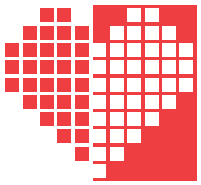
Cardiac Care Network



CCN PRIVACY AND SECURITY POLICIES AND PROCEDURES

September 2014

CARDIAC CARE NETWORK

Contents

INTRODUCTION

The Cardiac Care Network of Ontario (CCN) is an advisory body to the Ministry of Health and Long-Term Care that is responsible for developing, maintaining and reporting on the Registry of all patients waiting for selected adult advanced cardiac procedures in Ontario. Information about the Registry is publicly available on the CCN website at www.ccn.on.ca.

As a prescribed person within the meaning of the Personal Health Information Protection Act, 2004, CCN is permitted to collect, use, and disclose personal health information without consent for the purposes of facilitating or improving the provision of cardiac care services. In particular, CCN uses personal health information in its Registry of cardiac services to monitor and manage the health status of patients who are waiting to access advanced cardiac services and for service evaluation and planning to improve the provision of cardiac services in the province.

CCN is compelled by the Personal Health Information Protection Act, 2004, to collect, use, disclose, and dispose of personal health information according to that law and in such a manner that maintains its confidentiality and integrity. CCN has developed and implemented a number of policies and procedures to protect the privacy of individuals whose personal health information it collects. These policies and procedures are reviewed by the Information and Privacy Commissioner of Ontario every three years.

CARDIAC CARE NETWORK

PROTECTION OF PERSONAL HEALTH INFORMATION

The following ten principles provide the basis for the ongoing review, amendment, and development of the policies that comprise CCN's privacy and security program. CCN agents are bound by contractual agreement to comply with the procedures and imperatives set out in these principles, which are designated PR in CCN's privacy and security policy numbering system.

Developed by:	**Issued by:**	**Policy #:**
Director of Operations & Stakeholder Relations	CCN	PR1-PR10
Created:	**Effective:**	**Revised:**
September 2008	September 2008	July 19 2013

PR1 – Accountability for Personal Health Information

The Chief Executive Officer of the Cardiac Care Network of Ontario is ultimately accountable for the protection of personal health information in CCN's custody or control. The day to day responsibility for ensuring that personal health information is collected, used, and disclosed in accordance with its privacy policies and procedures and in compliance with the Personal Health Information Protection Act, 2004 has been delegated to the Privacy Officer, who is currently the Lead, Data Governance and Reporting.

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

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

PR2 – Identifying Purposes for Collecting Personal Health Information

Via front-line healthcare providers, CCN identifies to patients the purposes for which personal health information is collected proximate to the time that the personal health information is collected. Each patient registered in the Registry of cardiac services compiled and maintained by CCN is provided with an information brochure specifying the purposes for which personal health information is being collected. This information brochure is also available on the CCN website, www.ccn.on.ca. In addition, posters identifying the information practices of CCN are posted in the cardiac areas of the hospitals from which CCN collects personal health information.

CCN uses identifiable health information to maintain waiting lists for treatment. The types of personal health information collected include:

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

In the course of the annual review of CCN's privacy and security program, the Privacy Officer will, in cooperation with application development and clinical staff, review the elements of personal health information generally collected by CCN to ensure that it is minimal in scope. This review will be documented according to the procedures set out in the policy, "Annual Review of Privacy and Security Policies and Procedures".

CCN maintains a list of data holdings containing personal health information. This policy is set out as "Statements of Purpose for Data Holdings Containing Personal Health Information". Currently, CCN's only data holding is its Registry.

CARDIAC CARE NETWORK

PR3 – Notice/Consent for Collecting, Using, or Disclosing Personal Health Information

Via front-line healthcare providers, CCN provides notice to patients about its collection, use and disclosure of personal health information through a patient brochure. The brochure is provided to each patient whose personal health information is collected for its Registry of cardiac services and is available on the CCN website, www.ccn.on.ca.

As a prescribed person within the meaning of subsection 39(1)(c) of the Personal Health Information Protection Act, 2004, CCN is permitted to collect personal health information without consent for 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. CCN is also permitted to use and disclose this personal health information without consent where permitted by the Personal Health Information Protection Act, 2004.

CCN acknowledges that patients in its Registry of cardiac procedures are entitled to receive information to allow them to understand the purposes of the Registry, including information to help them understand how the Registry assists in facilitating their care. As set out in the policy entitled “Privacy Inquiries and Complaints”, CCN accepts and endeavours to resolve every inquiry or complaint submitted by patients and other individuals.

PR4 – Limiting Collection of Personal Health Information

CCN limits the collection of personal health information to that which is necessary for the purposes it has identified. CCN collects personal health information by fair and lawful means.

CCN does not collect personal health information where other information will suffice.

CCN's Privacy Officer ensures that each collection of personal health information is permitted under the Personal Health Information Protection Act, 2004 and its regulation. To that end, the Privacy Officer ensures that CCN only collects personal health information that will be used in the manner prescribed by Sections 39(c) and 45 of the Personal Health Information Protection Act, 2004.

PR5 – Limiting Use, Disclosure, and Retention of Personal Health Information

CCN only uses and discloses 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 and to assist in the management and planning of the delivery of cardiac care services in Ontario, and as permitted or required by law, including the Personal Health Information Protection Act, 2004.

CCN permits employees, consultants, contractors, and volunteers to access and use personal health information on a "need to know" basis, when access is required for the performance of their employment, contractual, or other relationship with CCN. CCN agents are not permitted to use any identifiable personal health information if de-identified or aggregate personal health information will suffice. Additionally, CCN agents are prohibited from using personal health information for research purposes. The CCN policy "Limiting Agent Access to and Use of Personal Health Information" sets out further procedures for ensuring that there are limits and restrictions on agent access to and use of personal health information.

As permitted in Section 45 of the Personal Health Information Protection Act, 2004, CCN has executed a data sharing agreement with the Ontario Institute for Clinical Evaluative Studies, a research institute that is contractually required to de-identify patient information upon receiving it. Additionally, CCN may disclose personal health information when required by law. Excluding these identified purposes, CCN prohibits the disclosure of personal health information. This rule also applies to data linkages of personal health information, which are also prohibited. De-identified personal health information may be provided to researchers in accordance with the policies "Aggregation and De-identification of Record Level Data" and "Disclosure of Aggregate and/or De-identified Personal Health Information to Researchers".

Personal health information is retained by CCN only as long as is necessary for the fulfillment of the identified purposes. Personal health information that is not required for the identified purposes is destroyed in a secure manner to ensure that reconstruction is not reasonably foreseeable in the circumstances according to the procedures set out in the policy "Destruction of Personal Health Information".

PR6 – Accuracy of Personal Health Information

Personal health information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. Data quality audits are routinely performed. CCN's wait list data on individuals are verified on a monthly basis.

PR7 – Safeguards for Personal Health Information

CCN protects personal health information through administrative, physical and technical safeguards.

Administrative safeguards include:

- The development and implementation of privacy and security policies and procedures;
- Standardized privacy and security training;
- Requiring employees, consultants, volunteers and members of the Board of Directors to sign Confidentiality Agreements that clearly state their obligations with respect to protecting the privacy of individuals with respect to personal health information;
- Requiring Participation Agreements to be executed prior to the collection of personal health information from member hospitals.

Physical safeguards include:

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

Technical safeguards include:

- The use of firewalls, network encryption, and intrusion detection systems; and
- A credible program for the 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.
- CCN has a security requirement traceability matrix (SRTM), a document which describes the security and privacy requirements are for the WTIS-CCN Reporting Module. This security requirement training matrix (SRTM) enables CCN to demonstrate that the application's design and implementation is able to, or is meeting, all of the required controls as defined by the business and legislative requirements.

CARDIAC CARE NETWORK

PR8 – Openness about Information Management Policies and Practices

The Cardiac Care Network Ontario (CCN) makes available information about its policies and procedures relating to the management of personal health information through its website.

Each individual in its Registry of cardiac services is provided with an information brochure by the cardiac centre setting out the purposes for which CCN collects and uses personal health information. Furthermore, CCN has posters in the cardiac areas of member hospitals identifying its information practices.

PR9 – Individual Access to Personal Health Information

Upon written request an individual is informed of the existence, use, and disclosure of his or her personal health information in the cardiac registry.

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

CARDIAC CARE NETWORK

PR10 – Challenging Compliance with the Privacy and Security Program

An individual is able to challenge compliance with CCN's privacy policies. Additionally, an individual can submit inquiries to the Privacy Officer regarding CCN's privacy and security program. In the Privacy Officer's absence, complaints and inquiries can be directed to the Director of Communications. The Chief Executive Officer, or the designated manager, will handle complaints and inquiries in the absence of the Privacy Officer and the Director of Communications.

All complaints should be directed to CCN's Privacy Officer, where the matter is documented and investigated further and referred onwards, if appropriate.

The Information and Privacy Commissioner of Ontario has jurisdiction over CCN's compliance with the Personal Health Information Protection Act, 2004.

Contact Information for CCN Privacy Officer:
4100 Yonge Street
Suite 502
Toronto ON
M2P 2B5
Web: www.ccn.on.ca
416-512-7472
Email: mail@ccn.on.ca

Contact Information for the Information and Privacy Commissioner/Ontario:
Information and Privacy Commissioner/Ontario
2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Web: www.ipc.on.ca
Toronto Area: (416/local 905) 416-326-3333
Long Distance: 1-800-387-0073 (within Ontario)
Email: info@ipc.on.ca

CARDIAC CARE NETWORK

PRIVACY POLICIES AND PROCEDURES

P1 – Annual Review of Privacy and Security Policies and Procedures

Developed by:	**Issued by:**	**Policy #:**
Director of Operations & Stakeholder Relations	CCN	P1
Created:	**Effective:**	**Revised:**
May 2009	June 2009	July 19 2013

Overview

This policy sets out the procedures for the annual review of all CCN privacy and security policies and procedures. The purpose of the review is to determine whether amendments are needed and/or whether new privacy policies, procedures and practices are required.

