longer with CCN but were still on the list of agents with access to personal health information were removed from the list (addressed March 2015).<br>▪ In the June 2015 audit, no recommendations were made.<br>▪ In the September 2015 audit, no recommendations were made.<br>▪ In the November 2015 audit, no recommendations were made.<br>▪ In the January 2016 audit, no recommendations were made.<br>▪ In the April 2016 audit, the following recommendations were made:<br>▪ The policy "Secure Transfer of Personal Health Information" was amended to include language that PHI would be transferred over secure encrypted connections however not just solely Secure File Transfer Protocol (addressed April 2016).<br>▪ In the September 2016 audit, no recommendations were made.<br>▪ In the November 2016 audit, no recommendations were made.<br>▪ In the March 2017 audit, no recommendations were made.<br>▪ In the June 2017 audit no recommendations were made. |
| **Information Security Breaches** | |

| | |
|---|---|
| ▪ The number of notifications of information security breaches or suspected information security breaches received by the prescribed person or prescribed entity since the prior review by the IPC. | ▪ There have been no information security breaches or suspected information security breaches since November 1, 2013. |
| ▪ With respect to each information security breach or suspected information security breach:<br>– The date that the notification was received,<br>– The extent of the information security breach or suspected information security breach,<br>– The nature and extent of personal health information at issue,<br>– The date that senior management was notified,<br>– The containment measures implemented,<br>– The date(s) that the containment measures were implemented,<br>– The date(s) that notification was provided to the health information custodians or any other organizations,<br>– The date that the investigation was commenced,<br>– The date that the investigation was completed,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. | ▪ There have been no information security breaches or suspected information security breaches since November 1, 2013. |

## 5.3 Part 3 – Human Resources Indicators

| Human Resources Indicators | CCN |
|---|---|
| **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. | ▪ 552 CCN agents, including applicable staff of health information custodians, committee members, and CCN staff have completed initial privacy training since November 1, 2013.<br>▪ 0 agents of CCN 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 CCN 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, CCN's privacy and security policies only required ongoing training on a biennial basis. Due to this policy a number of agents did not receive ongoing privacy training each year. CCN has since amended its policies to mandate annual privacy training. CCN will ensure that all agent's annual ongoing privacy training is completed by September 1, 2017. Moving forward all agents will receive ongoing privacy training on an annual basis.<br>▪ **November 1, 2013 to December 31, 2014**<br>▪ Zero agents attended ongoing privacy training<br>▪ 32 agents did not attend ongoing privacy training<br>**2015**<br>▪ 36 agents attended ongoing privacy training<br>▪ 8 agents did not attend ongoing privacy training<br>**2016**<br>▪ 1 agent attended ongoing privacy training<br>▪ 19 agents did not attend ongoing privacy training |

| | |
|---|---|
| | **2017**<br>▪ 2 agents attended ongoing privacy training<br>▪ 40 agents did not attend ongoing privacy 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 CCN bundles together into a single package, were posted on the CCN Intranet promptly following each review period that produced amendments. This occurred on:<br>▪ May 5, 2014<br>▪ November 17, 2014<br>▪ April 1, 2016<br>▪ June 22, 2016<br>▪ CCN's Privacy Officer and/or the CEO discussed privacy and security issues at staff meetings that took place on<br>– October 17, 2014<br>– February 27, 2015<br>– March 17, 2016<br>– June 22, 2016 |
| **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. | ▪ 552 agents of CCN, including applicable staff of health information custodians, committee members, and CCN staff have completed initial security training since November 1, 2013.<br>▪ 0 agents of CCN 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 CCN agents have attended initial security training since November 1, 2013. |
| ▪ 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, CCN's privacy and security policies only required ongoing security training on a biennial basis. Due to this policy a number of agents did not receive ongoing security training |

| | |
|---|---|
| | each year. CCN has since amended its policies to mandate annual security training. CCN will ensure that all agent's annual ongoing security training is completed by September 1, 2017. Moving forward all agents will receive ongoing security training on an annual basis.<br>**November 1, 2013 to December 31, 2014**<br>▪ Zero agents attended ongoing security training<br>▪ 32 agents did not attend ongoing security training<br>**2015**<br>▪ 36 agents attended ongoing security training<br>▪ 8 agents did not attend ongoing security training<br>**2016**<br>▪ 1 agent attended ongoing security training<br>▪ 19 agents did not attend ongoing security training<br>**2017**<br>▪ 2 agents attended ongoing security training<br>▪ 40 agents did not attend ongoing 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 CCN bundles together into a single package, were posted on the CCN Intranet promptly following each review period that produced amendments. This occurred on:<br>▪ May 5, 2014<br>▪ November 17, 2014<br>▪ April 1, 2016<br>▪ June 22, 2016<br>▪ CCN's Privacy Officer and/or the CEO discussed privacy and security issues at staff meetings that took place on<br>– October 17, 2014<br>– February 27, 2015<br>– March 17, 2016 |

| | |
|---|---|
| | – June 14, 2017 |
| **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, 78 agents have executed Confidentiality Agreements (called Non-Disclosure Agreements throughout this report) since November 1, 2013. This includes 22 agents who no longer have relationships with CCN.<br>▪ All agents have executed Non-Disclosure Agreements with CCN since November 1, 2013. |
| ▪ 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 CCN agents have signed Non-Disclosure Agreements with CCN. |
| **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, 2013:<br>▪ 6 contract employees had their contracts end<br>▪ 9 employees resigned/retired<br>▪ 7 employees were terminated |

## 5.4 Part 4 – Organizational Indicators

| Organizational Indicators | CCN |
|---|---|
| **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. | ▪ CCN has not reviewed the corporate risk register since the last review by the IPC. As of April 1, 2016 CCN and the Ontario Stroke Network have merged as a single corporate entity. CCN is currently undergoing a corporate strategy planning exercise being led by its Board of Directors. It is anticipated that a revised Corporate Risk Framework will be implemented as part of |

| | |
|---|---|
| | this process to populate a new Corporate Risk Registry. |
| ▪ 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 have been made to the corporate risk register. |
| **Business Continuity and Disaster Recover** | |
| ▪ The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC. | CCN developed a business continuity and disaster recovery plan in June 2015. The plan has not yet been tested. CCN is in the process of developing and implementing a corporate risk framework and register. CCN's CEO left just prior to implementation of its corporate risk framework and register and CCN has had an interim CEO for some time. As a result, the implementation of the corporate risk framework and register was delayed. However, CCN plans to meet with Healthcare Insurance Reciprocal of Canada (HIROC) in August to begin developing Risk Management tools and templates with the goal of have an initial corporate risk register in place by December 1, 2017. The exercise of creating and implementing the corporate risk register will identify risks to CCN and will inform a detailed review of the BCDRP. It is anticipated that as a result of the creation of a corporate risk register and a review of the BCDRP that revision will be required to the BCDRP. The BCDRP will be tested once that review process is complete. CCN will confirm timing for the revision and testing of an updated BCDRP once the corporate risk register has been completed. |
| ▪ 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 and disaster recovery plan. |