CARDIAC CARE NETWORK

2011 REPORT OF CARDIAC CARE NETWORK

TO

THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

August 30, 2011

Table of Contents

Introduction

The Cardiac Care Network (CCN) is a network of eighteen member hospitals providing selected advanced cardiac services in Ontario. CCN is mandated by the Ontario Ministry of Health and Long-Term Care (MOHLTC) to help plan, organize, and evaluate cardiovascular care in Ontario. In addition, CCN is responsible for developing, maintaining and reporting on the provincial cardiac wait list registry (Registry) for all patients waiting for select adult advanced cardiac procedures in Ontario. CCN maintains the Registry for the purposes of facilitating and improving the provision of cardiac care services in the Province of Ontario. CCN requires the personal health information it collects and maintains in the Registry to monitor and manage the health status of patients who are waiting to access advanced cardiac services and for service evaluation and planning.

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 Registry. Information about the Registry is publicly available on the CCN website at www.ccn.on.ca. Health Information Custodians (as defined in PHIPA) are allowed to disclose personal health information to CCN without patient consent under section 39(c) of PHIPA for the purposes of maintaining the Registry, a registry designed to improve the provision of health care.

In accordance with the general regulations made under PHIPA, 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 Patients and maintaining the confidentiality of personal health information, along with its strategy and plans for its privacy and security program. This report specifically addresses the improvements to CCN's privacy and security program at CCN achieved through the implementation of recommendations made by the IPC in following its Three-Year Review of CCN in 2008.

In this report, the term "mobile devices" means any portable storage devices that could be used to digitally/electronically copy, transcribe or store files, including but not limited to cell phones, smart phones, laptops and Blackberry devices. Furthermore, the term "agents" refers to any employees, health information custodians, contractors, consultants, volunteers, members of the Board of Directors, or other individual with whom CCN has a contractual or other type of relationship.

PART 1 – Privacy Documentation

Privacy Policy in Respect of its Status as a Prescribed Person

CCN has developed and implemented an overarching privacy policy ("Protection of Personal Health Information") to protect the personal health information that it receives. The policy was developed with respect to PHIPA and CCN's status as a prescribed person.

Status under the Act

CCN's over-arching privacy policy is named "Protection of Personal Health Information". It is made available on the CCN website (www.ccn.on.ca), and states that CCN is an advisory body to the MOHLTC and a prescribed person within the meaning of Section 39(1)(c) of PHIPA. "Protection of Personal Health Information" also states that as a prescribed person, CCN must implement practices and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. "Protection of Personal Health Information" articulates a commitment to comply with the provisions of PHIPA and its regulation applicable to CCN. "Protection of Personal Health Information" also states that the privacy and security policies, procedures, and practices of CCN are subject to review by the Information and Privacy Commissioner of Ontario every three years.

Privacy and Security Accountability Framework

The first policy statement of "Protection of Personal Health Information" states that CCN's Chief Executive Officer is ultimately responsible for ensuring compliance with PHIPA and its regulation. It further states that the CEO has delegated day-to-day authority to manage the privacy program and the security program to the CCN Privacy Officer, whose other title is the Director of Operations and Stakeholder Relations. "Protection of Personal Health Information" makes clear that the Privacy Officer is responsible for the implementation and enforcing of CCN's privacy policies and security policies and for ensuring compliance with PHIPA and its regulation.

Collection of Personal Health Information

"Protection of Personal Health Information" states that within the meaning of PHIPA, CCN is permitted to collect personal health information without patients' consent for the purposes of facilitating or improving the provision of cardiac care services. "Protection of Personal Health Information" states that personal health information from patients who undergo select adult cardiac care will be collected and lists the types of personal health information that are collected. "Protection of Personal Health Information" states that CCN will limit the collection of personal health information to that which is necessary for the purposes it has identified and that it will collect personal health information by fair and lawful means. "Protection of Personal Health Information" sets out that CCN must ensure that each collection of personal health information is consistent with the collections of personal health information permitted by PHIPA and its regulation. Furthermore, "Protection of Personal Health Information" identifies the PHIPA-compliant purposes for which personal health information is collected. "Protection of Personal Health Information" states that brochures will be given to all Patients from whom personal health information is collected and that these brochures provide information on 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 "Protection of Personal Health Information.

Use of Personal Health Information

"Protection of Personal Health Information" states that CCN only uses personal health information for purposes of facilitating or improving the quality and provision of cardiac care services, namely to maintain wait lists for cardiac care services; ensure that individuals receive timely, equitable, and appropriate access to cardiac care services; provide advice on issues relating to cardiac 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 care services in Ontario; and as permitted or required by law, including PHIPA and its regulation.

"Protection of Personal Health Information" states that CCN protects personal health information by only providing access to personal health information to its agents on a "need to know" basis as is required in the performance of their employment, contractual or other relationship with CCN. "Protection of Personal Health Information" states that CCN requires all CCN agents to sign Confidentiality and Non-Disclosure Agreements that clearly identify their obligations with respect to protecting the confidentiality of personal health information and protecting the privacy of individuals with respect to that information. "Protection of Personal

Health Information" makes clear that CCN is responsible for personal health information under its custody or control and that personal health information that is no longer required for the identified purposes is destroyed in a secure manner. "Protection of Personal Health Information" sets out that no personal health information or aggregate/de-identified health information, is permitted to be used by CCN agents for research purposes. Furthermore, the policy states that CCN agents are prohibited from using personal health information for the fulfilment of their job description or other contractual obligations if aggregate/de-identified health information will suffice. The policy also sets out that the Privacy Officer is responsible for ensuring that each use of personal health information is compliant with PHIPA and its regulation. The policy states that 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 CCN 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.

As CCN's member hospitals are agents of CCN, transfers of personal health information to CCN member hospitals constitute on their part use of personal health information. Hospitals use personal health information in CCN's custody to track the status of patients in their care, to aid in current and strategic planning, and as permitted or required by law, including PHIPA and its regulation. Transfers of personal health information are governed by the CCN policy "Secure Transfer of Personal Health Information". This policy ensures that transfers of personal health information are made 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. These policies ensure that CCN 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. The policy "Destruction of Personal Health Information" governs the secure disposal of personal health information. This policy ensures that CCN agents only dispose of personal health information in a manner that precludes reconstruction and is compliant with PHIPA and in accordance with CCN's privacy and security program.

Disclosure of Personal Health Information

"Protection of Personal Health Information" asserts that CCN does not disclose personal health information except to the Institute for Clinical Evaluative Sciences (ICES), with which CCN has

executed a strong data sharing agreement; and when required by law. Personal health information is disclosed to ICES pursuant to s.13(5) of PHIPA, for section 45 purposes. ICES immediately de-identifies the data upon reception and before any data analysis occurs. CCN does not disclose personal health information to any other organization or entity. “Protection of Personal Health Information” states that de-identified health information may be provided to 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”. This policy requires that aggregate or de-identified information be reviewed prior to its disclosure in order 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.

“Protection of Personal Health Information” sets out the statutory justification (within PHIPA) that allows 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

“Protection of Personal Health Information” states that personal health information collected by CCN is currently being retained for as long as is reasonably necessary for long-term analysis and statistical information. “Protection of Personal Health Information” sets out that 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 currently being retained is set out in the CCN policy, “Secure Retention of Personal Health Information. Currently, personal health information is being stored only 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”. Currently, personal health information may only be transferred under 128-bit encrypted SFTP. 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

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

- Annual privacy and security training
- 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 prior to their collection of personal health information
- CCN is located in a secure location with external video monitoring and progressive grades of 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

"Protection of Personal Health Information" policy identifies the agent to whom 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. "Protection of Personal Health Information" directs inquiries, concerns, and complaints to its Privacy Officer and provides the address contact information for CCN's Provincial Office. "Protection of Personal Health Information" states that inquiries, concerns, or complaints can be made via mail, e-mail, or telephone. As "Protection of Personal Health Information" sets out that individuals may direct complaints regarding the compliance of CCN with the Act and its regulation to the IPC, the privacy policy also lists contact information and the mailing address of the IPC.

Transparency of Practices in Respect of Personal Health Information

"Protection of Personal Health Information", which is made publicly available on CCN's website, states that the purposes for which personal health information is being collected. Furthermore, it provides for an information brochure explaining those purposes to be given to all patients upon the collection of their personal health information. This information brochure will also be made available on the CCN website. "Protection of Personal Health Information" makes clear that information about the Registry must be publicly available on the CCN website.

Policy and Procedures for Ongoing Review of Privacy 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 privacy policies, procedures and practices put in place by CCN. The purpose of the review is to determine whether amendments are needed or whether 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. "Annual Review of Privacy and Security Policies and Procedures" compels the CCN 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). In the event that the law is changed or the IPC issues new guidelines, factsheets, or best practices, CCN's 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 investigations into privacy or 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, procedures and practices and may make recommendations in these regards. In accordance with "Annual Review of Privacy and Security Policies and Procedures", the Privacy officer has the last word in the development and implementation of new and amended policies, the CEO having delegated that authority.

At the last review of the privacy policies, procedures and practices on January 10, 2011, the Privacy Officer did not make any changes as it was apparent that the policies, procedures and practices were in compliance with the IPC requirements and with the requirements of CCN.

As required in the policy, "Annual Review of Privacy and Security Policies and Procedures", CCN's Privacy Officer is also responsible for the communication of new or amended policies to the public and to CCN agents. "Annual Review of Privacy and Security Policies and Procedures" sets out that new and amended policies will be communicated to CCN 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 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. As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "Annual Review of Privacy and Security Policies and Procedures" at the outset of their relationship with CCN and annually. The Privacy Officer is responsible for determining the consequences of a breach, which may include disciplinary action up to termination of employment as set out in CCN Policy.

CCN audits "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". "Policy and Procedures for Privacy and Security Auditing" sets out that the Privacy Officer is responsible for auditing "Annual Review of Privacy and Security Policies and Procedures" to ensure compliance with the policy and its procedures on a quarterly basis.

Policy on the Transparency of Privacy Policies, Procedures and Practices

It is the Cardiac Care Network's policy ("Transparency") to ensure 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 solely of the WTIS-CCN database, which is 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 member 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 "Transparency".

"Transparency" compels CCN to place in all member hospitals brochures 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) registry 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 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 PHI 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.

Policy 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.

"Identifying Purposes for Collecting Personal Health Information" lists the most general types of personal health information that may be collected. 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

CCN health information custodians will also collect procedure-specific information and particulars about a patient's health condition.

"Limiting Collection of Personal Health Information" 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" states that CCN will limit the collection of personal health information to that which is necessary for the purposes of facilitating or improving the provision of cardiac care services and to use personal health information without consent for these purposes, including to maintain wait lists for treatment and to assist in the management and planning of the delivery of cardiac care services.

"Notice/Consent for Collecting, Using, or Disclosing Personal Health Information" articulates a 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 absolutely necessary for the fulfilment of those purposes, CCN requires all agents including employees, contractors, consultants, volunteers and members of the Board of Directors to sign Confidentiality and Non-Disclosure Agreements agreeing 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"). These Confidentiality and Non-Disclosure Agreements set out that failure to comply may result in disciplinary action as determined by the Privacy Officer, up to an including termination of an agent's relationship with CCN. Furthermore, CCN executes Participation Agreements with its member 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 with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's policies 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") at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of these policies, CCN's policy on privacy and security breaches imposes a duty on them to report the breach to CCN's Privacy Officer. If it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

"Limiting Collection of Personal Health Information" sets out that all hospitals must sign Participation Agreements with CCN that detail hospitals' obligations to protect 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 member hospitals. CCN's policy on privacy breaches ("Information Security and Privacy Breach Management") dictates the procedure followed by CCN agents should they suspect that a breach of this policy has taken place.

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"), which states that CCN's policies on the collection of personal health information will be audited quarterly by the Privacy Officer. "Policy and Procedures for Privacy and Security Auditing" also 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 nothing is being collected that is not necessary to fulfil CCN's mandate under PHIPA.

Review and Approval Process

CCN only collects personal health information from its member 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. CCN executes Participation Agreements with all member hospitals that articulate the obligations of both CCN and the hospital in question to protect personal health information. As set out the Participation Agreement, individual hospitals are responsible for ensuring compliance with applicable legislation and CCN privacy and security policies.

CCN only collects the elements of data that are absolutely necessary for its functions as a Registry as set out in subsection 39(1)(c) of PHIPA.