Background

CCN's privacy and security policies and procedures reflect laws, best practices, and technological standards at the time of their development. Ongoing review is necessary to ensure that the policies keep abreast of advancements in these and other categories of assessment.

Policy

1. The Privacy Officer is responsible for undertaking the review of privacy and security policies and procedures.

2. The annual review includes a review of CCN's privacy and security training program.

3. In the course of review, the Privacy Officer ensures that:
    - Privacy and security policies and procedures reflect advances in privacy enhancing technologies.
    - CCN policies reflect any relevant orders, guidelines, and best practices issued by the Information and Privacy Commissioner of Ontario.
    - Any applicable industry security and privacy best practices are implemented.
    - Any new amendments to existing privacy legislation relevant to CCN in respect of its Registry of cardiac services, including amendments to the Personal Health Information Protection Act, 2004 and its regulation, are implemented.

4. The Privacy Officer also reviews the degree to which existing policies have been implemented, and may make recommendations in that regard.

5. The Privacy Officer makes amendments to policies based on the recommendations made in the review as promptly as is reasonably possible.

6. The Privacy Officer communicates in a timely manner any changes to CCN's privacy and security program. This communication shall be made in written format. The manner of communication will be reviewed annually.

7. This review shall be undertaken at least annually at the beginning of each fiscal year (April).

8. Formal reviews may also be undertaken on the order of the Information and Privacy Commissioner of Ontario or if prompted by a privacy impact assessment, a recommendation made in a completed Privacy Breach Management Form, or a privacy or security audit.

9. A brief outline of the review of each policy is recorded using the Form for Formal Review of Privacy and Security Policies and Procedures. The Privacy Officer maintains a log of actions taken during the formal review.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Director of Communications or her/his designate on a quarterly basis. The auditor shall review the completed Form for Formal Review of Privacy and Security Policies and Procedures to ensure that the review has been properly conducted and that the recommendations have been properly logged. Should the Director of Communications determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

P2 – Transparency of Privacy and Security Policies and Procedures

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	P2
Created:	**Effective:**	**Revised:**
September 2009	January 1 2010	July 19 2013

Overview

This policy sets out the procedures for ensuring that CCN's privacy and security program is transparent and open to public scrutiny.

Background

It is the Cardiac Care Network's policy to ensure that appropriate information is made available to the public and other stakeholders. This policy identifies the means by which such information is made available.

Policy

1. The most current versions of the following documents shall be made available on the CCN website, www.ccn.on.ca:
    - All CCN privacy and security policies.
    - Brochures or frequently asked questions related to the privacy and security policies, procedures and practices implemented by the prescribed person
    - Documentation related to the review by the Information and Privacy Commissioner of Ontario of the policies, procedures and practices implemented by the prescribed person to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.
    - A list of data holdings containing personal health information maintained by CCN.
    - Instructions for how to submit inquiries and/or complaints related to CCN's privacy and security program to the CCN Privacy Officer. The contact information for the Privacy Officer shall be included.
    - Instructions for submitting concerns, complaints, and inquiries to the Information and Privacy Commissioner of Ontario regarding CCN's compliance with the Personal Health Information Protection Act, 2004 and any other privacy legislation or Information and Privacy Commissioner of Ontario directives. Contact information for the Information and Privacy Commissioner of Ontario shall be included

2. Brochures and posters shall be located in a visible location at all CCN member hospitals and at the CCN head office. These brochures shall include:
    - An explanation of CCN's legal status as a Section 39(1)(c) Registry under the Personal Health Information Protection Act, 2004, and 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 the Personal Health Information Protection Act, 2004 to the Information and Privacy Commissioner of Ontario;
    - Contact information for CCN's Privacy Officer and the Information and Privacy Commissioner of Ontario;
    - Some of the administrative, technical, and safeguards used by CCN to protect personal health information;
    - A statement setting out that CCN will take all necessary precautions to protect personal health information from theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;
    - A list of the types of personal health information collected and the persons or organizations from which this personal health information is typically collected;
    - An explanation of the purposes for which personal health information is collected;
    - An explanation of 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
    - An explanation of 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.

3. CCN shall respond to inquiries and complaints from any individual.

4. The information made available to the public shall be accurate and current. If CCN's privacy and security policies change, the Privacy Officer shall be responsible for updating relevant information in the brochure and on www.ccn.on.ca.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The procedures for the audits of CCN's policy on the response to complaints and inquiries are set out in the CCN policy, "Privacy Inquiries and Complaints". Additionally, the Privacy Officer will review the information made available on the CCN website to ensure that it has been

updated to reflect new or amended policies. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

P3 – Statements of Purpose for Data Holdings Containing Personal Health Information

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	P3
Created:	**Effective:**	**Revised:**
May 4 2011	June 1 2011	-

Overview

This policy sets out the procedures for the creation and retention of statements of purpose for data holdings containing personal health information.

Background

Statements of purpose for data holdings containing personal health information provide general information about data holdings and justify their existence under PHIPA and CCN policy. Statements of purpose are useful because they allow us to more easily assess the need for each data holding. CCN's objective of limiting the number of its data holdings reflects CCN's general commitment to limiting the use and retention of personal health information.

Policy

1. All data holdings containing personal health information shall have statements of purpose. These statements of purpose must be created by CCN's Privacy Officer or a designate.

2. The Privacy Officer is ultimately responsible for these statements of purpose.

3. When creating statements of purpose for data holdings containing personal health information, the Privacy Officer or a designate shall utilize the standard form for statements of purpose. The standard form captures the following information:
    - The purpose of the data holding.
    - The location of the data holding.
    - The date that the data holding was first used for the retention of personal health information.
    - The personal health information contained in the data holding.
    - The source(s) of the personal health information.
    - The need for the personal health information in relation to the identified purpose.
    - The agents responsible for the statement's preparation.
    - The date that the statement was prepared.

- The agent responsible for the last review of the statement of purpose.
- The date of the last review.

4. The Privacy Officer or a designate may consult with clinical and/or IT staff at CCN in order to accurately and comprehensively assess the purpose of the data holding.

5. The Privacy Officer shall maintain a repository of statements of purpose for data holdings containing personal health information at CCN.

6. Copies of statements of purpose for data holdings containing personal health information shall be made available to CCN member hospitals. New or newly amended statements of purpose shall be communicated to hospitals as promptly as is reasonably possible.

7. In the course of a formal privacy and security review, the procedures for which are set out in the policy "Annual Review of Privacy and Security Policies and Procedures", the Privacy Officer shall review the repository of 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 may be destroyed 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.

8. In the course of the review, the Privacy Officer may consult with CCN's clinical and software development staff to assess the goals of the statements of purpose as they relate to CCN's identified purpose.

9. 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 the Personal Health Information Protection Act, 2004, CCN's privacy and security policies, and relevant IPC guidelines.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer will review the repository of statements of purpose for data holdings containing personal health information and consult with IT staff to determine whether or not the statements are current and accurate. The Privacy Officer or a designate will also, on a quarterly basis, audit the CCN shared hard drive for evidence of unauthorized personal health information. .

Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

P4 – Limiting Agent Access to and Use of Personal Health Information

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	P4
Created:	**Effective:**	**Revised:**
May 5 2011	June 1 2011	July 19 2013

Overview

This policy sets out the means by which CCN limits its agents' access to and use of personal health information. As a prescribed person under the Personal Health Information Protection Act, 2004, CCN has a responsibility to minimize that access and use.

Background

This policy is guided by the "need to know" principle. CCN's objective is to provide only the minimum amount of personal health information to its agents.

Policy

1. All CCN agents are prohibited from using personal health information or aggregate health information for research purposes.

2. CCN agents who have not been given written permission from the Privacy Officer are prohibited from accessing and/or using personal health information.

3. CCN must execute participation agreements with member hospitals that detail the hospitals' obligations to protect personal health information. CCN's Privacy Officer is responsible for ensuring that these agreements have been executed prior to their collection of personal health information on CCN's behalf.

4. Access to and/or use of personal health information should only be granted to CCN agents whose job description or contractual obligations include:
    - Inputting patient information into WTIS-CCN from a member hospital.
    - Assisting health information custodians at member hospitals.
    - Correcting records in WTIS-CCN.
    - Compiling patient and procedure information for reports in pursuit of improved care as set out in Section 45 of the Personal Health Information Protection Act, 2004.

- Aggregating or de-identifying records of personal health information so that they may be provided to researchers.

The above responsibilities must be significant components of an agent's day-to-day work.

5. Unless an agent requires access to personal health information for one of the purposes identified above, aggregate or de-identified personal health information shall be used in its place. The procedures for the aggregation and de-identification of personal health information are set out in the CCN policy, "Aggregation and De-Identification of Record-Level Data". The use of identifiable personal health information, where aggregate and/or de-identified personal health information could have sufficed, is prohibited.

6. Agents granted access to aggregate and/or de-identified personal health information are prohibited from attempting to reconstruct identifiable data from the aggregate and/or de-identified data. This includes trying to decrypt encrypted information, trying to identify an individual using unencrypted information, and trying to identify an individual based on prior knowledge.

7. The Privacy Officer shall determine whether or not an agent requires access to personal health information at the outset of the agent's relationship with CCN. The criteria for this determination are:
    - The agent making the request will routinely require access to and use of personal health information on an ongoing basis or for a specified period for his or her employment, contractual or other responsibilities.
    - The identified purpose for which access to and use of personal health information is requested is permitted by the Personal Health Information Protection Act, 2004 and its regulation.
    - The identified purpose for which access to and use of personal health information is requested cannot reasonably be accomplished without identifiable personal health information.
    - De-identified and/or aggregate information will not serve the identified purpose.
    - In approving the request, no more personal health information will be accessed and used than is reasonably necessary to meet the identified purpose.

8. The Privacy Officer or a designate shall maintain a list of agents granted access to personal health information.

9. CCN's Privacy Officer shall cancel an agent's access to personal health information upon the termination of the agent's relationship with CCN.

10. Should the responsibilities of an agent with access to personal health information change, the Privacy Officer shall review the justification for access. If it is determined that the agent's access to personal health information is no longer required, the Privacy Officer shall cancel the agent's access privileges.

11. Agents granted access to personal health information shall retain personal health information according to the procedures set out in the CCN policy, "Secure Retention of Personal Health Information".

12. Agents granted access to personal health information shall dispose of personal health information according the procedures set out in the CCN policy, "Destruction of Personal Health Information".

13. Privileged WTIS-CCN accounts must not be shared and must be segregated.

Enforcement

All CCN agents must comply with this policy. On a quarterly basis, the Privacy Officer or a designate will audit this policy by reviewing the log of agents granted access to personal health information to ensure that all agents on the list require access to personal health information. Additionally, the Privacy Officer or a designate will, on a quarterly basis, audit the CCN shared hard drive for evidence of unauthorized personal health information. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

P5 – Domain Account Retention Policy

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations, Director Information and Information Technology, CCN Staff	CCN	P5
Created:	**Effective:**	**Revised:**
November 2007	November 26, 2007	-

Overview

This policy provides guidelines regarding the retention of computer accounts for all CCN employees.

Policy

1. Computer accounts are a privilege, not a right. Violation of the CCN's privacy policies may result in the termination of computer account privileges by the Privacy Officer.

2. Active employees are eligible to retain their CCN's computer account as long as they remain in active status and follow CCN's privacy policies.

3. Computer accounts of employees who are no longer eligible to work at CCN will be disabled and deleted.

4. Accounts are deactivated, such that they are only accessible by the Privacy Officer and designated IT staff, one day after termination date/last-work-date (whichever is more recent).

5. Accounts are purged, such that all account data except emails and work still relevant to CCN's operations are deleted, 30 days from the employee termination date/last-work-date (whichever is more recent).

6. All employees' email and documents relevant to CCN are to be stored on the company's file server for an indefinite period.

7. If the employee's account does not contain any information relevant to the CCN, it shall be deleted.

CARDIAC CARE NETWORK

P6 – Disclosure of Aggregate and/or De-Identified Personal Health Information to Researchers

Developed by:	**Issued by:**	**Policy #:**
Director of Operations & Stakeholder Relations	CCN	P6
Created:	**Effective:**	**Revised:**
May 8 2011	June 1 2011	July 19 2013

Overview

CCN's mandate includes support for activities that improve the provision of health care in Ontario. To fulfill this part of its mandate, CCN will from time to time partner with researchers to use aggregate/de-identified data to produce recommendations for better care. Personal health information becomes aggregate/de-identified data when it is collapsed into undifferentiable aggregates or scrubbed of identifiable information.

Background

CCN's policy "Limiting Use, Disclosure, and Retention of Personal Health Information" states that CCN has zero-tolerance for the unauthorized disclosure of personal health information. However, it sets out that in accordance with CCN's identified purpose as a prescribed person committed to the improvement of the provision of health care in Ontario, aggregate and/or de-identified personal health information may be provided to researchers.

Policy

1. CCN agents are prohibited from providing researchers with identifiable records of personal health information.

2. Aggregate/de-identified data provided to researchers must be compliant with the CCN policy "Aggregation and De-Identification of Record Level Data".

3. The Research and Publication Committee (RPC) shall be responsible for determining which research proposals merit the disclosure of aggregate/de-identified personal health information.

4. The RPC shall be accountable to CCN for all issues related to the use of CCN data by external researchers and the publication of work based on those data.

5. The RPC shall communicate regularly and meet when circumstances dictate.

6. The RPC may grant access to aggregate/de-identified personal health information only to researchers who can satisfy at least one of the following criteria:
    - Researcher is affiliated with an established research institution.
    - Researcher is affiliated with a national or provincial association representing cardiovascular services or a funder or related organization (Ministry of Health, etc.).
    - Researcher is undertaking a PhD thesis.
    - Researcher is doing research supported by a grant from a recognized granting agency.
    - Researcher intends to publish in a peer-reviewed journal.
    - Researcher can provide compelling arguments to the RPC of the need for access to data.

7. Researchers interested in a topic shall complete and submit to the RPC the standardized form "Letter of Intent to Conduct a Study for Publication". This form shall be made available online.

8. Researchers with a specific research plan in mind must complete and submit to the RPC the standardized "Data Request Form". This form shall be made available online.

9. The RPC shall take into consideration the following factors:
    - Acceptable uses of the data (e.g., the research protocol is peer reviewed (if applicable) and demonstrates scientific merit).
    - Safeguards to protect the privacy of the data.
    - Terms and conditions of use (e.g. recognition of CCN in publications).
    - Responsibility for Research Ethics Board approvals, if applicable.
    - Turnaround times for providing data are reasonable.
    - Appeals process for denied requests.
    - CCN cost to provide the data.

10. The Privacy Officer or a designate shall maintain a log of approved, denied, and pending requests for aggregate/de-identified personal health information for the purposes of research. This log shall record the reasons for a request's approval or denial, as well as the dates of the request and of the Research and Publication Committee's decision.

11. Upon approval of the disclosure of aggregate and/or de-identified data for research purposes it is the Privacy Officer's responsibility to ensure a Non-Disclosure Agreement will be executed with the researcher, or in the case of ICES researchers, ensure that CCN's Data Sharing Agreement with ICES is amended to cover the project in question. These agreements require the researcher to agree to not use the de-identified and/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.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer or a designate will review aggregate/de-identified personal health information that has been provided to researchers to ensure that the above procedures have been followed. Additionally, the Privacy Officer will review the log of approved, denied, and pending requests for access to aggregate/de-identified personal health information for research purposes. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be taken as per that agreement.

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

CARDIAC CARE NETWORK

P7 – Policy and Procedures for the Execution of Agreements with Third Party Service Providers with Respect of Personal Health Information

Developed by:	**Issued by:**	**Policy #:**
Director of Operations & Stakeholder Relations	CCN	P7
Created:	**Effective:**	**Revised:**
July 5 2011	August 1 2011	July 19, 2013

Overview

This policy sets out the procedures for the execution of agreements (i.e. contracts, service level agreements, etc.) with third party service providers.

Background

Agreements with third party service providers help to ensure that both parties understand the measures that must be taken to ensure that the personal health information in CCN's custody or control is protected from being compromised. Additionally, formal agreements give CCN legal protection against negligence on the part of the third party.

This policy makes some distinctions between agreements made with electronic service providers and all others. Under PHIPA, electronic service providers are those service providers whose primary contracted duty is to use electronic means to collect, use, modify, disclose, retain, or dispose of personal health information.

Policy

1. CCN must enter into an agreement with a third party service provider in respect of personal health information prior to permitting a third party service provider to access or use the personal health information in CCN's custody.

2. Agreements with third party service providers in respect of personal health information shall clearly outline roles and responsibilities in respect in order to ensure accountability.

3. The requirements set out in the template agreement provided at the end of this policy document must be satisfied for all agreements with third party service providers.

4. CCN's Privacy Officer is responsible for ensuring that agreements with third party service providers have been executed prior to any third party service provider being permitted access to or use of personal health information.

5. Prior to the execution of agreements with third party service providers, CCN's Privacy Officer must ensure that
    - The service provided by the third party in respect of personal health information is absolutely necessary for CCN's mandate under the Personal Health Information Protection Act, 2004;
    - 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
    - The service provided by the third party does not require any more personal health information than is absolutely necessary for the provision of that crucial service.

    Only when these requirements have been satisfied may the Privacy Officer proceed with the execution of an agreement with a third party service provider.

6. The transfer of personal health information to the third party provider must be compliant with the CCN policy "Secure Transfer of Personal Health Information". 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.

7. 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 shall contact the third party provider to seek an explanation and the certificate. If the Privacy Officer is not satisfied with the third party's response or if there is no response after two days, they shall provide notification to CCN's Chief Executive Officer. CCN may seek legal action against the third party at this point.

8. Agreements with IT service providers shall require the third party to provide detailed technical and architecture documentation.

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

Template Agreement

Agreements executed with third party service providers must include all of the stipulations set out in this template**.**

General Provisions

- A description of the status of CCN under the Personal Health Information Protection Act, 2004 and CCN's duties under the Personal Health Information Protection Act, 2004.
- 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 the Personal Health Information Protection Act, 2004 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 the Personal Health Information Protection Act, 2004.
- 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 the Personal Health Information Protection Act, 2004 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 personal 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, "Limiting Use, Disclosure, and Retention of 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 the Institute for Clinical Evaluative Studies pursuant to a data sharing agreement and to CCN member hospitals requesting personal health information that was collected on site). 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 unless 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 can be transferred by the third party.
- Indications of to whom personal health information can 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 its receipt of personal health information.
- 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 ways, 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 documentation relating to the transfer of personal health information 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 complies with 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 the Personal Health Information Protection Act, 2004.
- 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 the Personal Health Information Protection Act, 2004 and its regulation.
- A statement setting out the time frame within which 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 personal health information.
- A stipulation that the third party must set out the method by which its agents will be made aware of the terms of the agreement (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 to 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.
- A copy of the written agreement between the third party and the subcontractor must be provided to CCN.