As set out in the CCN policy "Identifying Purposes for Collecting Personal Health Information", CCN's Privacy Officer is responsible for reviewing the elements of data that are collected and ensuring that only the personal health information that is absolutely necessary for CCN's core functions is collected. "Identifying Purposes for Collecting Personal Health Information" 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".

Conditions or Restrictions on the Approval

In accordance with the CCN policy "Accountability for Personal Health Information", CCN executes Participation Agreements with its member hospitals prior to the 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 follow 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 with hospitals have been properly executed prior to the collection of personal health information. As set out in the Participation Agreement, individual hospitals are responsible for ensuring their compliance with applicable legislation and CCN privacy and security policies. As stated in "Accountability for Personal Health Information", CCN's Privacy Officer is responsible for ensuring that hospitals have executed Participation Agreements.

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 following recommendations made by the IPC after its prior review of CCN in 2008. The policy was developed and came into effect in April 2010. Under the new policy, any digital transmissions of personal health information to CCN are made under a VeriSign 128-bit digital 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. "Secure Transfer of Personal Health Information" prohibits the transfer of personal health information in paper format.

Secure Return or Disposal

Currently, personal health information is being retained for as long as necessary for long-term statistical analysis. CCN has developed and implemented a policy on the secure destruction of records of personal health information ("Destruction of Personal Health Information") that identifies the precise method by which records of personal health information in paper and electronic format are required to be securely disposed of. 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, an external company 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, "Destruction of Personal Health Information" states that the drive must be formatted 4 times and then mechanically destroyed.

List of Data Holdings Containing Personal Health Information

CCN documents information relating to its one data holding containing personal health information. This is the WTIS-CCN software database, which is hosted onsite at the CCN provincial office. The WTIS-CCN database stores the personal health information of all patients who undergo select advanced cardiac procedures in Ontario. This information includes a list of data elements that the WTIS-CCN database contains, 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 very specific data points regarding the patient's condition and the procedure that prompted their personal health information being 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 WTIS-CCN database 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 prepare data 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 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 WTIS-CCN database following the procedures set out in the CCN policy, "Secure Retention of Personal Health Information".

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

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. "Statements of Purpose for Data Holdings Containing Personal Health Information" compels these statements of purpose to 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 wholly 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 CCN member hospitals that collect personal health information on behalf of CCN in accordance with "Statements of Purpose for Data Holdings Containing Personal Health Information".

During the course of his/her annual review of CCN's privacy and security program, the Privacy Officer shall review the statements of purpose for data holdings containing personal health information in accordance with "Statements of Purpose for Data Holdings Containing Personal Health Information". As required by "Statements of Purpose for Data Holdings Containing Personal Health Information", the Privacy Officer shall assess 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 shall amend the statement of purpose accordingly. 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, CCN's privacy and security policies, and relevant IPC guidelines.

As set out in "Statements of Purpose for Data Holdings Containing Personal Health Information", CCN's Privacy Officer shall consult with CCN's software development and clinical teams to assess the goals of the statements of purpose as they relate to CCN's identified purpose. As the Privacy Officer is wholly responsible for all statements of purpose for data holdings containing personal health information, the CEO having delegated that authority, 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 "Statements of Purpose for Data Holdings Containing Personal Health Information", new or recently amended statements of purpose are communicated to CCN member hospitals as soon as is reasonably possible.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's policy on statements of purpose for data holdings containing personal health information ("Statements of Purpose for Data Holdings Containing Personal Health Information") at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this 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 Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

"Statements of Purpose for Data Holdings Containing Personal Health Information" is audited on an annual basis as set out in the CCN policy "Policy and Procedures for Privacy and Security Auditing". In accordance with "Policy and Procedures for Privacy and Security Auditing", this audit is conducted by the Privacy Officer, who is also responsible for ensuring compliance with the policy and its procedures.

Statements of Purpose for Data Holdings Containing Personal Health Information

CCN maintains a statement of purpose for its one data holding, WTIS-CCN. This statement of purpose explains the purpose and goals of the data holding, justifies the data holding's existence as critical to CCN's function as a registry under Section 39(1)(c) of PHIPA, includes a description of the personal health information contained within the data holding, and lists the sources of the personal health information.

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

CCN has developed and implemented a policy ("Limiting Agent Access to and Use of Personal Health Information") that ensures that personal health information is only accessible to a

limited number of agents. This policy only permits agents to access and use personal health information on a "need to know" basis when access is required in the performance of their employment, contractual or other relationship with CCN. According to "Limiting Agent Access to and Use of Personal Health Information", the CCN Privacy Officer is responsible for determining which CCN agents are granted permission to access or use personal health information for purposes necessary to the fulfillment of their employment requirements, contractual obligations or other activities.

"Limiting Agent Access to and Use of Personal Health Information" sets out the procedures for the Privacy Officer's approval of agent access to and use of personal health information. Upon the commencement of an agent's relationship with CCN, the Privacy Officer 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, where patient data is entered by hospitals and where it resides for the purposes of reporting and analysis. "Limiting Agent Access to and Use of Personal Health Information" sets out the narrowly defined purposes for which access to and use of personal health information may be granted – namely, to aid health information custodians at CCN member 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. "Limiting Agent Access to and Use of Personal Health Information" compels agents with access to WTIS-CCN to only use personal health information if de-identified or aggregate personal health information will not serve the same purpose, and to use as little personal health information as possible when de-identified or aggregate personal health information will not serve the purpose.

The CCN database is unitary, meaning that it is not compartmentalized. Furthermore, the CCN agents who require access to and use of personal health information need complete access to the 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 WTIS-CCN have full rights to modify data as required for the correction of records. CCN will contact the IPC should any part of this policy change.

CCN agents who do not absolutely need personal health information for the fulfilment of their job description or other contractual duties are required by "Limiting Agent Access to and Use of Personal Health Information" must instead use de-identified health information, the preparation of which is governed by the CCN policy "Aggregation and De-identification of Record Level Data". "Limiting Agent Access to and Use of Personal Health Information" prohibits agents, who use de-identified and/or aggregate health information 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 and attempting to identify an individual based on prior knowledge.

Review and Approval 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”. This policy states that CCN’s Privacy Officer is responsible for determining which CCN agents are granted permission to access or use 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 WTIS-CCN; the decision is made by the Privacy Officer alone. The Privacy Officer grants the agent access to and/or use of personal health information only if it is absolutely necessary for the agent’s fulfilment of his/her contractual or other obligations. The only agents that are granted access to WTIS-CCN require that access in order to regularly correct errors in records and to assist agents at CCN member 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 to and use of personal health information is permitted by the Act and its regulation; the identified purpose for access to and use of personal health information cannot reasonably be accomplished without personal health information; de-identified and/or aggregate information 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 WTIS-CCN, CCN’s Privacy Officer is required by “Limiting Agent Access to and Use of Personal Health Information” to document the date that access is granted or denied, the reasons for which access is required, and the justification for access with regard to PHIPA and CCN policies. This documentation shall be 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 WTIS-CCN, 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

CCN's Privacy Officer is responsible for the imposition of conditions or restrictions on the approval of agent access to and/or use of personal health information. Currently, there is only one access level of WTIS-CCN, and CCN agents granted access to personal health information have full access rights to read, create, update and delete records of personal health information. All CCN agents sign Confidentiality and Non-Disclosure Agreements 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 and Non-Disclosure Agreement amounts to a breach of contract, and CCN may seek legal action against the agent(s) responsible.
Currently, all agents with access to WTIS-CCN require that access for the fulfilment of their job description. CCN does not provide any agent temporary access to WTIS-CCN. Should the job description of an agent with access to WTIS-CCN 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 the Privacy Officer is also the Director of Operations, it is not conceivable 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 notification when access to WTIS-CCN is no longer needed.

"Limiting Agent Access to and Use of Personal Health Information" prohibits agents with access to WTIS-CCN from accessing or using more personal health information than is absolutely necessary for the fulfilment of their job description. Only accesses or uses of personal health information that serves CCN's mandate as a prescribed person under PHIPA are allowed, and CCN is compelled by "Limiting Agent Access to and Use of Personal Health Information" to ensure that all accesses or uses of personal health information meet this criteria. Additionally, agents are prohibited from accessing or using personal health information if de-identified personal health information or other information 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 "Protection of Personal Health Information". Therefore, CCN has not found it necessary to develop procedures for the imposition of conditions or restrictions on any disclosure of personal health information.

CCN does not have processes to automatically terminate agents' abilities to access and use personal health information. This because, as set out in "Limiting Access to and Use of Personal

health Information", CCN agents are granted access to WTIS-CCN upon commencing employment if their job description requires them to regularly access and/or use personal health information. Instead, as set out in "Policy and Procedures for Privacy and Security Auditing", the Privacy Officer audits the log of agents with access to WTIS-CCN on a quarterly basis to ensure that the day-to-day duties all agents involve the use of the WTIS-CCN database. If an agent no longer requires access to WTIS-CCN, the Privacy Officer will then terminate the agent's access rights.

Notification and Termination of Access and Use

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 e-mail 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 (25, including all staff, managers, executives, and temporary contractors) and the fact that the Privacy Officer is also the Director of Operations, it is not conceivable that an agent could 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 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 "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 any device, including their work computers, excepting the secure servers within CCN's secure server room and their tape backups.

Secure Retention

The CCN policy "Secure Retention of Personal Health Information" includes provisions governing the secure retention of personal health information. "Secure Retention of Personal Health Information" states that personal health information may be stored only 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: E-mail, Internet, and Computing Devices". Currently, personal health information is being retained for as long as is reasonably necessary for long-term statistical analysis.

Secure Disposal

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. "Destruction of Personal Health Information") was developed by CCN's Privacy Officer in August 2008 and came into effect that same month. As set out in this policy, CCN 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 Approved Access to and Use of Personal Health Information

"Limiting Agent Access to and Use of Personal Health Information" compels 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 WTIS-CCN in a password-protected location on his/her 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 dates on which they were granted access and the dates on which access to WTIS-CCN was revoked or terminated if applicable, along with a brief reasoning for the revocation or termination.

Compliance, Audit and Enforcement

As with all CCN policies, agents are required by the policy "Execution of Confidentiality and Non-Disclosure Agreements" to sign agreements stating that they understand and will uphold CCN's policy on the use of personal health information at the outset of their relationship with

CCN and annually. The computers of all CCN agents who have been permitted to use personal health information, the computers of CCN agents whose permission to use personal health information has expired, and the computers of CCN agents who have not been permitted to use personal health information are audited for personal health information on a quarterly basis as set out in the policy "Policy and Procedures for Privacy and Security Auditing". Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report this, at the first reasonable opportunity, to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

"Policy and Procedures for Privacy and Security Auditing" also sets out that an additional quarterly audit of agents who have been granted access to WTIS-CCN must be conducted by the Privacy Officer. This audit requires the Privacy Officer to review these agents' work duties to ensure that it remains necessary for agents to have access to personal health information.

As set out in the policy "Maintenance and Review of System Control and Audit Logs", changes made to WTIS-CCN are tracked, logged, and audited by the Database and Application Development Supervisor to ensure the integrity of the application. The WTIS-CCN 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".

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

In accordance with the policy "Limiting Agent Access to and Use of Personal Health Information", CCN maintains a log of agents who have been granted approval to access and use WTIS-CCN. Information tracked includes the names of agents granted personal health information access, the dates on which they were granted access, the dates of the last and next audits, and the dates on which access was terminated, if applicable. This log is maintained by CCN's Software Application Manager under the direction of CCN's Privacy Officer.

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

Currently, CCN does not do any research internally. As such, CCN does not require a policy or procedures for the use of personal health information for research.

Where the Use of Personal Health Information is not Permitted for Research

The CCN policy "Limiting Agent Access to and Use of Personal Health Information" states that all CCN agents are prohibited from using personal health information and aggregate health information for research purposes.

Log of Approved Uses of Personal Health Information for Research

Currently, CCN does not do any research internally. As such, CCN does not require a policy or procedures for the maintenance of a log of approved uses of personal health information for research.

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

As part of CCN's zero-tolerance policy on the disclosure of personal health information, CCN summarily denies any requests for personal health information that do not fall under CCN's data sharing agreement with ICES. As such, CCN has deemed a written policy specifically on the disclosure of personal health information for purposes other than research to be unnecessary.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's zero-tolerance (apart from disclosure to ICES) policy on the disclosure of personal health information, which is set out in CCN's policy entitled "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information", at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer, at the first reasonable opportunity. If it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

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 unauthorized purposes.