Notification

- A stipulation that the third party must notify CCN's Privacy Officer, in written format, at the 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 compromised.
- 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 of auditing that will be provided to the third party.

Enforcement

All CCN agents must comply with this policy. The Privacy Officer shall review documentation related to the ongoing services provided by the third party to ensure that the procedures of this policy and the provisions of the agreement are being adhered to. Should the Privacy Officer determine that a third party service provider has not complied with the terms of the agreement, he/she may seek to terminate the agreement or seek legal action as circumstances dictate. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

P8 – Aggregation and De-Identification of Record Level Data

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	P8
Created:	**Effective:**	**Revised:**
August 2008	August 2008	April 25 2011

Overview

This policy describes the procedures and safeguards employed to ensure that aggregate or de-identified personal health information can be produced for researchers safely and securely.

Background

Aggregation of data is the process by which data sets are created through the collation of patient records. The results are data sets that can show characteristics of a particular group without showing the personal health information of any one individual. De-identification of data is the process by which data elements that could be used to identify an individual are removed from personal health information, leaving only the minimum information needed for a particular purpose. The 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 the Personal Health Information Protection Act, 2004.

Policy

1. Personal health information may not be used or disclosed for any purpose, except to the Ontario Institute for Clinical Evaluative Studies under the terms of its data sharing agreement with CCN or to hospitals requesting personal health information collected on site, if aggregate or de-identified personal health information will serve the same purpose.

2. 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, postal code, telephone number.

3. Partial de-identification of record level data is sometimes required to support the requirements of specific research. For example, geographic studies require some ability to aggregate data by location. In this case part of a postal code or the name of a province, city or county may be required. The provision of partially de-identified data to researchers is conditional on their signing a Confidentiality and Non-Disclosure Agreement. In general, the following elements of data should be removed:
    - Patient health insurance number;
    - Patient name, middle name and surname;
    - Patient chart and/or medical record numbers;
    - Medical report numbers and/or specimen accession numbers;
    - Patient address, city/town, province;
    - Patient telephone numbers;
    - Last three characters of the postal code.

4. If cells of personal health information contain the records of fewer than five patients, the disclosure of aggregate/de-identified personal health information is forbidden.

5. Aggregate or de-identified personal health information will be reviewed by CCN's Privacy Officer or a designate prior to its disclosure.

6. 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.

7. A log of researchers who request access to aggregate/de-identified personal health information shall be kept by the Director of Clinical Quality and Performance. This log shall record the reasons for a request's approval or denial, as well as the dates of the request and of the Research and Planning Committee's decision. This log shall include an indication as to whether or not the researcher has executed a Confidentiality and Non-Disclosure Agreement.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer or a designate will review aggregate/de-identified personal health information that has been provided to researchers to ensure that the above procedures have been followed. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and, depending on the circumstances, may recommend that an

agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

P9 – Policy and Procedures for Privacy and Security Auditing

Developed by:	**Issued by:**	**Policy #:**
Director of Operations & Stakeholder Relations	CCN	P9
Created:	**Effective:**	**Revised:**
August 2008	August 2008	July 31 2012

Overview

This policy sets out the procedures for completing privacy and security audits at CCN.

Background

Privacy and security audits are used to ensure compliance with CCN's privacy and security policies, privacy legislation, and its general objective of completely protecting the personal health information in its custody and/or control.

Policy

1. CCN will perform formal audits of its privacy and security program at least quarterly. Some audits will be undertaken more frequently. Formal audits may also be conducted upon the request of the IPC or other government entity, as a result of a privacy impact assessment, or upon recommendation following a privacy or security breach (as defined in the CCN policy, "Information Security and Privacy Breach Management").

2. The Privacy Officer is ultimately responsible for the completion of privacy and security audits, but may delegate that responsibility to another CCN agent. In such cases, the designated CCN agent will report to the Privacy Officer. For audits of policies that place positive duties on the Privacy Officer alone, the agent responsible for completing the audit will be named below.

3. Formal, comprehensive audits must include at least the following:
    - Audit of aggregate/de-identified data provided to researchers.
        - Purpose: to ensure that aggregate/de-identified data provided to researchers have been properly scrubbed of data and do not include cells with fewer than five patient records in contravention of the CCN policy, "Aggregation and De-Identification of Record Level Data".
        - Nature and scope: the Privacy Officer or a designate shall review data that have been aggregated/de-identified.

- Audit of the logs of agents with whom CCN has executed Confidentiality and Non-Disclosure Agreements
    - Purpose: to ensure that all individuals employed by CCN or with whom CCN has a contractual or other relationship which may expose them to corporate or personal health information, have signed a current Confidentiality and Non-Disclosure Agreement at the outset of their employment or have signed the Agreement within the last year.
    - Nature and scope: the Privacy Officer or a designate shall compare the log of agents who have signed Confidentiality and Non-Disclosure Agreements with the log of CCN employees and individuals with whom CCN has a contractual or other relationship which may expose them to corporate or other information. The Privacy Officer or his/her designate shall seek to identify individuals who should have signed a Confidentiality and Non-Disclosure Agreement, but have not.

- Audit of CCN shared drive for unauthorized personal health information
    - Purpose: to identify personal health information being stored on CCN's shared hard drive in contravention of the following CCN policies: "Secure Retention of Personal Health Information," "Information Security and Privacy Breach Management," "Secure Transfer of Personal Health Information," "Limiting Agent Access to and Use of Personal Health Information," "IT Policy: E-mail, Internet, and Computing Devices," and "Statements of Purpose for Data Holdings Containing Personal Health Information."
    - Nature and scope: the Privacy Officer or a designate will search the drive for certain strings often found in records of personal health information such as "DATE OF BIRTH," "SEX," "FIRST NAME," and others. The search results will be reviewed, and the auditor will seek to identify evidence of personal health information.

- Audit of the log of agents granted access to personal health information
    - Purpose: to ensure that all agents granted access to personal health information have a definite and clearly articulated need to do so. This will ensure compliance with the CCN policy, "Limiting Agent Access to and Use of Personal Health Information".
    - Nature and scope: the Privacy Officer or a designate will review the log of agents granted access to personal health information. The auditor will seek to identify agents who have no definite and clearly articulated need to access personal health information.

- Audit of the log of agents who have completed privacy and security training.

- Purpose: to ensure that all CCN agents have completed the online privacy and security training program in accordance with the CCN policy, "Privacy and Security Training".
- Nature and scope: the Privacy Officer or a designate will review the log of agents who have and have not completed privacy and security training. The auditor will seek to identify individuals with whom CCN has a relationship and who have not completed privacy and security training.

- Audit of repository of statements of purpose for data holdings containing personal health information.
  - Purpose: to ensure that all CCN data holdings containing personal health information have current and accurate statements of purpose in accordance with the CCN policy, "Statements of Purpose for Data Holdings Containing Personal Health Information".
  - Nature and scope: the Privacy Officer or a designate shall review the statements of purpose contained in the repository. The auditor shall seek to identify data holdings that are no longer required for CCN's identified purposes or inaccuracies in statements of purpose for data holdings that remain necessary.

- Review of information made available on CCN's website and included in the brochure distributed to hospitals.
  - Purpose: to ensure that the information about CCN's privacy and security program provided to the public is comprehensive, updated, and accurate in accordance with CCN's policy, "Transparency of Privacy and Security Policies and Procedures".
  - Nature and scope: the Privacy Officer or a designate shall review the information made available on CCN's website and included in the brochure distributed to hospitals. The auditor will seek to identify in the brochure information that does not accurately reflect the most current privacy and security policies at CCN. The auditor will also ensure that all CCN privacy and security policies, including new ones, have been made available on the CCN website and are the most current versions.

- Review of logs kept for the purposes of securing the physical security of the CCN provincial office.
  - Purpose: to ensure that the procedures of the CCN policy "Physical Security", which call for various CCN agents to keep logs of agents granted access to the office, agents granted access to the secure server room, and alarms and security calls (provided by building security), are followed.

  - Nature and scope: the Privacy Officer or a designate shall review the logs described above. The auditor shall seek to identify suspicious activity or any instances in which the logs were not completed accurately.

- Review of documentation related to the reception and response to privacy and security inquiries and complaints.
  - Purpose: to ensure that CCN's procedures on the reception of and response to privacy complaints and inquiries, which allow the public to hold CCN accountable to its principles and provincial legislation, are uniformly followed. CCN aims to ensure total compliance with its policy, "Privacy Inquiries and Complaints".
  - Nature and scope: the Privacy Officer or a designate shall review the log of all complaints and inquiries submitted to CCN. The auditor shall seek to identify cases in which complaints or inquiries were not responded to within the allowed timeframe of one week. The auditor shall also review the logs of action taken in the event that the Privacy Officer has determined that a complaint in fact identifies a breach of or deficiency in CCN's privacy and security program. The auditor shall seek to ensure that all of the procedures and timeframes set out in the CCN policy "Privacy Inquiries and Complaints" have been followed.

- Review of documentation related to the formal review of privacy and security policies.
  - Purpose: to assess CCN's compliance with its policy regarding the formal review of privacy and security policies. Compliance with this policy ("Annual Review of Privacy and Security Policies and Procedures") is necessary to ensure that CCN's policies keep abreast of formal recommendations and advancements in industry standards, technology, and privacy legislation.
  - Nature and scope: the Director of Communications shall review the Form for Formal Review of Privacy and Security Policies and Procedures that was completed by the Privacy Officer at the time of the last review. The auditor shall seek to identify instances in which reviews of policies were not conducted or not properly documented.