Where the Disclosure of Personal Health Information is Permitted

CCN has a zero-tolerance policy on the disclosure of personal health information for any purpose other than those set out in CCN's data sharing agreement with ICES (which are the purposes set out in s.45 of PHIPA, such disclosures being permitted by s.13(5) of the Regulation under PHIPA). The disclosure of personal health information other than to ICES for purposes set out above is not permitted under any circumstances. As such, CCN has determined that a written policy on when the disclosure of personal health information for purposes other than research is permitted is unnecessary.

Review and Approval Process

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require a review and approval process for the disclosure of personal health information for purposes other than research. The rare requests for data containing personal health information are summarily denied without consideration.

Conditions or Restrictions on the Approval

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require procedures for placing conditions or restrictions on the approval of disclosure of personal health information for purposes other than research.

Secure Transfer

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require procedures for secure transfer of personal health information for purposes other than research.

Secure Return or Disposal

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require procedures for secure return or disposal of personal health information after it has been disclosed to a third party for purposes other than research.

Documentation Related to Approved Disclosures of Personal Health Information

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require procedures for documenting disclosures of personal health information for purposes other than research.

Where the Disclosure of Personal Health Information is not Permitted

As set out in "Protection of Personal Health Information", in no circumstances does CCN permit the disclosure of personal health information for purposes other than research, except to ICES. In addition, "Protection of Personal Health Information" states that CCN does not permit the disclosure of aggregate and/or de-identified health information for purposes other than research, except where aggregate information on elective coronary artery bypass surgeries is provided to the MOHLTC on a monthly basis as per their request.

Review and Approval Process

As set out in "Protection of Personal Health Information", CCN does not disclose aggregate or de-identified personal health information to any individual or organization for purposes other than research. As such, it does not require a process for review and approval of those requests.

Conditions or Restrictions on the Approval

As set out in "Protection of Personal Health Information", CCN does not disclose aggregate or de-identified personal health information to any individual or organization for purposes other than research. As such, it does not require a process for placing conditions or restrictions on the approval of requests for personal health information for purposes other than research.

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

CCN has a zero-tolerance policy of disclosing personal health information in any circumstances except those listed in CCN's data sharing agreement with ICES. The rare requests for personal health information for the purposes of research are summarily denied without consideration.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's zero-tolerance policy on the disclosure of personal health information for research purposes at the outset of their relationship with CCN and annually after that. Should an agent discover or suspect a breach of this policy ("Notice/Consent for Collecting, Using, or Disclosing Personal Health Information"), CCN's policy on privacy and security breaches imposes a duty on them to report the breach to CCN's Privacy Officer. If it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

As stated in CCN's policy on the auditing of privacy practices and policies, CCN undertakes regular auditing of agents' computers to ensure that personal health information is not disclosed for any purpose other than those set out in CCN's data sharing agreement with ICES.

Where the Disclosure of Personal Health Information is Permitted for Research

CCN has a zero-tolerance policy on the disclosure of personal health information for any purpose other than those set out in CCN's data sharing agreement with ICES. The disclosure of personal health information for research purposes is not permitted under any circumstances. As such, it has determined that a written policy on when the disclosure of personal health information for research purposes is permitted is unnecessary.

Review and Approval Process

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require a review and approval process for the disclosure of personal health information for research purposes. The rare requests for data containing personal health information are summarily denied without consideration.

Conditions or Restrictions on the Approval

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require procedures for placing conditions or restrictions on the approval of disclosure of personal health information for research purposes.

Secure Transfer

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require procedures for secure transfer of personal health information for research purposes.

Secure Return or Disposal

Due to CCN's zero-tolerance policy on the disclosure of personal health information, 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.

Documentation Related to Approved Disclosures of Personal Health Information

Due to CCN's zero-tolerance policy on the disclosure of personal health information, CCN does not require procedures for documenting disclosures of personal health information for research purposes.

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

In 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 aggregate and/or de-identified information 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 aggregate and/or de-identified personal health information. As set out in "Disclosure of Aggregate and/or De-identified Health Information to Researchers", requests for aggregate or de-identified health information are reviewed by the Research and Publications Committee, a body composed of medical researchers and hospital administrators who ensure that any data provided by CCN to researchers will be used in a secure and ethical manner.

"Disclosure of Aggregate and/or De-identified Health Information to Researchers" states that researchers who request de-identified or aggregate data must be affiliated with an established and respected 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, the policy sets out that 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 or aggregate data from CCN. 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.

As set out in the policy "Disclosure of Aggregate and/or De-identified Health Information to Researchers", researchers interested in a topic requiring de-identified or aggregate health information 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. After a research plan has been formulated, researchers must complete and submit to the Research Publications Committee the standardized "Data Request Form". This form can be made available to the IPC upon request. Both the "Letter of Intent to Conduct a Study for Publication" and the "Data Request Form" require the researcher to identify what data elements are necessary for their study and to summarize their research plan. The "Data Request Form" requires researchers to attach the certificate of approval from a research ethics board. As set out in "Disclosure of Aggregate and/or De-identified Health Information to Researchers", the researcher must prove to the Research Publications Committee that their research proposal has scientific value and does not compromise any CCN privacy policy, practice, or procedure. If the Research 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 “Aggregation and De-Identification of Record Level Data”, before the de-identified personal health information is disclosed to the researcher the Privacy Officer or a designate must review it to ensure that the data cannot be used to identify any individuals.

“Disclosure of Aggregate and/or De-identified Health Information to Researchers” requires CCN’s Director of Clinical Quality and performance 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 the Approval

If the researcher is granted access to de-identified 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 and Non-Disclosure Agreement stating that they will preserve the confidentiality of the data and prevent their disclosure. Additionally, the policy prohibits the researcher from using the de-identified or aggregate information, 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 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”, CCN’s Director of Clinical Quality and Performance keeps a log of official log of requests, approvals, and denials of access to de-identified and aggregate personal health information. Of all nine requests that CCN has ever received for de-identified and aggregate information, all but one, which is currently under review, has been approved.

Template Research Agreement

Because CCN does not disclose personal health information in any circumstances except those stated in CCN's data sharing agreement with ICES, it does not require a template research agreement. As such, this section is not applicable to CCN.

Log of Research Agreements

Because CCN does not disclose personal health information in any circumstances except those stated in CCN's data sharing agreement with ICES, it does not execute research agreements and thus has no need for a log of research agreements. As such, this section is not applicable to CCN.

Policy and Procedures for the Execution of Data Sharing Agreements

CCN has only one data sharing agreement in place. This agreement was made with ICES. It is unlikely that a further data sharing agreement will be made with another organization, and even less likely that such an agreement would be made for purposes other than research. As such, CCN has not developed a policy on the execution of data sharing agreements for purposes other than research. Should this change in the future, CCN will develop a new policy that includes all of the requirements set out in the *Manual* and further, will notify the IPC.

Template Data Sharing Agreement

CCN has only one data sharing agreement in place and it is with ICES. This agreement has been reviewed by IPC and includes all of the provisions set out in this section of the *Manual*. Because further data sharing agreements are unlikely in the foreseeable future, CCN has determined that having a template for data sharing agreements is unnecessary.

Log of Data Sharing Agreements

CCN has only executed one data sharing agreement, with ICES. The execution of this data sharing agreement was highly exceptional, and as such, CCN has not found it necessary to maintain a log of data sharing agreements.

Should CCN's relationship with ICES change, or should CCN seek a new data sharing agreement with another organization, CCN will provide all information to the IPC.

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 and use of the personal health information in CCN's custody. The template agreement for this purpose has been developed by CCN's Privacy Officer and contains all relevant information from the template provided by the IPC.

"Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" sets out that CCN's Privacy Officer is responsible for ensuring that agreements are executed with third party service providers prior to their access to and use of personal health information.

"Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" states that prior to the execution of agreements with third party service providers allowing the third party access to and/or use of personal health information, CCN's Privacy Officer must ensure that:

- The service provided by the third party in respect of personal health information is absolutely necessary for the persistence of CCN's mandate under PHIPA;
- 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 their needing access to and/or use of personal health information;
- The service provided by the third party cannot be conducted without identifiable personal health information (i.e. the service cannot be conducted using de-identified/aggregate personal health information);
- And that CCN will not provide to the third party any more personal health information than is absolutely necessary for the provision of that crucial 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.

"Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" sets out that 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 "Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" 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. "Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" states that CCN may seek legal action against the third party at this point.

"Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" sets out that 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.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's policy on the execution of agreements with third party service providers in respect of personal health information at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty

on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which sets out that CCN's Privacy Officer is responsible for auditing the policy on a quarterly basis.

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 is required by "Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect to Personal health Information" to set out the following:

General Provisions

- A description of the status of CCN under PHIPA
- CCN's duties and responsibilities under PHIPA
- 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 found in Section 4 of PHIPA
- 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. Additionally, the third party must 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
- A justification under PHIPA 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, the agreement states 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, such as aggregate/de-identified health 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 zero-tolerance policy on the disclosure of personal health information, "Notice/Consent for Collecting, Using, or Disclosing Personal Health Information", prohibits the disclosure of personal health information to any individual or any organization for any purpose (excepting disclosure of personal health information to ICES pursuant to a data sharing agreement). As such, CCN's template agreement for third party service providers in respect to personal health information has no provisions

regarding the disclosure of personal health information except to prohibit it 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. The agreement will also set out how the manner of transfer has regard to the CCN policy "Secure Transfer of Personal Health Information"
- A list of the conditions under which personal health information is permitted to be transferred by the third party
- Indications of to whom personal health information is permitted to be transferred by the third party
- A stipulation that third parties whose primary service is the retention or disposal of personal health information away from the CCN premises 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 pursuant to the agreement

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 manners, 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. The agreement will also set out how the manner of retention has regard to the CCN policy "Secure Retention of Personal Health Information"
- A stipulation that third parties whose primary service is the retention of personal health information away from the CCN premises must maintain an inventory of the records of personal health information being retained pursuant to the agreement and set out a method of tracking the records being maintained

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
- 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". This policy was created in accordance with relevant privacy legislation, 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", and PHIPA and its regulation.
- 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 at its discretion

Implementation of Safeguards

- A stipulation that the third party must take reasonable steps to protect the personal health information accessed or 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 the records of personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the personal health information
- 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 other parties, the agreement must stipulate that the third party will notify CCN in advance and that the subcontract will be consistent with its obligations to CCN under the agreement

Notification

- A stipulation that the third party must notify CCN's Privacy Officer, in written format, 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 as to whether or not CCN will be monitoring the third party`s compliance with the agreement, and if yes, the manner in which compliance will be audited and the notification, if any, of auditing that will be provided to the third party

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 records of personal health information must be returned or disposed of or access terminated.

"Policy and Procedures for the Execution of Agreements with Third Party Service Providers in Respect of Personal Health Information" sets out that the Privacy Officer must retain this log in a password-protected location on his/her local drive or on the shared company drive.

Policy and Procedures for the Linkage of Records 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. Because it is not reasonably foreseeable that CCN would ever approve a linkage of personal health information records, CCN has determined that a written policy on linkages of personal health information records would be unnecessary.

Log of Approved Linkages of Records of Personal Health Information

Because it is not foreseeable that CCN would ever allow the linkage of records of personal health information, CCN has determined that developing a log of approved linkages of records of personal health information would be unnecessary.

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. "Aggregation and De-identification of Record Level Data" 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 compliant with those set out in the *Manual*.

“Aggregation and De-identification of Record Level Data” 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 aggregate or de-identified personal health information will serve the same purpose. Researchers are required by “Aggregation and De-identification of Record Level Data” to execute Non-Disclosure Agreements compelling them to protect the information to which they have been granted access. A breach of any of the procedures of “Aggregation and De-identification of Record Level Data” constitutes a breach of contract, and CCN may take legal action against any researcher who does this.

In de-identifying data, “Aggregation and De-identification of Record Level Data” dictates that fields that can be used to identify a person are collapsed and aggregated or removed from data. 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, “De-identification of Record Level Data” states that CCN will de-identify the record-level data, eliminating all but the minimum level of demographic or geographic detail required for the study.

"De-identification of Record Level Data" states that de-identified 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.

"De-identification of Record Level Data" sets out that CCN agents are prohibited from using aggregate or de-identified personal health information 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. The policy also identifies the mechanisms used to ensure this.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's "Aggregation and De-identification of Record Level Data" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

As set out in "Policy and Procedures for Privacy and Security Auditing", CCN's Privacy Officer is required to audit for compliance with "Aggregation and De-Identification of Record Level Data" on a quarterly basis.

Privacy Impact Assessment Policy and Procedures

Given the limited scope of CCN's current operations, CCN has determined that the ordering of frequent, regular privacy impact assessments would be unnecessary. As such, CCN has not developed a written policy on the ordering of privacy impact assessments. CCN orders privacy impact assessments when circumstances dictate, such as a major change in its privacy and security program, upon recommendation from the IPC, upon the reception of a valid privacy complaint, or upon a breach as defined in "Policy and Procedures for Privacy and Information Security Breach Management". CCN last ordered a privacy impact assessment in 2009. This assessment was reviewed by the IPC, who provided comments. All recommendations made in the privacy impact assessment and by the IPC were adopted.

Should CCN determine in the future that another privacy impact assessment is necessary, CCN's Privacy Officer will prepare a policy and associated procedures for issues relating to privacy impact assessments that is compliant with the expectations set out in pages 62-64 of the *Manual*.

Log of Privacy Impact Assessments

CCN rarely orders privacy impact assessments to be conducted. As such, it has determined that the maintenance of a log of privacy impact assessments would be unnecessary. The recommendations made in the last privacy impact assessment, conducted in 2009, are included in CCN's consolidated log of recommendations. The recommendations made in any future privacy impact assessments will also be included in that consolidated log of recommendations.

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. Additionally, "Policy and Procedures for Privacy and Security Auditing" sets out that the Privacy Officer is responsible for the development and implementation of an auditing schedule.

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 at least one day in advance of the scheduled audit in written format by the Privacy Officer. "Policies and Procedures for Privacy and Security Auditing" states that agents will be notified of the process of the audit.

For each type of privacy audit, "Policy and Procedures for Privacy and Security Auditing" sets out the process to be followed in conducting the audit. Also included is a discussion on 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 referred to in "Policy and Procedures for Privacy and Security Auditing" is a template form that, according to the policy, collects the following information at 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

As set out in "Policy and Procedures for Privacy and Security Auditing", the Privacy Officer along with their designate, the Supervisor of Database/Application Development, will have authority to manage the privacy and security program. The Privacy Officer will be 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 shall also identify the nature of documentation that will be completed, provided and/or executed at the conclusion of each privacy audit.

"Policy and Procedures for Privacy and Security Auditing" states that 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 that do not identify any deficiencies in CCN's privacy and security program are communicated to CCN agents within one week of the conclusion of the privacy or security audit.

"Policy and Procedures for Privacy and Security Auditing" sets out that a log of all privacy and security audits must be maintained on the main CCN company drive by the Privacy Officer. The Privacy Officer along with their designate, the Supervisor of Database/Application Development, 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 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 in itself non-compliance with CCN policy, and may result in disciplinary action.

Log of Privacy Audits

As set out in "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 requires the following fields to be completed:

- 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

"Policy and Procedures for Privacy and Security Auditing" sets out that this log must be completed by the Privacy Officer and retained by the Privacy Officer on CCN's shared drive.

Policy and Procedures for Privacy Breach and Information Security Breach Management

In response to a recommendation made by the IPC during its prior review of CCN in 2008, CCN has 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 new 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.

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

- Personal health information is lost, stolen or disclosed to those unauthorized.
- Personal health information is used for purposes other than specified in CCN's mandate as a Registry
- The collection, use and disclosure of personal health information is not in compliance with PHIPA or its regulations
- 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 retained by CCN
- Personal health information is stolen, lost or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification or disposal.

Additionally, 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, CCN agents must immediately notify the Privacy Officer in oral or written format as set out in “Information Security and Privacy Breach Management”. 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 indeed been compromised, they are required by “Information Security and Privacy Breach Management” to notify the CEO immediately.

The Privacy Officer is responsible ensuring that the proper steps are taken, given the particular circumstances of the breach, to contain the breach, 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 and date of the disposal.

The Privacy Officer must also take or recommend any remedial action required, provide notice where appropriate to the member 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 also responsible for consulting with privacy and information security authorities at affected hospitals to ascertain risk and determine what action may be necessary. The Privacy Officer or a designate of 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, if any, 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.

CCN's Privacy Officer has developed a template for reporting the details of the breach to the CEO. This report is provided to the CEO for review prior to attaining resolution. This template requires the Privacy Officer to fill out the following fields:

- 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 "Information Security and Privacy Breach Management", the Privacy Officer's investigation may include interviews with CCN agents or other individuals associated with the breach. Recommendations made in these reports are compiled with other recommendations in CCN's consolidated log of recommendations. The consolidated log of recommendation is maintained by CCN's Privacy Officer. 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, investigation 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.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's policy on privacy and information security breaches ("Information Security and Privacy Breach Management") at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, "Information Security and Privacy Breach Management" imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

Log of Privacy Breaches

As set out in "Information Security and Privacy Breach Management", 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 the prescribed person 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.

Policy and Procedures for Privacy Complaints and Privacy Inquiries

In response to a recommendation made by the IPC during its prior review of CCN in 2008, CCN has revised its policy on receiving, documenting, tracking, investigating, remediating and responding to privacy inquiries and complaints made by individuals. The new 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.

"Privacy Inquiries and Complaints" states that "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 further sets out that "Inquiries" are defined 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".

"Privacy Inquiries and Complaints" sets out that CCN receives and will respond to complaints, inquiries, and comments made by any individual. This policy, which is publicly available on CCN's website, clearly states that these communications should be directed to CCN's Privacy Officer, and provides contact information for both CCN's provincial office and the office of the IPC. "Privacy Inquiries and Complaints" states that the contact information of CCN, CCN's Privacy Officer, and the IPC must be made available. This contact information includes mailing addresses, e-mail addresses, and telephone numbers for CCN's Privacy Officer and for the IPC. Contact information for CCN's Privacy Officer is also included in brochures given to member hospitals.

"Privacy Inquiries and Complaints" 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. "Privacy Inquiries and Complaints" lists the documentation must be completed, provided, and/or executed by the individual making the complaint or inquiry, the content required, and the nature of the information that will be requested from the individual making the complaint or inquiry.

If the communication alleges a breach of CCN's privacy and security policies, procedures and practices, the Privacy Officer must determine whether or not the complaint does in fact refer to a breach of the privacy and security policies, procedures, and practices. The policy sets out the processes for which and the time frame within which the Privacy Officer must make his/her 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. If the Privacy Officer determines that there has in fact been a breach, he/she will investigate the complaint.

If it is determined that an investigation will be undertaken into a privacy complaint, "Privacy Inquiries and Complaints" sets out that 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, indicating whether or not the individual will be contacted for further information concerning the privacy complaint, 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 policy requires that an individual who has made a privacy complaint be notified in writing of the nature and findings of the investigation and of the measures taken, if any, in response to the complaint. It also set out that the individual shall be advised that he or she may make a complaint to the IPC, if there are reasonable grounds to believe that PHIPA or its regulation has been or is about to be contravened and that contact information for the IPC must be provided.

"Privacy Inquiries and Complaints" sets out that all inquiries and complaints will be responded to, in writing, even if it is determined that the inquiry or complaint is without validity and the Privacy Officer does not initiate an investigation 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, if there are reasonable grounds to believe that CCN has contravened or is about to contravene PHIPA or its regulation; and providing contact information for the IPC.

"Privacy Inquiries and Complaints" requires that the Privacy Officer maintain a log of privacy inquiries and complaints. The policy states that the log must indicate 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.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's policy on privacy complaints at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this 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. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

Log of Privacy Complaints

CCN is required by the policy "Privacy Inquiries and Complaints" to maintain a log of privacy complaints. The Privacy Officer is responsible for maintaining and updating the log when complaints are made. The log of privacy complaints collects 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.

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

Information Security Policy

The policy "Protection of Personal Health Information" 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 the security program. Accordingly, CCN has developed and implemented a comprehensive information security program that ensures that the personal health information under its custody is protected against theft, loss and unauthorized use or disclosure and that the records of personal health information are protected against unauthorized copying, modification or disposal. This policy establishes and documents a methodology for identifying, assessing and remediating threats and risks and for prioritizing all threats and risks identified for remedial action. This program is directed by CCN's 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. CCN's 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 one data holding 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 should he/she determine that changes to the software or operating environment used by CCN are necessary for the protection of the 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 eliminate vulnerabilities and increase overall security. The last such assessment was conducted in 2008 by Cygnos IT Security. The results of this assessment were reviewed by the IPC and all recommendations were adopted.

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;
- Self-updating anti-virus 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.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's security policies at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management"") imposes a duty on them to report the breach or suspected breach, at the first reasonable opportunity, to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach

of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

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.

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 are needed or whether new security policies, procedures and practices are required.

CCN's policy on the review of its security policies has been combined with its policy on review of its privacy policies. "Annual Review of Privacy and Security Policies and Procedures" compels the CCN 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). In the event that the law is changed or the IPC issues new orders, guidelines, factsheets, or best practices, CCN's 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. In accordance with "Annual Review of Privacy and Security Policies and Procedures", the Privacy officer has the last word in the development and implementation of new and amended policies, the CEO having delegated that authority.

At the last review of the security policies, procedures and practices on January 10, 2011, the Privacy Officer did not make any changes as it was apparent that the policies, procedures and practices were in compliance with the IPC requirements and with the requirements of CCN.

As required in the policy, “Annual Review of Privacy and Security Policies and Procedures”, CCN’s Privacy Officer is also responsible for the communication of new or amended policies to the public and to CCN agents. “Annual Review of Privacy and Security Policies and Procedures” sets out that new and amended policies will be communicated to CCN 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 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. As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold “Annual Review of Privacy and Security Policies and Procedures” at the outset of their relationship with CCN and annually. The Privacy Officer is responsible for determining the consequences of a breach, which may include disciplinary action up to termination of employment as set out in CCN Policy.

CCN audits “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”. “Policy and Procedures for Privacy and Security Auditing” sets out that the Privacy Officer is responsible for auditing “Annual Review of Privacy and Security Policies and Procedures” to ensure compliance with the policy and its procedures on a quarterly basis.

Policy and Procedures for Ensuring Physical Security of Personal Health Information

CCN has developed a policy (“Physical Security”) addressing the physical safeguards against loss and unauthorized use or disclosure and to protect records of personal health information against 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;

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN’s policy on physical security (“Physical Security”) at the outset of their

relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Physical Security" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which sets out that the Privacy Officer is responsible for auditing "Physical Security" on a quarterly basis.

Policy, Procedures and Practices with Respect to Access by Agents

As set out in the policy "Physical Security", CCN's 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 records of personal health information are stored. Access is granted to CCN 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 have access to the server room to perform maintenance. This privilege is given to these CCN agents conditional on a continued need in order to fulfil the agent's job description or contractual duties. As set out in 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 justification, must be provided by the Privacy Officer in the log of agents with access to the provincial office.

"Physical Security" sets out that the Privacy Officer is responsible for providing access cards to CCN agents and for providing an indication of this in the log of agents with access to the provincial office.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "Physical Security" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

As set out in "Physical Security", CCN's Privacy Officer is responsible for maintaining a log of agents granted access to the premises and to the secure server room. This log collects 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 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 a CCN policy named "Physical Security". This policy sets out that keys and access cards provided to CCN 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 to the agent a new card at his/her own expense. 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 access 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 shall be retained in a repository by the Privacy Officer.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "Physical Security" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

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) from individuals whose employment has been terminated. Because of the limited number of people employed by CCN (currently 25 people including management, executive, and temporary contractors) and the fact that the Privacy Officer is also the Director of Operations, it is not conceivable that an agent could end their employment without the knowledge of the Privacy Officer. As such, CCN does not require individuals whose employment has been terminated to provide notification. 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 a CCN agent with access to the server room would see their job description or contractual obligations change so 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 502.

Tracking and Retention of Documentation Related to Access to the Premises

CCN's Privacy Officer is required by "Physical Security" to maintain a log of agents granted access to the CCN provincial office and to the secure server room that houses records of 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; 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. Building security provides written reports as needed or when 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.

Visitors to the CCN office must sign in at the front office. CCN's receptionist is required 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)

Additionally, CCN's receptionist is required by "Physical Security" to notify the Privacy Officer upon reception of a visitor.

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. 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.

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

As stated above, CCN's Privacy Officer is required by "Physical Security" to maintain a log of agents granted access to the CCN provincial office and to the secure server room that houses records of 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 to the prescribed person , if applicable.