- Review of Consolidated Log of Recommendations.
  - Purpose: to ensure that the Consolidated Log of Recommendations is regularly updated and that its entries are being addressed in accordance with the CCN policy, "Maintaining a Consolidated Log of Recommendations".
  - Nature and scope: the Director of Communications shall review the timeframes and action points set out for each entry in the consolidated log of recommendations and compare it to actions that have in fact been taken. The auditor shall seek to identify recommendations that have not been addressed.

The auditor shall also ensure that no recommendations made in any form (listed in the policy, "Maintaining a Consolidated Log of Recommendations") have been omitted from the Log.

- Review of documentation related to the transfer of records of personal health information for disposal.
    - Purpose: to ensure that the third party service provider responsible for the disposal of records of personal health information in paper format has sent certificates within the specified timeframe in accordance with the CCN policy, "Destruction of Personal Health Information" and the contractual agreement. Additionally, this audit will ensure that the inventory of personal health information being transferred for the purpose of disposal is being maintained.
    - Nature and scope: the Privacy Officer or a designate shall review the repository of certificates of destruction received from the third party service provider and the inventory of personal health information transferred for disposal. The auditor shall seek to ensure that the third party service provider has been diligent in sending certificates confirming the destruction of records of personal health information in paper format. Additionally, the auditor shall seek to identify instances in which the inventory of personal health information transferred to the third party service provider for disposal has not been properly maintained.

4. If in the course of completing one of these audits, the auditor suspects that a breach (as defined in the CCN policy, "Information Security and Privacy Breach Management") has occurred, the procedures from that policy must be followed.

5. If in the course of completing one of these audits, the auditor identifies a deficiency in the CCN privacy and security program, the auditor shall order a review of the policy. The procedures found in the CCN policy "Annual Review of Privacy and Security Policies and Procedures" should then be followed.

6. If a privacy or security audit does not identify a deficiency in CCN's privacy and security program, notification to that effect will be provided by the Privacy Officer to CCN agents in written format within one week. In the event that a privacy or security audit does in fact identify a problem, the CEO must be notified by the Privacy Officer in written format as quickly as is reasonably possible.

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

CARDIAC CARE NETWORK

P10 – Information Security and Privacy Breach Management

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	P10
Created:	**Effective:**	**Revised:**
December 2009	April 1 2010	July 31 2012

Overview

This policy describes the procedures for information security and privacy breach management. Additionally, it sets out the procedures for investigations to be undertaken in the aftermath of a breach.

Background

A breach occurs in any of the following circumstances:

- The collection, use and disclosure of personal health information that is not in compliance with the Personal Health Information Protection Act, 2004 or its regulations;
- A contravention of the privacy policies, procedures or practices implemented by the prescribed person or prescribed entity;
- A contravention of Data Sharing Agreements, Research Agreements, Confidentiality Agreements and Agreements with Third Party Service Providers retained by the prescribed person or prescribed entity; and
- Circumstances where 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.

It is CCN's objective to minimize the negative impact of a breach should one occur and to take corrective action to prevent further breaches.

Policy

1. If any CCN agent suspects that a breach has occurred, he/she must report this suspicion to the Privacy Officer, in written or oral format, as soon as is possible. The agent must tell the Privacy Officer when the suspected breach took place and report the scope of the suspected breach.

2. The agent must then complete CCN Privacy Breach Management Form in cooperation with the Privacy Officer. The Privacy Breach Management Form will record, at minimum, the following:
    - The date of the privacy breach;
    - The date that the privacy breach was identified or suspected;

- Whether the privacy breach was internal (personal health information compromised, but exposure limited to unauthorized CCN agents) or external (personal health information exposed to wider public);
- 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 or prescribed entity 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.

3. The Privacy Officer will then determine if a breach has in fact occurred, and if so, if personal health information has been compromised.

4. If personal health information has been compromised, the Privacy Officer must notify CCN's Chief Executive Officer in written format as soon as is reasonably possible.

5. If a breach has occurred, CCN's Privacy Officer will take the appropriate measures to isolate the breach and prevent a reoccurrence. Depending on the circumstances, these measures will include:
    - The Privacy Officer will ensure that no copies of compromised personal health information have been made.
    - If copies have been made, the Privacy Officer will retrieve and dispose of all copies in a secure manner as set out in the CCN policy, "Destruction of Personal Health Information".
    - The Privacy Officer will obtain written confirmation that copies have been disposed of in a secure manner, including the time and date of the disposal.
    - The Privacy Officer will ensure that no further breaches can take place through the same means.
    - The Privacy Officer will determine whether the breach would allow access to any other personal health information.
    - The Privacy Officer will take action to prevent any additional breaches.

6. The Privacy Officer is responsible for reviewing the actions taken to contain the breach to ensure their efficacy.

7. If personal health information has been compromised, the Privacy Officer must consult with privacy staff at hospital that was the source of the compromised information. Health information custodians at affected hospitals may notify the patients to whom the compromised personal health information relates pursuant to subsection 12(2) of the Personal Health Information Protection Act, 2004.

8. The Privacy Officer, in the course of his/her investigation, may undertake interviews and site inspections to document the scope and depth of the issues that led to the breach.

9. The Privacy Officer is responsible for setting a timeline for addressing recommendations arising from investigation, assigning agents to address recommendations, monitoring recommendations, and is ultimately responsible for their implementation

10. The Privacy Officer will maintain a log of all completed Privacy Breach Management Forms. Recommendations made in this format will be added to the Consolidated Log of Recommendations.

Enforcement

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

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

CARDIAC CARE NETWORK

P11 – Privacy Inquiries and Complaints

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	P11
Created:	**Effective:**	**Revised:**
July 2008	November 1 2008	April 25 2011

Overview

This policy sets out the procedures for responding to complaints and inquiries from the public about CCN's privacy and security policies and compliance with the Personal Health Information Protection Act, 2004. CCN is committed to public transparency and will respond to any inquiry or complaint made by an individual.

Background

An individual will be able to submit to the designated individual or individuals at Cardiac Care Network of Ontario (CCN) complaints and/or inquiries about CCN's privacy and security program. The designated Privacy Officer for CCN is the Director of Operations and Stakeholder Relations; in this person's absence, challenge/enquiry should be directed to the Director of Communications. The Chief Executive Officer, or the designated manager, will handle inquiries/challenges in the absence of the Director of Operations and Stakeholder Relations and the Director of Communications. "Complaints" are defined as "concerns or complaints relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the Personal Health Information Protection Act, 2004 and its regulation". "Inquiries" are defined as "inquiries relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the Act and its regulation".

Policy

1. CCN will respond to any complaints or inquiries from any individual. The Privacy Officer will to the best of his/her ability respond to inquiries to the satisfaction of the individuals who submit inquiries within one week.

2. All complaints will be assessed by the Privacy Officer.

3. If the Privacy Officer determines that the complaint does not in fact identify a deficiency in or breach of CCN's privacy and security program, he/she will respond to the individual who submitted the complaint within one week explaining why an investigation was not undertaken.

4. If the Privacy Officer determines that the complaint does in fact identify a deficiency in or breach of CCN's privacy and security program, he/she will notify the individual who submitted the complaint and launch an investigation within one week.

5. If there has been a breach, as defined in "Information Security and Privacy Breach Management", the procedures in that policy will be followed.

6. The Privacy Officer is responsible for setting the parameters of the investigation, including time frame and scope.

7. Upon the completion of the investigation, the Privacy Officer will inform the individual who submitted the complaint of the steps that CCN has taken to resolve the problem.

8. All complaints and inquiries will be tracked and logged using the Privacy Complaints Template.

9. The Privacy Officer will maintain a log of all complaints and inquiries.

10. All challenges should be directed to CCN's Privacy Officer, where the challenge is documented and investigated further, and appropriately referred onwards, if appropriate.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. Audits of this policy involve the Privacy Officer's review of completed and ongoing investigations of legitimate complaints. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

Contact Information for CCN Privacy Officer:
4100 Yonge Street
Suite 502
Toronto ON
M2P 2B5
416-512-7472
Email: mail@ccn.on.ca

Contact Information for the Information and Privacy Commissioner/Ontario:
Information and Privacy Commissioner/Ontario
2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Web: www.ipc.on.ca
Telephone: Toronto Area (416/local 905): 416-326-3333
Long Distance: 1-800-387-0073 (within Ontario)
Email: info@ipc.on.ca

CARDIAC CARE NETWORK

P12 – Privacy Impact Assessments

Developed by:	Issued by:	Policy #:
CCN Privacy Officer	CCN	P12
Created:	**Effective:**	**Revised:**
July 2014	August 1, 2014	

Overview

This policy sets out the procedures for ordering, carrying out, and documenting privacy impact assessments (PIAs).

Background

It is good practice every few years, and whenever a new information system containing personal health information under CCN's custody is inaugurated, for privacy impact assessments to be carried out. These assessments, typically conducted by third-party legal professionals, are designed to ensure that privacy and security programs comply with applicable privacy legislation, related regulations, and guidelines issues by privacy regulators such as the Information and Privacy Commissioner of Ontario. Privacy impact assessments may also apply industry best practices to ensure that personal health information under CCN's custody is protected against all reasonable risks. This policy has been prepared with regard to the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act* and the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, both published by the Information and Privacy Commissioner of Ontario.

Policy

1. Privacy impact assessments must be conducted on existing and proposed data holdings involving personal health information and whenever the implementation of a new or a change to an existing, information system, technology or program involving personal health information is contemplated.

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

3. For existing data holdings containing personal health information, privacy impact assessments must be conducted every three years at minimum. The assessments should be conducted in advance of the three-year review by the Information and Privacy Commissioner of Ontario. The

Privacy Officer is responsible for establishing a three-year timetable and ensuring that the timetable is adhered to.

4. Privacy impact assessments are not required to be conducted on updates to user portals for the WTIS-CCN as long as the updates do not affect the storage or transfer or personal health information or rules regarding access to the WTIS-CCN. The Privacy Officer is responsible for reviewing updates to the WTIS-CCN to ensure that these aspects are not affected by the updates.

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

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

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

    - The data holding, information system, technology or program at issue;
    - The nature and type of personal health information collected, used or disclosed or that is proposed to be collected, used or disclosed;
    - The sources of the personal health information;
    - The purposes for which the personal health information is collected, used or disclosed or is proposed to be collected, used or disclosed;
    - The reason that the personal health information is required for the purposes identified;
    - The flows of the personal health information;
    - The statutory authority for each collection, use and disclosure of personal health information identified;

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

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

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

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

    - A description of the data holding, information system, technology, or program involving personal health information at issue;
    - The date that the privacy impact assessment was completed or is expected to be completed;
    - The agent responsible for completing or ensuring the completion of the privacy impact assessment;
    - The recommendations arising from the privacy impact assessment;

- The agent responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed;
- The manner in which each recommendation was or is expected to be addressed.

11. In a separate section of the log of privacy impact assessments, there shall also be a log of data holdings involving personal health information and of new or changes to existing information systems, technologies, or programs involving personal health information for which privacy impact assessments have not been undertaken. For each such data holding, information system, technology or program, the log shall either set out the reason that a privacy impact assessment will not be undertaken and the agent responsible for making this determination or set out the date that the privacy impact assessment is expected to be competed and the agent responsible for completing or ensuring the completion of the privacy impact assessment.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. Audits of this policy involve the Privacy Officer's review of completed and ongoing investigations of legitimate complaints. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

SECURITY POLICIES AND PROCEDURES

S1 – Physical Security

Developed by:	**Issued by:**	**Policy #:**
Director of Operations & Stakeholder Relations	CCN	S1
Created:	**Effective:**	**Revised:**
April 25 2011	June 1 2011	July 19 2013

Overview

This policy governs the methods used by CCN to secure the physical premises of its provincial office. Securing the physical premises is necessary to ensure that CCN agents are safe and the personal health information in CCN's custody is protected.

Definitions

Access Card – All staff members are provided with a CCN access card that combines the Yonge Corporate Centre "after-hours" access card with the CCN security access to suite 502. Each access card is numbered and is linked to a specific staff member.

Activated Security System – When the security system is activated, building security responds to all alarms generated as per the Yonge Corporate Centre alarm procedure.

De-activated Security System – When the security system is de-activated, the building security will not respond to alarms generated.

Password – Specific Designated CCN staff members will have security passwords to activate and de-activate the alarm code in the LAN/Server Room. Passwords are unique to each staff member, are not to be shared, and are only known by the individual. Interface Technologies Inc., CCN's Network Support Provider, will also have a unique password. Each designated staff member will determine his/her own password, and the CEO, Director Operations & Stakeholder Relations, and the Director Informatics & Business Intelligence will have the main override code.

Business Hours of Operation – The CCN's business hours of operation are from 8:30 a.m. to 5:00 p.m. Monday to Friday.

Access to CCN

It is the Cardiac Care Network's policy to ensure that appropriate security systems and procedures are in place to maintain the security and privacy of patient information and work-related documents. Visitors to CCN should be accompanied by a member of the CCN staff and escorted to the designated meeting area. Given the large number of meetings taking place at CCN it is important that staff is vigilant at all times about visitors being present in the office.

Policy – General

1. CCN is not a public access office. Therefore, the CCN external doors are kept locked at all times. The public does not have access to the CCN suites unless accompanied by a CCN staff member.

2. The landlord has unrestricted access to the CCN's suites as per the terms of the lease. However, a CCN staff member or Yonge Corporate Centre staff member is required to be on site at all times when external contractors and/or guests are present, except in emergency situations (e.g., security calls, fire, building damage).

3. CCN's Privacy Officer will maintain a log of agents granted access to the CCN provincial office premises. This log shall record 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 and keys and/or were provided.

Staff Access

1. Staff will access the CCN suites via the main 502 entrance using their own access card.

2. Staff will exit the CCN Suites via the main 502 entrance or via the back entrance between the hours of 8:30 am and 5:30 pm.

3. During normal business hours of operation, the front door and the back door alarms will be de-activated, unless the building security is otherwise advised.

4. Staff entering the CCN office with their access card after hours will not generate an alarm. Exiting the office through the main door after business hours will not generate an alarm, as the motion detector disables the alarm upon exiting. However, exiting the office through the back door will generate an alarm after 5:30 pm.

5. IT Staff are responsible for arming and disarming the LAN/Server Room alarm on a daily basis. Interface Technologies Inc. has a pass code in case of work after hours.

6. Only the Director of Operations & Stakeholder Relations will be responsible for changing alarm codes, security cards and key distribution. A log of alarms and calls will also be provided to CCN by building security as required.

Visitors

1. A "visitor" is defined 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.

2. Visitors to CCN must be admitted to the suite by a CCN staff member. Visitors will announce themselves by ringing the bell at the main 502 door, and CCN reception or a staff member can press the release button located at the front reception desk to admit the visitor.

3. Unexpected or unrecognized visitors are not to be admitted into the CCN office.

Committee Member Meetings

1. Committee members will enter the CCN suites for their meetings via the main 502 doors.

2. If the committee meeting is scheduled outside of normal business hours, security is pre-notified.

3. Committee members should exit via the main 502 doors during or after the meeting.

Cleaning and Maintenance

1. All routine housekeeping and maintenance will occur during normal business hours and is currently scheduled for 3:30 to 4:30 p.m.

2. For housekeeping and maintenance that is required to be completed outside of normal business hours of CCN staff, the Yonge Corporate Centre charges a fee. This is subject to approval by the Director Operations & Stakeholder Relations. There is a fee for housekeeping outside of the routine maintenance and housekeeping time of 3:30 to 4:30.

Securing Work Areas

Ensuring the security of work areas is fundamental to the physical security of the CCN provincial office premises.

Policy

1. Outside of normal business hours, all confidential material, including all files, documents, and papers containing personal health information shall be maintained in locked filing cabinets.

2. Desks and workstations must be kept clean of confidential/work-related documents at the end of the business day.

3. Desks/drawers are to be locked after working hours.

4. Laptops/PCs are to be turned off after hours and laptops secured to the desks unless the staff member plans to access Citrix after hours – in that case the computer should be left on with password protected access.

5. Doors are to be locked upon exit from the employee's own office.

Key Access and Control

CCN controls access to its suite in the Yonge Corporate Centre by giving access cards only to employees.

Policy

1. Upon commencement of employment, staff will be issued security cards to the CCN office, as well as key to relevant office filing cabinets. The access card and keys are the responsibility of the employee at all times. Upon termination of employment, all access cards and keys are to be returned to the Privacy Officer or delegate, and the "last day checklist" completed.

2. Copies of the CCN office keys are kept: a) on the building "Grand Master" keys as per fire code regulations and b) with the Building Security Manager (Kevin Wylie, Manager Security and Life Safety as of July 19/2013). Tracey Lynch and Rose Obien also have access to suite keys.

3. CCN agents who have lost or misplaced access cards must report, in oral or written format, to the Privacy Officer immediately. Subsequently, the Privacy Officer will notify Cadillac Fairview security staff, who will deactivate the access card and provide a new card at a fee of $15.

4. Only staff who require access to the server room for the purposes of fulfilling the conditions of their job description or other contractual obligations will be granted access by CCN's Privacy Officer. The Privacy Officer will maintain a log of CCN agents granted access to the server room.

Alarm Generation and Response

An alarm is generated on the 502 main door outside of normal hours of operation due to forced entry and/or the door being held open for longer than 30 seconds. Exiting the 502 door at any time will not generate an alarm, as the door has a motion detector that disables the alarm on exiting. A door held open for longer than 30 seconds will generate an internal warning alarm to notify CCN staff and building security.

An alarm is generated on the back door outside of normal hours of operation due to any entry including entry using a key, exiting, and door held open for longer than 30 seconds.

Alarms are generated in the server room when the system is activated by any motion in the room; increase in temperature above 32 degrees; and entry into the server room without de-activating the alarm keypad.

Response to Alarm

1. The building security will respond to alarms according to the protocol set out by the Yonge Corporate Centre and CCN requirements.

2. An audible sound is generated in the office when an alarm is generated to notify staff.

3. Alarms generated during normal business hours of operation:
    a. All alarms generated by the main 502 door and the back door during normal business hours of operation are disregarded by the security company unless otherwise advised.
    b. Alarms generated by the server room – the building security will contact the CCN office before dispatching a security officer. If the CCN office cannot be reached, a security guard will be dispatched.

4. Alarms generated outside of normal business hours of operation:
    a. Response by building security who also patrol all floors regularly.
    b. The building security will respond to all alarms generated outside of normal business hours of operation.
    c. If the alarm is due to a false alarm, or there is no obvious reason for the alarm and the premises are secure, the Director Operations & Stakeholder Relations will not be called. The building security will leave a written report documenting the alarm and the response.
    d. If the alarm is activated due to a real forced entry, a critical function alarm (temperature sensor), the Director Operations & Stakeholder Relations will be contacted. If the

Director Operations & Stakeholder Relations cannot be reached, the building security will continue to attempt to reach the other contacts on the response list in order.

5. First Response:
    a. All Directors and the CEO will participate in the first response.
    b. The Director Operations & Stakeholder Relations will be required to come to the CCN office, after the office has been secured for forced entry, a critical function alarm, and a power failure.

6. In the event that a false alarm is generated, a CCN staff member will notify the building security immediately to cancel the alarm.

Security Reports

The security staff of Yonge Corporate Centre can prepare reports on the security of the CCN provincial office premises.