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

For the secure retention of personal health information, CCN follows its policy "Secure Retention of Personal Health Information". This policy 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 discouraged from

retaining personal health information on paper and are only permitted to do so for minimal time periods. When CCN agents have personal health information on paper they are expected to transfer to electronic document format when the project is completed and store it on CCN's secure network until no longer required. During the period that CCN agents have personal health information on paper it must kept in a locked drawer and only accessible by the agent conducting the project work. Furthermore, CCN is only accessible by security pass which ensures another layer of protection. 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. According to "Secure Retention of Personal Health Information", CCN's Privacy Officer is the CCN agent responsible for ensuring that all CCN agents follow this policy and all personal health information in CCN's custody is retained in a secure manner.

"Secure Retention of Personal Health Information" states that personal health information may be retained only as long as is reasonably necessary. The policy states that personal health information in CCN's custody is currently being retained for as long as is reasonably necessary for long-term statistical analysis.

CCN does not use or disclose personal health information for research purposes, and as such it does not require procedures relevant to that purpose.

"Secure Retention of Personal Health Information" sets out that records of health information that are subject to data sharing pursuant to a data sharing agreement are to be retained according to the provisions in that agreement. The policy further states that it is forbidden for either party of a data sharing agreement to retain personal health information for any period longer than what is set out in the data sharing 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 records of personal health information are 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;
- 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 member 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.

"Secure Retention of Personal Health information" sets out that records of personal health information will be transferred to a third party service provider for long-term tape backup. According to the policy, 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 Supervisor of Database/Application Development. The backups must be provided to the representative in a locked metal box. The same locked metal box will be provided back to the Supervisor of Database/Application development upon request. These procedures are compliant with the CCN policy "Secure Transfer of Personal Health Information".

The Supervisor of Database/Application Development is required by "Secure Retention of Personal Health Information" 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 the records of personal health information.

CCN's Supervisor of Database/Application Development is required by "Secure Retention of Personal Health Information" to maintain a detailed inventory of the records of personal health information being transferred to the third party service provider and received from the third party service provider.

"Secure Retention of Personal Health Information" sets out that records of personal health information may only be transferred to a third party service provider if it has executed with CCN a contract modelled on the Template Agreement for All Third Party Service Providers that

was developed by the IPC. The policy states that CCN's Privacy Officer is responsible for ensuring that such a contract is executed prior to transferring the records of personal health information for secure retention.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's policy on the secure retention of personal health information at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Secure Retention of Personal Health Information" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which sets out that CCN's Privacy Officer is responsible for auditing the policy on a quarterly basis.

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

Mobile devices are defined in CCN's information technology policy ("IT Policy: E-mail, Internet, and Computing Devices") as electronic devices including laptops, personal digital assistants (PDAs), tablets, smart phones, mobile phones, Blackberry devices, and any portable storage device that could be used to digitally/electronically copy, transcribe or store files. The policy expressly forbids the retention of personal health information on mobile devices. Personal health information can only be stored electronically on CCN's secure network.

Additionally, "IT Policy: E-mail, Internet, and Computing Devices" prohibits agents who are working remotely from accessing personal health information.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "IT Policy: E-mail, Internet, and Computing Devices" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach

Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Policy: E-mail, Internet, and Computing Devices" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which states that the Privacy Officer is responsible for auditing for compliance with the policy on a quarterly basis.

Policy and Procedures for the Secure Transfer of Records 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 records of personal health information via secure file transfer protocol (SFTP) with VeriSign SSL digital certificates and at least 128-bit encryption. These transmissions are primarily made to CCN by Cancer Care Ontario, who in turn receives personal health information from health information custodians at CCN member 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's IT staff are required by "Secure Transfer of Personal Health Information" 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 under a separate cover.

"Secure Transfer of Personal Health Information" 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 "Secure Transfer of Personal Health Information" 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.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "Secure Transfer of Personal Health Information" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Secure Transfer of Personal Health Information" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which states that the Privacy Officer is responsible for auditing for compliance with this policy on a quarterly basis.

Policy and Procedures for Secure Disposal of Records of Personal Health Information

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

"Destruction of Personal Health Information" lists the means by which records of personal health information may be disposed of. 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 WTIS-CCN database 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 "Secure Retention of Personal Health Information" is contravened. It is highly uncommon for personal health information on any medium other than the secure servers or their tape backups to be disposed of.

For records of personal health information on paper:

- CCN 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 shall review the agent's actions to determine whether or not a breach has occurred according to the procedures set out in "Information security and Privacy breach Management".
- CCN's Privacy Officer is responsible for maintaining a repository of these forms.
- CCN's 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.
- CCN's 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.
- CCN's Privacy Officer is responsible for ensuring that transfers of paper, which may include records of personal health information, are made in a secure manner.
- CCN's Privacy Officer must document the mode, time, and date of the transfer of paper records to be shredded by Shred-It

For records of 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 records of 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 records of 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.

"Destruction of Personal Health Information" 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 "Review of Privacy and Security Policies and Procedures", CCN's Privacy Officer reviews "Destruction of Personal Health Information" 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 "Secure Retention of Personal Health Information", which dictates that all records of personal health information must be stored on CCN's secure network or its tape backups, which are handled by Recall. Additional procedures in "Destruction of Personal Health Information" 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 "Destruction of Personal Health Information" were developed for instances in which the provisions in "Secure Retention of Personal Health Information" are not followed. That CCN has procedures for the disposal of records 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.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "Destruction of Personal Health Information" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits “Destruction of Personal Health Information” in accordance with its privacy and security audit policy (“Policy and Procedures for Privacy and Security Auditing”), which sets out that CCN’s Privacy Officer, is responsible for auditing the police for compliance on a quarterly basis

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. “Password Policy” compels CCN agents to not share their passwords with anyone and to take reasonable steps to protect it 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 a period of 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.

“Password Policy” sets out that 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 Policy also provides for the imposition of the mandatory system-wide password-protected screen saver, after 10 minutes of inactivity.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold “Password Policy” at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN’s policy on privacy and security breaches (“Information Security and Privacy Breach Management”) imposes a duty on them to report the breach or suspected breach to CCN’s Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Password Policy" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which sets out that CCN's Privacy Officer is responsible for auditing the policy on a quarterly basis.

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.

"Maintenance and Review of System Control and Audit Logs" 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 CCN member 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 WTIS-CCN application is hosted by Cancer Care Ontario, whose staff log the username, time of login, and changes made to the WTIS-CCN database. Neither software logs geographic information because of the limited number (eighteen member hospitals and the provincial office) of sites from which CCN network can be accessed through the firewall.

On a daily basis, CCN's Supervisor of Database/Application Development is required by the policy "Maintenance and Review of System Control and Audit Logs" to audit the following:

- WTIS-CCN data transfer logs
    - Verify if database replicated by Cancer Care Ontario is successfully received and resides at CCN
    - Examine FTP event log and verify FTP server has receive capabilities
    - Verify FTP queue.

- WTIS-CCN database replication logs
    - WTIS-CCN database restore process logs. Check the number of tables/records between replicated and restored database
    - Verify database is mounted properly
- Server operating system log and performance
    - Examine available MBs performance counter, processor time counter, committed bytes in use performance counter, disk usage, and performance log
    - Monitor filtering application
    - Monitor system logs on Windows Servers to see repetitive warning and error logs
    - Discover failures and problems
- Backup logs
    - Ensure that daily backup is completed
    - Verify that the previous backup operation is completed
    - Analyze and respond to errors and warnings during the backup operation.
    - Follow the established procedure for tape rotation, labelling, and storage (done through Recall)

On a weekly basis, CCN's Supervisor of Database/Application Development is required by the policy "Maintenance and Review of System Control and Audit Logs" to audit the following:

- CCN network antivirus threat report and update logs

On a monthly basis, CCN's Supervisor of Database/Application Development is required by the policy "Maintenance and Review of System Control and Audit Logs" to audit 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 Supervisor of Database/Application Development. To achieve this, "Maintenance and Review of System Control and Audit Logs" states that 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 Supervisor of Database/Application Development. These logs are required by the policy to be retained for at least one year by the Supervisor of Database/Application Development.

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 by "Maintenance and Review of System Control and Audit Logs" 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 required to be made accessible to the Privacy Officer, who must be notified as soon as is reasonably possible, in written or oral format, by the Supervisor of Database/Application Development in the event that the problem is not easily resolvable or unauthorized access is suspected.

"Maintenance and Review of System Control and Audit Logs" states that CCN's Privacy Officer is responsible for ensuring that these audits are in fact conducted by the Supervisor of Database/Application Development.

If the Supervisor of Database/Application Development 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. "Maintenance of System Control and Audit Logs" 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 time-lines in the course of a formal privacy and security audit or review.

If in the course of completing these audits the Supervisor of Database/Application Development 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.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "Maintenance and Review of System Control and Audit Logs" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Maintenance of System Control and Audit Logs" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which sets out that CCN's Privacy Officer is responsible with auditing for compliance with this policy on a quarterly basis.

Policy and Procedures for Patch Management

While CCN's Privacy Officer is ultimately responsible for the management of patch updates to CCN's internal network, CCN has executed an agreement with Interface Technologies, a third party information technology services provider, for this purpose. Interface Technologies assesses the need for new patches and applies them if they provide meaningful security, performance, or feature enhancements without negatively affecting the function or performance of CCN software.

Policy and Procedures Related to Change Management

CCN does not require a policy on the management of changes to its operating environment. If changes to CCN's operating environment are to be made, the Privacy Officer, in consultation with CCN's IT team, is responsible for determining when changes are made. CCN has hardware unconnected from 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.

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

CCN has developed a policy ("Back-Up and Recovery of Personal Health Information") to ensure that its systems are backed up and recoverable 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 "Back-Up and Recovery of Personal Health Information", CCN is required to use the Acronis Backup & Recovery 10 Advanced Server system, which automatically, in real time, 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 Acronis system could restore all lost data.

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 "Back-Up and Recovery of Personal Health Information" 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 in fact 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 to be retained in a filing cabinet by CCN's Data Manager. This method of transfer is compliant with "Secure Transfer of Personal Health Information". 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 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 first 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.

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. "Back-Up and Recovery of Personal Health Information" requires the Supervisor of Database/Application Development to test the Acronis Backup & Recovery 10 Advanced Server system on a weekly basis and provide written notification to the Privacy Officer in the event that errors are identified.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "Back-Up and Recovery of Personal Health Information" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Back-Up and Recovery of Personal Health Information" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which sets out that CCN's Privacy Officer is responsible with auditing for compliance with this policy on a quarterly basis.

Policy and Procedures on the Acceptable Use of Technology

CCN has developed a policy ("IT Policy: E-mail, Internet, and Computing Devices") governing the use of CCN-supplied technology by CCN 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, "IT Policy: E-mail, Internet, and Computing Devices" 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.
- 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.

“IT Policy: E-mail, Internet, and Computing Devices” also governs e-mail use by CCN 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 e-mail, 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 e-mail chain, agents are to review all of the e-mails in the chain to make sure that they are needed by the current recipient.
- In all cases, agents must confirm that the recipient's e-mail 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 you an e-mail 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 e-mail account. Likewise, agents are to never send CCN confidential information to a non-CCN e-mail account belonging to another party so that agents may then access the information or have it forwarded.
- Agents must use appropriate language in your e-mail messages and adhere to CCN values and policies. Agents are to use the same rules and the same polite forms of address that you would use in other types of business communication.
- Agents are to never reply to e-mails that they believe to be spam.

- Agents are to use discretion when opening attachments to e-mail 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 e-mail addresses are not to be added to mailing lists unless required as part of your assigned job duties. Doing so may lead to CCN e-mail systems receiving excessive unwanted mass e-mail (spam.)
- Another user's e-mail 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 e-mail account if access is absolutely necessary for ensuring the persistence of CCN's critical functions.
- CCN e-mail 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 e-mail using CCN e-mail systems are the property of CCN. CCN reserves the right to monitor and disclose all messages sent over its e-mail system for any purpose.
- Incidental personal use of e-mail is occasionally permitted but it must never interfere with job responsibilities and work-related needs.

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold "IT Policy: E-mail, Internet, and Computing Devices" at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "IT Policy: E-mail, Internet, and Computing Devices" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which sets out that the Privacy Officer is responsible for auditing for compliance with the policy on a quarterly basis.

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. Additionally, "Policy and Procedures for Privacy and Security Auditing" sets out that the Privacy Officer is responsible for the development and implementation of an auditing schedule.

"Policy and Procedures for Privacy and Security Auditing" sets out that the 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 limited scope 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. 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, upon the reception of a valid privacy complaint, or upon a breach as defined in "Policy and Procedures for Privacy and Information Security Breach Management". CCN last ordered a threat and risk assessment in 2008. This assessment was reviewed by the IPC, who provided comments. All recommendations made in threat and risk assessment and by the IPC were adopted.