Policy

Security reports can be requested from the building security upon request or according to a schedule. The report will provide a list of names, dates, and times the CCN office or the perimeter building has been accessed. The report can be generated on a daily, weekly or monthly basis at no cost.

Staff Training and Orientation

It is CCN's policy that new staff be oriented to the security system and the related security policy and procedures.

Policy

Upon employment, staff will be provided an orientation to the security system and the security policies and procedures by the Director of Operations & Stakeholder Relations. The employee and their supervisor will sign the orientation check list indicating the completion of this orientation.

Access to Secure Server Room

The personal health information in the custody of CCN is kept in the secure server room on the premises of the CCN provincial office. It is the Cardiac Care Network's policy to ensure that appropriate security systems and procedures are in place to maintain the security and privacy of patient information and work-related documents.

Policy

1. Only the CCN IT staff and Directors have access to the server room and the server room pass codes. Only the CEO and the Director of Operations & Stakeholder Relations will have the main override code.

2. IT Staff are responsible for arming and disarming the LAN/Server Room alarm on a daily basis. Interface Technologies Inc. has a pass code in case of work after hours.

3. Only the Director of Operations & Stakeholder Relations will be responsible for changing alarm codes, security cards and key distribution. A log of alarms and calls will also be provided to CCN by building security as required.

4. Alarms are generated in the server room when the system is activated by any motion in the room; increase in temperature above 32 degrees and entry into the server room without de-activating the alarm keypad.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer or a designate will, on a quarterly basis, review the logs described above. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

S2 – Secure Retention of Personal Health Information

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	S2
Created:	**Effective:**	**Revised:**
April 25 2011	June 1 2011	-

Overview

This policy governs the secure retention of personal health information. CCN is committed to ensuring that the personal health information in its custody and/or control is protected and is only used for CCN's identified purposes.

Background

CCN retains personal health information on one database server and one archive server in its locked server room. The safeguards for the physical security of personal health information in CCN's custody are set out in the CCN policies, "WTIS-CCN Application Security" and "Safeguards for Personal Health Information".

Policy

1. All personal health information must be stored within the locked server room on the database server or archive server.

2. Agents are prohibited from retaining personal health information on mobile devices, paper, optical media, or other media except the database server and archive server in the locked server room.

3. Records of personal health information may be retained only for as long as is reasonably necessary

4. Any data sharing agreement will govern the retention of records of personal health information that relate to that agreement. If the data sharing agreement is ended for any reason, this policy will then apply to those records of personal health information. Personal health information may not be retained for periods longer than those set out in data sharing agreements.

5. 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.

6. Personal health information will be transferred to a third party service provider for long-term tape backup. Long-term tape backup ensures that the CCN database is secure in the event of a disaster affecting the database held at CCN's provincial office.

7. Tape backups will 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 returned to the Supervisor of Database/Application development upon request.

8. The Supervisor of Database/Application Development must 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.

9. The Supervisor of Database/Application Development must 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.

10. Zoning network principles including a segregated public Wi-Fi network, Operation Zone, and Restricted Zone for servers and infrastructure must be implemented. The Privacy Officer and IT Team may consult federal standards (ITSG-22) to ensure that this requirement is met.

11. CCN IT Staff shall apply Request Filtering and URL Rewrite in the CCN Application so as to mitigate vulnerabilities to threats such as SQL injection.

12. Error messages in the CCN Application shall be as generic as possible, and not display version information to end users.

13. CCN's IT team shall develop and implement standard hardening procedures including a standard configuration for all servers and workstations, regular vulnerability scans, and use JIRA to track request and change management.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer or a designate will, on a quarterly basis, audit the CCN shared hard drive for evidence of unauthorized personal health information. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken.

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

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

CARDIAC CARE NETWORK

S3 – Secure Transfer of Personal Health Information

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	S3
Created:	**Effective:**	**Revised:**
April 2010	April 1 2010	July 13, 2013

Overview

This policy describes the methods utilized for transferring personal health information securely. Personal health information is transferred to CCN by Cancer Care Ontario, the agent responsible for hosting the WTIS-CCN application. Health information custodians at CCN's member hospitals use the WTIS-CCN application to input the patient records that CCN uses to fulfill its functions as a Registry and as an advisory body to the provincial Ministry of Health and Long-Term Care as set out in the Personal Health Information Protection Act, 2004.

Background

The policy describes the method of transferring personal health information securely. All data will be transmitted via SFTP (Secure File Transfer Protocol) with at least 128-bit encryption strength. All passwords will be provided under separate cover.

Policy

1. All CCN data and information should be stored on the CCN network for security purposes. Upon completion, all data provided to the Requestors must be returned to CCN or destroyed in a manner consistent with established standards.

2. The SFTP utilizes key exchange and is unique for every CCN Member Hospital.

3. CCN utilizes VeriSign SSL digital certificates (128-bit encryption) for any online transmission of personal health information.

4. CCN's Privacy Officer or a designate of CCN's Privacy Officer is responsible for ensuring that transfers of personal health information are conducted in a secure manner.

5. Transfers of personal health information will be automatically recorded and logged for auditing. These logs are to be retained indefinitely.

6. Any transfer of personal health information to a third party service provider will be governed by the conditions of the contractual agreement made with the third party service provider.

7. CCN prohibits the transfer of personal health information in other formats, including paper.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer or a designate will review the logs of transfers of personal health information to ensure that the above procedures have been followed. Additionally, the CCN shared hard drive is audited for evidence of unauthorized personal health information on a quarterly basis. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

S4 – Destruction of Personal Health Information

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	S4
Created:	**Effective:**	**Revised:**
August 2008	August 2008	May 7 2011

Overview

This policy sets out the procedures for the permanent destruction of records of personal health information in various formats.

Background

When personal health information is no longer required, it must be destroyed in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstances. CCN is committed to protecting all of the personal health information in its custody, including that which is no longer needed for its identified purposes.

Policy

1. Records of personal health information that are no longer necessary for CCN's identified purposes must be destroyed in a secure manner.

2. Records of personal health information that are awaiting destruction must be segregated from personal health information still in use and retained in accordance with CCN's policy, "Secure Retention of Personal Health Information".

3. Ultimate responsibility for the secure disposal of records of personal health information lies with the Privacy Officer.

4. In cases in which CCN's policy against the retention of personal health information on paper has been breached, CCN agents are to use the locked shredding bins found on either side of the office to dispose of personal health information in paper format. These bins are operated by Shred-It, a third-party service provider whose employees are bonded.

5. CCN agents who dispose of personal health information on paper shall complete the Transfer of Personal Health Information for Disposal Form, which collects basic information about the nature of the personal health information transferred to Shred-It. CCN's Privacy Officer shall maintain an inventory of these forms.

6. 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.

7. CCN's Privacy Officer shall maintain a repository of these certificates of destruction.

8. 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.

9. For records of personal health information on optical disk (CD or DVD), CCN agents are to notify the Privacy Officer. The Privacy Officer or a designate will then do the following:
    a. Remove or black out any information printed on the CD that describes the CD's contents, author, owner, sender and/or recipient.
    b. Using scissors, scratch the CD's optical (data) surface from the center outwards to the rim. Make several deep scratches.
    c. Using scissors or other implements, cut or break the CD into several pieces.

10. For records of personal health information on magnetic tape or floppy diskette, CCN agents are to notify the Privacy Officer. The Privacy Officer or a designate will then do the following:
    a. Remove or black out any information printed on the tape or diskette that describes the contents, author, owner, sender and/or recipient.
    b. Break apart the housing of the tape or diskette.
    c. Remove the magnetic tape or the floppy diskette.
    d. Bend, tear and otherwise cut up the magnetic material. Shredding is acceptable.

11. For records of personal health information on flash memory cards and/or USB devices, CCN agents are to notify the Privacy Officer. The Privacy Officer or a designate will then do the following:
    a. Remove or black out any information printed on the device that describes the contents, author, owner, sender and/or recipient.
    b. Delete the contents of the portable memory device.
    c. Physically break the memory card or USB device into pieces.

12. For records of personal health information on hard disk, CCN agents are to notify the Privacy Officer. The Privacy Officer or a designate will then do the following:
    a. Remove the disk(s) from the computer housing.
    b. Open the disk pack chassis and remove the platters, by force, if necessary.

c. Deform the platters using pliers or drill holes through the platters.

Enforcement

All CCN agents must comply with this policy. The Privacy Officer shall review the repository of certificates of destruction received from Shred-It and the inventory of personal health information transferred for disposal. The Privacy Officer or a designate will also, on a quarterly basis, audit the CCN shared hard drive for evidence of unauthorized personal health information. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

S5 – Password Policy

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	S5
Created:	**Effective:**	**Revised:**
May 2 2011	June 1 2011	-

Overview

This policy sets out the means by which CCN ensures that the passwords used by its staff and by CCN agents at member hospitals are robust, remain secure, and are not vulnerable to attacks.

Background

The use of passwords to authenticate user access to the CCN network is an important safeguard that protects both corporate data and personal health information. Complex passwords that change regularly reduce the likelihood of a successful password attack. This policy sets out the complexity requirements and lifetime for passwords. This will help us to centralize control of user passwords and create a well-crafted Windows security scheme.

Policy

1. The Director of It is responsible for implementing these procedures.

2. Password must be at least 8 characters long.

3. Password must contain characters from three of the following four categories:
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters (!,#,%,$)

4. Password must not contain any part of the user's account name.

5. Staff will be prompted to change their password every 90 days.

6. Staff will not be able to reuse either of the last two passwords used.

7. Staff must protect the integrity of their password by ensuring that it is not made known to any other individual.

8. Screensavers must be activated system-wide following one minute of inactivity. Agents must use a password to bypass the screensaver.