Should CCN determine in the future that another threat and risk assessment or other type of specialized security auditing is 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 at least one day in advance of the scheduled audit in written format by the Privacy Officer. "Policies and Procedures for Privacy and Security Auditing" states that agents will be notified 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. Privacy Officer is responsible for completing providing and/or executing the documentation. The documentation referred to in “Policy and Procedures for Privacy and Security Auditing” is a template form that, according to the policy, collects the following information at 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 “Policy and Procedures for Privacy and Security Auditing”, the Privacy Officer along with their designate, the Supervisor of Database/Application Development, will have authority to manage the privacy and security program. The Privacy Officer will be 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.

“Policy and Procedures for Privacy and Security Auditing” states that 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 that do not identify any deficiencies in CCN’s privacy and security program are communicated to CCN agents within one week of the conclusion of the privacy or security audit.

A log of all privacy and security audits is required by “Policy and Procedures for Privacy and Security Auditing” to be created and maintained by the Privacy Officer. This log is required to be retained on the main CCN company drive. The Privacy Officer along with their designate, the Supervisor of Database/Application Development, 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 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 in itself non-compliance with CCN policy, and may result in disciplinary action.

Log of Security Audits

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

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.

Log of Information Security Breaches

As set out in "Information Security and Privacy Breach Management", 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;
- 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 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.

PART 3 – Human Resources Documentation

Policy and Procedures for Privacy and Security 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. Since its last report to the IPC, CCN has enhanced and expanded its privacy and security training procedures. CCN now 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 the fiscal year in April. CCN 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 and this is reflected through new privacy and security policies, procedures and practices and has regard to any recommendations with respect to privacy and security training made in PIAs, privacy and security audits and the investigation of privacy and security breaches and privacy and security complaints.

CCN developed an online privacy and security training module for the minimal number of agents that had access to personal health information for analysis, reporting or testing from our Wait Time Information System application. This role-based training initiative was recommended in the privacy impact assessment conducted by CCN. The PIA was a recommendation from the 2008 IPC review. CCN went the extra step and had all staff take the online privacy and security training to be aware of personal health information and privacy and security in general. Thus, while only 14 CCN employees have access to personal health information, all CCN staff engage in privacy training regardless of their level of access to personal health information. Similarly all other agents including Regional Cardiac Care Coordinators and Data Clerks within our member 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.

"Privacy and Security Training" 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; a description of the nature of personal health information collected and from whom this information is typically collected and why it is 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 the Privacy Officer of CCN manages the privacy program.

“Privacy and Security Training” 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 and to protect records of personal health information against unauthorized 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. "Privacy and Security Training" requires the training to include a discussion of the nature and purpose of the Confidentiality and Non-Disclosure Agreement that agents must execute and the key provisions of the Confidentiality and Non-Disclosure Agreement 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. All agents are also told that the life of the Confidentiality Agreement continues on after an agent is terminated from CCN.

Earlier this year CCN significantly increased their number of staff who required personal health information access to conduct their job, and thus our role-based training will be evolving over time.

The privacy and security program is mandatory. All new employees are required to sign a Confidentiality and Non-Disclosure Agreement as well as complete an online privacy and security training program. The results of this program are automatically tracked online. As a further component of privacy and security, each new employee is required to sign a Confidentiality and Non-Disclosure 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 and Non-Disclosure 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 are available to the Privacy Officer at any time. Review of these policies is completed on an annual basis.

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' Privacy Officer communicates with its 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, 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. Formalized, regularly scheduled privacy and security auditing will commence by the end of June 2011. The Privacy Officer will then be responsible for auditing for compliance with CCN's policy and procedures on a quarterly basis.

All agents are made aware that they must comply with the policy and procedures and report at the first reasonable opportunity any suspected breaches to the Privacy Officer. If any agent is found to be in breach of the Confidentiality and Non-Disclosure Agreement, the agent may be terminated in accordance with "Information Security and Privacy Breach Management".

Upon discovering or suspecting a breach, CCN agents must immediately notify the Privacy Officer. 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 and if personal health information has been compromised. The Privacy Officer is responsible ensuring that the proper steps are taken, given the particular circumstances of the breach, to contain the breach, and investigate the breach. The Privacy Officer must also take or recommend any remedial action required, provide notice where appropriate to the member hospital(s) and the IPC and complete the Privacy Breach template document.

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

As set out in "Privacy and Security Training", 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 conducted the privacy training and the score they obtained. CCN employees take this online privacy training every year on an ongoing basis and the results are obtainable by the Privacy Officer whenever they are required.

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 and Non-Disclosure Agreements with CCN at the outset of their employment or other contractual relationship and annually, at the beginning of each calendar year. "Execution of Confidentiality and Non-Disclosure Agreements" sets out that the confidentiality agreement used by CCN must include all of the conditions set out in the template provided by the IPC.

"Execution of Confidentiality and Non-Disclosure Agreements" sets out that CCN's Privacy officer is responsible for ensuring that the Confidentiality and Non-Disclosure Agreement has been executed with all CCN agents at the outset of their employment or other contractual relationship and annually, at the beginning of each calendar year. To ensure this, The Privacy Officer is required to provide agents with copies of the Agreement to sign at the outset of their employment or other contractual relationship and on an annual basis at the beginning of each calendar year.

"Execution of Confidentiality and Non-Disclosure Agreements" sets out that the Privacy Officer must provide notification regarding the necessity of their executing Confidentiality and Non-Disclosure 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 the role of the Privacy Officer is assumed by the Director of Operations, 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 "Execution of Confidentiality and

Non-Disclosure Agreements" does not require notification to be provided to the Privacy Officer at the outset of an agent's employment or other contractual relationship.

Additionally, the Privacy Officer must provide written notification regarding the Confidentiality and Non-Disclosure Agreement to all CCN agents at the beginning of each calendar year.

"Execution of Confidentiality and Non-Disclosure Agreements" 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. "Execution of Confidentiality and Non-Disclosure Agreements" sets out that if CCN agents who fail to execute confidentiality agreements with repeated notification will be denied permission to access or use personal health information. If the agent fails to execute the Agreement within one week, the agent will be subject to disciplinary action as set out in "Policy and Procedures for Discipline and Corrective Action".

As with all CCN policies, agents are required to sign agreements stating that they understand and will uphold CCN's policy on the execution of confidentiality agreements ("Execution of Confidentiality and Non-Disclosure Agreements") at the outset of their relationship with CCN and annually. Should an agent discover or suspect a breach of this policy, CCN's policy on privacy and security breaches ("Information Security and Privacy Breach Management") imposes a duty on them to report the breach or suspected breach to CCN's Privacy Officer. Consequences of a breach are determined by the Privacy Officer, 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 it is determined that there has been a breach of the Confidentiality and Non-Disclosure Agreement, CCN may seek legal action against the agent(s) responsible.

CCN audits "Execution of Confidentiality and Non-Disclosure Agreements" in accordance with its privacy and security audit policy ("Policy and Procedures for Privacy and Security Auditing"), which sets out that the Privacy Officer is responsible for auditing "Physical Security" on a quarterly basis.

Template Confidentiality Agreements with Agents

As required by "Execution of Confidentiality and Non-Disclosure Agreements", CCN has developed a template the confidentiality agreement that all agents are required to execute at

the outset of their employment and at the beginning of each calendar year. At minimum, this confidentiality agreement must set out the following:

General Provisions

- A description of CCN's status under PHIPA
- An explanation of CCN's duties under PHIPA
- A statement setting out that individuals who sign the Confidentiality and Non-Disclosure Agreement 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 and Non-Disclosure Agreement 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 and Non-Disclosure Agreement
- The definition of personal health information found in Section 4 of PHIPA

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
- A justification 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 and Non-Disclosure Agreement
- A stipulation that agents are prohibited from disclosing personal health information except as permitted by the Confidentiality and Non-Disclosure Agreement 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 "Termination of Employment" and "Termination or Cessation of Contractual Relationships"
- A statement setting out the time frame within which CCN property must be returned, the secure manner in which the property must be returned

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 policy "Information Security and Privacy Breach Management"

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 and Non-Disclosure Agreement

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 and Non-Disclosure Agreements in a locked drawer. Additionally, the policy dictates that the Privacy Officer will maintain an electronic log that charts CCN agents' execution of Confidentiality and Non-Disclosure Agreements. The policy requires the log to include the name of the agent, the date of commencement of employment, contractual or

other relationship with CCN and the dates the that the Confidentiality and Non-Disclosure Agreements were executed.

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

CCN has developed a job description for the role of the Privacy Officer ("CCN Privacy Officer Job Description"). "CCN Privacy Officer Job Description" 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.

"CCN Privacy Officer Job Description" 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 CCN Policy "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 clients. "CCN Privacy Officer Job Description" 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, "CCN Privacy Officer Job Description" 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 within 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 complaints and breaches of personal health information by CCN clients. The Privacy Officer must develop the mechanisms employed to determine to which parties personal health information is released, and monitors any personnel involved in this process.

The Privacy Officer must also ensure back up coverage with other staff with specific privacy and security responsibilities (e.g., Supervisor Database/Application Development) and can be delegated other responsibilities by the CEO.

CCN requires its Privacy Officer to have a full knowledge of privacy laws and 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 pursuant to "Privacy Inquiries and Complaints"
- Receiving, documenting, tracking, investigating and remediating privacy breaches, suspected privacy breaches, information security breaches and suspected information security breaches pursuant to "Information Security and Privacy Breach Management"

Conducting privacy and security audits pursuant to “Policy and Procedures for Privacy and Security Auditing”

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. ”Termination of Employment” states that resignations must be submitted in writing to the CEO. CCN currently utilizes its Master Services Agreement with its contractors to outline termination protocol.

“Termination or Cessation of Contractual Relationships” sets out the following procedures for the termination or cessation of a contract either by the contractor or by CCN:

- the failure of the other party to carry out a material duty or obligation under this 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 reserves the right to determine on a case-by-case basis, whether the consultant should have the right to terminate on 30 days notice, or should only CCN have this right.]
- in accordance with Section 23 (Force Majeure) of this Agreement; or
- mutual agreement of both parties to terminate the Agreement or a Service Schedule.

Furthermore, the contractor shall be entitled to be paid for any Services rendered to the reasonable satisfaction of the Client prior to the effective date of termination of the Agreement.

For CCN employees a protocol is in place (set out in the CCN policy, “Termination of Employment”). As part of the policy ”Termination of Employment”, the Supervisor must immediately advise the CEO and Director, Operations & Stakeholder Relations of all resignations 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,

Operations & Stakeholder Relations 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, Operations & Stakeholder Relations must ensure that communications to staff are appropriate to the situation.

The Director, Operations & Stakeholder Relations will make arrangements to obtain all CCN property on last day of work as is set out in the policy.

When an employee terminates their 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 Privacy Officer (all passwords are required to be immediately deactivated by the Supervisor of Database/Application Development).

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 Privacy Officer. Typically there is no issue if 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.

All access to the premises where records of personal health information are 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 Privacy Officer of CCN)

All access and parking cards to the main building, housing the location of CCN, are collected by the CCN Privacy Officer and in partnership with the building personnel deactivate the terminated employee on the same day of termination.

When CCN terminates an employee the CEO or Director of Operations and Stakeholder Relations 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 policy and procedures on a quarterly basis.

As set out in the CCN policy "Information Security and Privacy Breach Management", CCN agents are compelled to immediately notify the Privacy Officer should they identify or suspect a breach as defined in the breach policy.

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 a CCN 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 Administrative Supervisor shall conduct 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 shall be communicated to the CEO in a timely manner. In determining what discipline or corrective measures may be taken, the Privacy Officer shall take into consideration:

- Whether or not the agent intended to breach a CCN policy and/or expose personal health information
- Whether personal health information was breached or simply exposed to unacceptable risk
- The extent of the breach; if 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, shall be responsible for determining the seriousness of the corrective action. This determination shall be made on a case-by-case basis. Any agent found to have intentionally disclosed personal health information shall be summarily fired. The Privacy Officer shall complete the Form for Discipline and Corrective Action and submit it to the CEO. The Privacy Officer shall maintain a repository of copies of these forms both in hard copy and in a secure location on the CCN company electronic drive.

PART 4 – Organizational and Other Documentation

Privacy and Security Governance and Accountability Framework

The Chief Executive Officer of CCN is ultimately accountable for the protection of personal health information in the custody or 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. A more detailed description of the Privacy Officer's duties is located in Part 3 of this Report. Currently, the Privacy Officer of CCN is the Director of Operations and Stakeholder Relations who is also 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 contractors will receive a hard copy of the privacy and security governance and accountability framework upon final signatures of their Master Services Agreement and they will receive the privacy and security governance and accountability framework document directly via email or hardcopy from the Privacy Officer if there any changes.

The CCN Board of Directors will be provided with a written report of the status of the privacy and security practices of CCN at the CCN Annual General Meeting held in June or September. This report, developed by the Privacy Officer, will 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 will also provide 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 will also be advised if CCN receives any privacy complaints or discovers any privacy or security breaches, including the results of any investigations and the status of recommendations where applicable. This practice will begin in 2011.

At the governance level, the privacy and security governance and accountability framework is headed by the Chair of the CCN Board of Directors. At the operations level, it is headed by the CEO who has delegated duties to the Privacy Officer. Unless preceded by the CEO, the Privacy Officer is responsible for all communications relating to privacy and security, including those

relating to exigent issues. The main agents that would be affected are the CCN member hospitals, our hosting agent for our web based wait time information system application and our contracted vendor who provides network administration support.

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

Cardiac Care Network does not require terms of reference as the privacy and security program are led by the Privacy Officer and there are no committees that have a role in respect of the privacy and/or security program. The Privacy Officer will assign an internal staff member from the Information Technology to assist with the audit functions of CCN as required.

Corporate Risk Management Framework

CCN does not have a formal corporate risk management framework. However, it has implemented several measures to mitigate any known and unknown risks. Each of the items listed below has been discussed in other parts of this document, along with rules governing their maintenance and frequency of review.

CCN:

- only allows access to personal health information to staff that require personal health information to conduct their day to day work
- receives personal health information from hospitals through their host vendor via a secure FTP site
- does not allow personal health information with portable media/devices to leave the physical perimeter of its office
- performs and tracks privacy and security audit logs of personal health information
- has participation agreements with all CCN member hospitals compelling them to adhere to privacy and security policy
- maintains a rigid, privacy-focused data sharing agreement with key partner
- requires all staff and contractors to sign non-disclosure agreements and complete online privacy training

In addition, CCN's hosting vendor, Cancer Care Ontario, has well defined privacy and security policies and a robust disaster recovery plan, both of which will be submitted to the IPC in Cancer Care Ontario's report.

Corporate Risk Register

While CCN has determined that it does not require a formal corporate risk register, it is committed to keeping abreast of the evolving risks that it faces. These considerations are reflected in the safeguards that CCN implements to protect the personal health information in its custody. These safeguards are set out in the CCN policy "Safeguards for Personal Health Information" and are listed in the above section.

Policy and Procedures for Maintaining a Consolidated Log of Recommendations

It is the CCN's policy ("Maintaining a Consolidated Log of Recommendations") to ensure that 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 be maintained. This new document has a consolidated and centralized log which shall also be required to include recommendations made by the IPC that must be addressed by the prescribed person prior to the next review of its practices and procedures.

The centralized 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.

All agents of CCN must comply with this policy and related procedures. Compliance will be audited in accordance with the "Policy and Procedures for Privacy and Security Auditing". These audits will occur quarterly conducted by the Privacy Officer with the first one occurring at the end of June 2011.

All agents are required to notify CCN at the first reasonable opportunity in accordance with CCN's "Information Security and Privacy Breach Management" if an agent breaches or believes there may have been a breach of this policy or procedures.

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 Information and Privacy Commissioner of Ontario. Information included in the log is name and date of the document, investigation, audit and/or review from which the recommendation arose. The log includes the recommendation made, the date that the recommendation was addressed or by which it is required to be addressed and the agent responsible for addressing the recommendation. The Privacy Officer will review each recommendation by date and ensures that each requirement is met for all recommendations in the consolidated log.

Business Continuity and Disaster Recovery

CCN has taken measures to ensure that in the event of a disaster, continuity of service can be assured. CCN uses the Acronis Backup & Recovery 10 Advanced Server system, which automatically backs up information stored on CCN servers and workstations, including personal health information. If the internal CCN network were to fail, the Acronis system could restore all lost data. To further ensure the security and persistence of CCN networks in the event of a disaster, CCN has tape backups of its servers performed through an external vendor, which stores the tapes at an off-site location. Based on the comprehensive nature of CCN's backup practices, service can be restored within a day of a non-catastrophic disaster, or two days at maximum.

The WTIS-CCN application is hosted offsite at Cancer Care Ontario, whose business continuity and disaster recovery arrangements are discussed are detailed in its own submission to IPC.

In light of the nature and scope of CCN's activities and the measures it takes to ensure continuity of service, CCN has determined that it need not have a business continuity and disaster recovery plan that sets out all the requirements of the *Manual*.

PART 5: Privacy and Security Indicators

CCN Response to 2008 IPC Recommendations

After receiving the ten recommendations made by the IPC in its 2008 report, CCN worked extensively to expand and enhance its privacy and security program. CCN has addressed all ten recommendations by amending or developing and implementing new policies,

IPC Recommendation 1: Amend the *Response to a Breach Policy* CCN policy to expand the definition of "breach", to impose a positive duty on agents to notify the Privacy Officer of a breach, to identify what information must be reported and the format for this report, to address the process for containment, investigation and remediation of a breach and to address notification in the event of a breach, including to the Health Information Custodian that provided the personal health inform. Develop written policies and procedures to address the identification, reporting, containment, notification, investigation and remediation of information security incidents.

Developed by CCN's privacy officer in December of 2009, CCN's new policy on breaches ("Information Security and Privacy Breach Management") took effect on April 1, 2009. It was amended on April 25, 2011. The new policy:

- includes an expanded definition of a personal health information breach;
- imposes a positive duty on CCN employees and third party service providers to notify the CCN Privacy Officer if a breach takes place including "when personal health information is lost, stolen or disclosed to those unauthorized";
- provides a form to be used to report privacy and security incidents that outlines the information required and format to be used for reporting an incident;
- assigns responsibility for breach management to the Privacy Officer who will ensure that the proper steps are taken, given the particular circumstances of the breach, to contain the breach, investigate the breach, take or recommend any remedial action required, provide notice where appropriate to the member 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;
- requires CCN to take corrective measures to prevent further breaches.

IPC Recommendation 2: Develop and implement a written policy and associated procedures for receiving, documenting, tracking, investigating and remediating privacy complaints and for receiving, documenting, tracking and responding to privacy inquiries.

CCN has developed a new policy relating to the processing of privacy complaints and privacy inquires ("Privacy Inquiries and Complaints"). This policy was developed in July 2008 and took effect in November 2008. It was amended on April 25, 2011. The new policy clarifies that CCN will accept and respond to complaints and inquiries by any person about CCN's management of PHI and PHI management practices. Questions or complaints are to be sent to the CCN Privacy Officer, who will investigate and take appropriate action where indicated by the results of the investigation. Instructions for how to contact CCN's Privacy Officer are posted on the CCN website and printed in pamphlets provided to member hospitals for distribution.

IPC Recommendation 3: Develop and implement a written policy and associated procedures for the annual review of the privacy and security policies and procedures implemented by CCN and review these privacy and security policies and procedures in light of the WTIS-CCN.

In July 2009, CCN implemented a policy under which its Privacy Officer reviews its privacy and security policies and practices at the beginning of each fiscal year ("Annual Review of Privacy and Security Policies and Procedures"). The Privacy Officer is required to ensure that CCN policies reflect advancements in technology and in industry practices. The Privacy Officer is also to verify that CCN's policies and practices are consistent with directions and orders of the IPC and PHIPA. In the event that the IPC issues new guidelines or the law is changed, CCN's Privacy Officer is to recommend changes to bring its policies and practices into compliance and ensure that such recommendations are implemented by CCN as quickly as possible.

IPC Recommendation 4: Conduct a comprehensive privacy impact assessment on WTIS-CCN and implement all the recommendations arising from the threat and risk assessment performed on the WTIS-CCN in June 2008.

CCN had a privacy impact assessment conducted by David Flaherty, Inc. After receiving comments from the IPC, CCN adopted all recommendations made in the privacy impact assessment and a final review was conducted by CCN's legal counsel.

CCN has adopted all of the recommendations made in the threat and risk assessment performed in June 2008.

<u>IPC Recommendation 5</u>: Develop written policies and procedures with respect to the use and disclosure of personal health information for research purposes in accordance with PHIPA and its regulation prior to any use or disclosure of personal health information for research purposes.

As CCN does not use or disclose identifiable personal health information for research purposes, the written policies and procedures referred to in Recommendation 5 are unnecessary. As CCN discloses personal health information in aggregate/de-identified format to researchers if certain conditions are met, CCN has developed a policy ("Disclosure of Aggregate and/or De-identified Health Information to Researchers") that requires such disclosures to be made in accordance with PHIPA and its regulation. This policy was developed on May 8, 2011 and came into effect on May 31, 2011.

<u>IPC Recommendation 6</u>: Amend the *Destruction of Personal Health Information Policy* to set out the type of shredding that is employed for records of PHI in paper format and ensure that the shredding employed is consistent with Order HO-001 and *Fact Sheet 10* issued by the IPC and with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to PHIPA.

CCN's "Destruction of Personal Health Information" Policy has been amended in accordance with this recommendation. The new policy ("Destruction of Personal Health Information") was developed by CCN's Privacy Officer in August 2008 and took effect that same month. It was amended on May 7, 2011 It provides that all paper documents containing personal health information must be placed in secure shredding boxes for removal and off-site shredding by Shred-it, an outside company the employees of which 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. Under the policy, if personal health information is to be deleted from a hard drive, the drive must be formatted 4 times (sanitizing the hard drive) and then mechanically destroyed.

<u>IPC Recommendation 7</u>: Amend the initial privacy and security orientation in accordance with the comments provided by the IPC, formalize ongoing privacy and security training, and ensure that ongoing privacy and security training includes role-based training and a

discussion of any new policies, procedures and practices implemented or significant amendments to existing policies, procedures and practices implemented by CCN.

In September 2009, CCN's Privacy Officer developed and implemented a policy ("Privacy and Security Training") under which all CCN employees must complete privacy training upon being hired and annually thereafter. The policy was amended on May 2, 2011. The training is completed online and is administered by CCN's Communications Coordinator. If an agent fails the test administered at the end of training program, he or she is required to repeat the training program until successful. The training program will be reviewed annually and where necessary updated, by CCN's Privacy Officer to ensure that it includes a discussion of any new policies, procedures and practices implemented or significant amendments to existing policies, procedures and practices implemented by CCN. CCN makes the training program available to employees of member hospitals and to employees of third party service providers.

IPC Recommendation 8: Develop and implement a written policy and procedure to formalize CCN's practices and procedures related to the execution of the Confidentiality and Non-Disclosure Agreement.

CCN has amended its policy on the execution of its Confidentiality and Non-Disclosure Agreement ("Execution of Confidentiality and Non-Disclosure Agreements by Agents"). Under the amended policy, upon being hired by CCN and at the beginning of each fiscal year, employees will sign the Confidentiality and Non-Disclosure Agreement as a part of their contract with CCN.

IPC Recommendation 9: Amend the *Participation Agreement, Master Services Agreement, and Consulting Agreement* pursuant to the IPC's comments.

CCN has amended its template Participation Agreement and a consolidated version of its Master Services and Consulting Agreements in accordance with the IPC's recommendations. The Agreements now reference PHIPA and bind the signatories to protect personal health information. CCN intends to have a complete legal review performed of its agreements and to approach the member hospitals and third party service providers about executing any new form of Participation Agreement and Services Agreement that arises out of that review.

<u>IPC Recommendation 10</u>: Develop and implement a privacy and security audit program as well as written policies and procedures relating to the maintenance, review and analysis of audit logs; the conduct of privacy and security audits; and the secure transfer of personal health information.

CCN has developed policies on the secure transfer of personal health information and the auditing of its systems. CCN will only transfer personal health information that has been encrypted using 128-bit encryption, either on CDs or via SFTP (Secure File Transfer Protocol). The use of portable media to transfer personal health information is prohibited. For transmissions over the Internet, CCN uses 128-bit VeriSign SSL Digital Certificate encryption.

CCN has implemented a number of privacy and security auditing programs, including system control audit log review. These programs are set out in the policies "Policy and Procedures for Privacy and Security Auditing" and "Maintenance and Review of System Control and Audit Logs". On a daily basis, CCN audits logs of irregular server activity, regular system backup, data transfers, and changes to the WTIS-CCN database. On a weekly basis, CCN audits anti-virus threat reporting and update logs. Monthly, CCN reviews logs of e-mail transmissions to ensure that internal accounts have not been compromised, log-in attempts (on-site and remote), and changes to security and privacy settings. CCN's Director of Operations and Stakeholder Relations delegates responsibility for the review and analysis of these system control audit programs to CCN's Supervisor Database/Application Development. Additionally, CCN's privacy and security auditing program assesses CCN agents' compliance with CCN policies, privacy legislation, and IPC orders and guidelines.

Privacy, Security, Human Resources, and Organizational Indicators

Privacy and Security Indicators

Categories	Privacy Indicators
General Privacy & Security Policies, Procedures and Practices	• Privacy and security policies and procedures were formally reviewed in January 2011 and will be reviewed on an annual basis in the month of April • No amendments were made to existing privacy policies and procedures • No new privacy policies and procedures were developed and implemented as a result of the review • No new privacy policies and procedures were developed • The communication materials including brochures and posters are all available to the public and no new communication materials were sent to public and other stakeholders
Physical Security	• CCN is only accessible via electronic card reader and the Server Room is accessible by a few CCN employees via card reader. The Server Room is also armed with an alarm with keypad. This room is only accessible by a few CCN employees. • The only external vendor that has access to CCN is Interface Inc. – they have an assigned card reader and a specific code to the Server Room • The CCN Privacy Officer conducts random audits of the premises and receives Yonge Corporate Centre reports of who accessed Suite 502 via the card reader • CCN audits its employees' access to the premises on a quarterly basis via reports from the Yonge Corporate Centre Security Office. The last one was on June 30 2011 and there were no recommendations required.
Collection	• CCN collects personal health information from member hospitals through the WTIS-CCN application which is hosted at Cancer Care Ontario's facility pursuant to a hosting agreement • There is one statement of purpose developed for the CCN Wait Time Information System data holdings containing personal health information

	• No statements of purpose for data holdings containing personal health information were reviewed since the prior review by the Information and Privacy Commissioner of Ontario • No amendments were made to the existing statement of purpose for data holdings containing personal health information.
Use	• CCN uses personal health information for the purposes of maintaining the Registry as further described in this report • As of January 4 2011 there are 14 agents (in addition to the 18 member hospitals, who have access to the personal health information collected at their sites) who have been granted approval to access and use personal health information for purposes other than research (maintain the registry including analysis, reporting and testing) – Prior to January 2011 there were 6 agents who had access to use personal health information for purposes other than research. • CCN does not use personal health information for research. There were no requests by CCN agents to use personal health information for research.
Disclosure	• CCN does not disclose the personal health information it collects in any circumstances except those discussed in CCN`s data sharing agreement with the ICES • There have been zero requests for the disclosure of personal health information for purposes other than research • There have been zero requests for the disclosure of personal health information for research purposes • Between April 2009 and April 2010, CCN received two requests for de-identified/aggregate data from researchers not affiliated with CCN's member hospitals and seven such requests from researchers affiliated with CCN's member hospitals • Between January 2009 and June 2011, CCN received 115 requests for de-identified/aggregate data from CCN member hospitals for other purposes. CCN maintains a database of all requests from member hospitals, CCN staff and other

	networks/organizations • All these requests were granted because the data were de-identified/aggregate and no longer constituted personal health information. Additionally, the provision of aggregate/de-identified data is conditional on the researcher's fulfillment of the conditions set out in the CCN policy "Disclosure of Aggregate and/or De-Identified Health Information to Researchers". • No requests have been received for the disclosure of personal health information (and no Research Agreements executed with researchers) since CCN's last report to the Information and Privacy Commissioner of Ontario • There has been one agreement executed by ICES to which de-identified and/or aggregate information for both research and other purposes was provided since the prior review by the IPC.
Data Sharing Agreements	• CCN is a party to one data sharing agreement with ICES, executed in March 2009 • CCN is disclosing personal health information to ICES
Agreements with 3rd Party Service Providers	• CCN is party to an agreement with Cancer Care Ontario for hosting services, an agreement with Interface Inc. for network management and backup (IT) services
Data Linkage	• No data linkages have been approved/implemented since CCN's last report to the Information Privacy Commissioner of Ontario
Privacy Impact Assessment	• CCN did not have any privacy impact assessments undertaken but not completed since the prior review by the IPC and the proposed date of completion • CCN did not have any privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion • There were no 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 • CCN had a privacy impact assessment of its data holding (WTIS-CCN) conducted by David Flaherty Inc. In June 2009. Amendments to the assessment were made in February 2010.

	The assessment delivered the following recommendations: ○ An annual review of the privacy impact assessment for the Cardiac Registry to keep it up to date, relevant and informative. It should also be posted on the CCN web site in a page on privacy and security. The assessment was reviewed and amended in February 2010 and will be posted to the CCN website pending the site's upcoming redesign. ○ CCN has only a small staff at the provincial office and in the field that require specialized privacy training that reflects CCN's particular characteristics. This will be packaged as brief, concise, on-line training that staff can repeat on an annual basis. This recommendation has been addressed via our online web privacy and security training module and is repeated in April of every year. ○ Regional Coordinators need to be trained in CCN's privacy policy, since they receive new information for CCN from patients or family, physicians or other members of the Health Care Team, and other Regional CCN Coordinators. This would happen at hospitals and at Regional Cardiac Care Coordinator meetings. This recommendation has been addressed via our online web privacy and security program. CCN only has one "role" with respect to personal health information (all agents with access to personal health information have the same level of access to the same data holding). Based on this, CCN developed a program for agents with access to personal health information. The Privacy Officer then decided to administer this training to all CCN agents, giving them all the highest possible level of training. ○ All agents will be informed that the database will be audited for unauthorized or illicit access as the available software permits. Sanctions should be in place to deny privileges to access the database, if problems with unauthorized or illicit access are found. ○ As stated in CCN's "Policy and Procedures for Privacy and Security Auditing", the Privacy Officer conducts privacy and security audits on a quarterly basis. These

	audits assess compliance with the CCN privacy and security program and seek to identify any possible breaches or deficiencies.

Privacy and Security Audit Program	• As per the IPC's recommendation, CCN has developed a privacy and security audit program governed by its policy "Policy and Procedures for Privacy and Security Auditing"
	• The policy sets out the purpose of each log and the procedures for completing each log
	• The following automated security audits are currently being conducted:
	  ○ On a daily basis, CCN audits the following:
	  ▪ WTIS-CCN data transfer logs - verify if database replicated by Cancer Care Ontario is successfully received and resides at CCN and examine file transfer protocol event log and verify file transfer protocol server has receive capabilities
	  ▪ Verify file transfer protocol queue.
	  ▪ WTIS-CCN database replication logs - WTIS-CCN database restore process logs. Check the number of tables/records between replicated and restored database and verify database is mounted properly
	  ▪ Server operating system log and performance - examine available MBs performance counter, processor time counter, committed bytes in use performance counter, disk usage, and performance log; monitor filtering application; monitor system logs on Windows Servers to see repetitive warning and error logs and discover failures and problems
	  ▪ Backup logs - ensure that daily backup is completed; verify that the previous backup operation is completed; analyze and respond to errors and warnings during the backup operation and follow the established procedure for tape rotation, labelling, and storage (done through Recall)

	○ On a weekly basis, CCN audits the following - CCN network antivirus threat report and update logs ○ On a monthly basis, CCN audits the following - Security logs ▪ 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 ▪ Each audit was done on a daily, weekly or monthly basis - No recommendations were made because all standards were maintained. ▪ Other security audits such as quarterly review of entrance into CCN premises including Server Room and random review of computer and mobile devices for personal health information will be conducted at the end of June 2011 and every quarter following. • Additionally, the policy sets out that a log must be maintained by the Privacy Officer that records the date of the audit, recommendations made as a result of the audit, the manner in which the recommendations are to be addressed, the agent responsible for addressing the recommendations, and the timeline for addressing the recommendations • CCN has conducted its quarterly privacy audit according to the CCN policy and procedures for privacy and security auditing on July 4 2011. This included an audit of aggregate/de-identified data provided to researchers; an audit of staff computers for unauthorized personal health information; an audit of CCN laptops and mobile devices lent to staff; an audit of the log of agents granted access to personal health information; a review of information made available on CCN's website and included in the brochure distributed to hospitals and a review of documentation related to the formal review of privacy and security policies. There were no recommendations to report – the second privacy audit will be conducted in the second quarter of the fiscal year.

Information Security and Privacy Breaches	• Since its last report to the IPC, there have been no instances in which personal health information was compromised. CCN has identified and resolved two cases in which full compliance with its privacy and security program was not achieved: o The first incident occurred October 10 2008. A partial record of patient information was inadvertently sent via e-mail by a health information custodian at a CCN member hospital to the CCN help desk. CCN management was informed the same day and the data was deleted at both locations in accordance with "Destruction of Personal Health Information". The investigation, which was finalized on October 14 2008, found that it was a case in which a CCN agent had failed to comply with CCN privacy policies. An email communication was sent to all users not to send emails containing personal health information unless it was 128-bit encrypted. No further instances have been identified. o The second incident occurred on July 7 2010. A change to a patient record in WTIS-CCN was made by a software developer at CCN's hosting agent, who mistakenly believed that he/she was working in a testing environment. The software developer was authorized to access the PHI. CCN management was informed the same day and the error was identified and rectified by hosting vendor who in consultation with CCN delivered the final report on August 3, 2010. Cancer Care Ontario took steps to improve their training and auditing programs in order to prevent a reoccurrence of similar errors. A monthly audit was conducted and is shared with CCN – this occurred immediately following the resolution of this issue.
Privacy Complaints	• There have been no privacy complaints made to CCN since its last report to the Information and Privacy Commissioner of Ontario

Human Resources Indicators

Categories	Human Resources Indicators
Privacy and Security Training & Awareness	• All CCN staff and vendors contracted by CCN have received privacy and security training • Privacy and security training is conducted on an annual basis via an online program which tracks program completion by participant and date – this is conducted on an annual basis in April • There are no agents who have not attended ongoing privacy and security training each year since the prior review by the Information and Privacy Commissioner of Ontario • When it is time for the privacy and security training the Privacy Officer sends an email and tells all CCN employees at the monthly staff meeting that they will have to conduct privacy training. This practice is beginning on April 1 2011. • The Privacy Officer ensures that at the orientation there is a verbal description of the privacy and security program at CCN including the policies, the Confidentiality and Non-Disclosure Agreement, the online privacy and security module. This has occurred on January 4, 2011, January 24 2011 and June 6 2011. They are told that the CCN Privacy Officer handles all privacy issues or concerns and that any questions that arise should be directed to the Privacy Officer. • The Privacy Officer also provides verbal updates for the CCN staff at staff meetings (the following 2 staff meetings had verbal updates: October 29th, 2010 and May 27th, 2011) • Agents at member hospitals are made aware of any privacy updates or changes and they receive the same orientation from CCN for the privacy and security program and then expected to complete the privacy and security program while achieving a passing mark. A verbal update was provided for our WTIS-CCN application team from Cancer Care Ontario in July 2010. • CCN maintains a database of number of agents who complete and pass the privacy and security training. This is sorted by date, organization and name.

Confidentiality Agreements	• All CCN staff and vendors contracted by CCN have signed the Confidentiality and Non-Disclosure Agreement and sign the Confidentiality and Non-Disclosure Agreement on an annual basis at the beginning of the fiscal year in April. • There are 74 CCN employees or other agents who have signed the Confidentiality and Non-Disclosure Agreement since October 31 2008. • There are no CCN employees or other agents who have not signed the Confidentiality and Non-Disclosure Agreement
Termination or Cessation	• CCN has not received any notifications from agents since the prior review by the Information and Privacy Commissioner of Ontario related to termination of their employment, contractual or other relationship with CCN. Several CCN employees have left CCN for other job opportunities and CCN has hired several new employees since the last review by the Information and Privacy Commissioner of Ontario.

Organizational Indicators

Categories	Organizational Indicators
Risk Management	• CCN implemented a consolidated and centralized log of recommendations as a corporate risk management tool in December 2010, reporting protocols (to the Privacy Officer, CEO and the Board), an audit program and regular monitoring of its systems • No amendments have been made to the corporate risk tool
Business Continuity and Disaster Recovery	• CCN's limited disaster recovery plan which does not contain all the requirements of the IPC *Manual* was tested via a practice run on April 16, 2010 by CCN's Network Support Provider, Interface Inc. • No changes were found to be necessary on the basis of the April 16, 2010 vulnerability assessment. • The current Business Continuity and Disaster Recovery plan will be tested on an annual basis in April.