9. The WTIS-CCN Reporting Module must lock out users after multiple failed log-in attempts.

10. The WTIS-CCN Reporting Module must provide self-service update and recovery services.

Enforcement

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

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

CARDIAC CARE NETWORK

S6 – Maintenance and Review of System Control and Audit Logs

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	S6
Created:	**Effective:**	**Revised:**
May 2 2011	June 1 2011	May 2 2014

Overview

This policy lists the audits that must performed by CCN staff to ensure that the technical components of its infrastructure function securely and properly.

Background

CCN will perform a number of security audits to ensure that its systems perform as expected. All system logs will be audited by CCN's Supervisor Database/Application Development under the direction of the Privacy Officer and will be retained indefinitely.

Policy

1. All accesses to personal health information are to be logged for later review.

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

3. CCN's contracted IT service provider, Interface, will monitor system performance:
    - Review 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 identify any repetitive warning and error logs.

4. On a weekly basis, CCN will audit the network antivirus threat report and update logs.

5. The system control and audit logs must track any time PHI is accessed through CCN's reporting tools. These logs will track:
    a. The date and time that PHI is accessed
    b. The date and time of the disconnection
    c. The user accessing PHI

d. The network name or identification of the computer through which the connection was made.
e. The operations or actions that create, amend, delete or retrieve PHI and their nature, date and time, and the name of the user performing them.

6. On a monthly basis, the following audits will be completed:
    - Security logs
        - Match security changes to known, authorized configuration changes;
        - Investigate unauthorized security changes identified in security event log;
        - Verify that SMTP does not relay anonymously;
        - Verify that SSL (used for transmission of personal health information) is functioning for configured security channels;
        - Review the log of failed attempts to access WTIS-CCN.
    - Review remote access logs.
    - Verify and filter application and system logs on the remote servers to see all errors and repetitive warnings. Respond to discovered failures and problems.
    - Track login failures and the times at which they occurred.

7. If an IT staff member discovers a problem in one of these logs, the staff member must as soon as possible take steps to resolve it. If the problem regards privacy and security and 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. Additionally, if the IT staff member suspects that an unauthorized user has accessed personal health information, the Privacy Officer shall be alerted, in oral or written format, as soon as possible.

8. The review of these system control logs must be documented only if an error is identified. In such circumstances, the reviewer must complete the Log of System Errors and communicate the results to the Privacy Officer in writing at the first reasonable opportunity. The Privacy Officer will work with the Director of IT to develop timelines to address the error discovered, dependent on the nature of the error. The Director of IT will be responsible for tracking and ensuring the findings have been addressed and communicating that to the Privacy Officer.

9. If in the course of completing these audits an IT staff member 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.

10. Logs will be password protected so that only the Privacy Officer and designated IT staff may make changes to them. Alternatively, logs will be retained on a partition of the networked hard

drive to which only the Privacy Officer and designated IT staff have access. Unauthorized agents are forbidden from attempting to access and/or change system control and other audit logs.

11. Logs will be retained for a period of at least one quarter.

Enforcement

All CCN agents must comply with this policy. On a quarterly basis, CCN's Privacy Officer or a designate will audit for compliance with this policy by reviewing the logs for repeated problems. This will ensure that system control audits are in fact completed. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

S7 – Back-Up and Recovery of Personal Health Information

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	S7
Created:	**Effective:**	**Revised:**
May 2009	June 2009	May 2 2011

Overview

This policy sets out the procedures for the proper back-up and recovery of personal health information.

Background

To ensure the integrity of the CCN Registry, even when faced with a service interruption or hardware failure, CCN has developed procedures for the backing-up of all critical data with multiple redundancies. Additionally, CCN has developed procedures for the safe recovery of backed-up information.

Policy

1. CCN's Privacy Officer is responsible for ensuring that backups of personal health information are retained, transferred, and destroyed in accordance with this policy, "Secure Retention of Personal Health Information", "Secure Transfer of Personal Health Information", and "Destruction of Personal Health Information".
2. The CCN database shall be backed-up in real time using the Veeam Backup and Recovery 10 Advanced Server software.
3. The Supervisor of Database/Application Development shall test the Veam system weekly and provide written notification to the Privacy Officer in the event of an error.
4. The CCN database shall be backed-up on a daily basis on tape medium by Recall, a third-party service provider, and taken to an external location.
5. CCN must execute an agreement with Recall based on the template developed by the IPC. This agreement must be executed prior to Recall being provided personal health information. The Privacy Officer is responsible for ensuring that an agreement has been executed.
6. The Director of IT shall test the CCN backup systems on a scheduled basis.
7. The Director of IT shall be responsible for carrying out these back-ups.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Director of Communications or her/his designate on a quarterly basis. The auditor shall review the completed Form for Formal Review of Privacy and Security Policies and Procedures to ensure that the

review has been properly conducted and that the recommendations have been properly logged. Should the Director of Communications determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

S8 – IT Policy: E-mail, Internet, and Computing Devices

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	S8
Created:	**Effective:**	**Revised:**
April 2010	April 1 2010	June 19 2013

Overview

The policy describes the rules covering use of email, internet and mobile computing devices that can be attached to CCN Networks or contain CCN information. As technology and business demands move forward, there has been an introduction of electronic information management, including devices that can be classed as portable media. CCN permits the usage of electronic information (email, internet and portable media) as part of normal business processes. Each individual is responsible for electronic information management and to take care of their use of electronic media and of the data that is accessed and stored either on a portable device or through the network or local computer memory.

Mobile Devices

Mobile Devices are defined as but are not restricted to:

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

Policy

1. All CCN data and information should be stored on the CCN network for security purposes. Any storage of information on portable media must be authorized by the Supervisor Database/Application Development, with appropriate security standards in place.

2. All CCN supplied portable media and their contents remain the property of the organization and are subject to regular audit and monitoring. These devices should only be connected to a laptop and/or desktop that has been approved for use at the CCN.

3. Users must be aware that the portable media device contains CCN data, and must take appropriate action to protect the device from being lost or stolen. Only devices which have been built to CCN published standards and/or from approved suppliers, shall be attached to the CCN data network either directly or through a CCN PC or laptop.

4. If a CCN owned device is lost or stolen, it must be reported immediately to the Director of IT and CEO as a matter of urgency, so that the CCN data network can be protected from the device.

***Please note that at no time should any personal health information be stored on portable media.**

Internet Use

Users must always conduct their internet activities securely and appropriately to protect the integrity of CCN and the CCN information technology network, and to avoid degrading the performance of CCN computing and network resources. In addition, internet access is provided with the understanding that all users at all times will use conduct on the internet that is professional and representative of CCN and consistent with the mission and vision of CCN.

Policy

1. Do not download music, video, or other files from the Internet, unless authorized to do so.

2. Exercise discretion when downloading files and content. Ensure such files and content are only from reputable sources and that you have a clear business need for them.

3. 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.

4. Do not 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.

5. Do not 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.

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

E-Mail Use

E-mail is an important business communication tool that provides CCN with many benefits. However, if e-mail is used inappropriately, it can expose CCN to a range of risks including the disclosure of confidential information.

Policy

1. 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.

2. All CCN emails are subject to the specific controls required by the CCN Privacy Officer.

3. Before sending, remove any confidential information that is not needed by the recipient. For example, delete unnecessary fields or attachments.

4. When you are replying to or forwarding an e-mail chain, review all of the e-mails in the chain to make sure that they are needed by the current recipient.

5. In all cases, confirm that the recipient's e-mail address is correctly entered in the e-mail's "To" field before sending the message. Do not "Reply to All" if some recipients on the address line do not need the information.

6. In cases involving particularly sensitive information, request that the recipient first send you an e-mail, so that you can reply directly to their message.

7. Never send or forward CCN information to or from your own personal e-mail account. Likewise, never send CCN confidential information to a non-CCN e-mail account belonging to another party.

8. Always use appropriate language in your e-mail messages, and adhere to CCN values and policies. Use the same rules and the same polite forms of address that you would use in other types of business communication.

9. If you believe that you have been sent spam or some other form of mass communication, such as a chain e-mail, do not respond to it. Never initiate unsolicited mass e-mail (spam).

10. Use discretion when opening attachments to e-mail messages. Carefully weigh the risk of introducing malicious code such as a virus before opening any attachment.

11. Use discretion when forwarding files and other confidential information. Recipients must have a legitimate business need for receiving the information.

12. Do not provide your CCN e-mail address or those of other CCN users 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).

13. Never access or use another user's e-mail account without formal authorization from the CCN Privacy Officer. Authorization will only be given for cases in which it is critically necessary for the integrity of CCN's functions as defined within the Personal Health Information Act, 2004.

14. Your CCN e-mail account is provided to improve your productivity. Do not use it 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.

15. Incidental personal use of e-mail is occasionally permitted but it must never interfere with your job responsibilities and work-related needs

Working Remotely from CCN

Working remotely (away from CCN's premises) can lead to disclosure of sensitive CCN corporate information, as well as loss or theft of CCN devices. Any remote work must be authorized by the CEO or the Director of IT.

This policy provides a reference of approved activities and recommended behaviours. All CCN employees must adhere to these in order to protect CCN information and computing systems when working remotely. Note: Any work involving Personal Health Information may not be performed remotely.

Policy

1. For security purposes, remote work must be performed using Citrix. Any other portable media must be approved by the Director of IT. All CCN supplied mobile devices and their contents remain the property of CCN and are subject to regular audit and monitoring. These devices should only be connected to a CCN approved laptop or desktop.

2. Users must be aware that the devices contain CCN corporate data and must take appropriate action to protect them from being lost or stolen. If a CCN owned device is lost or stolen, it must be reported immediately to the Director of IT and CEO as a matter of urgency, so that the CCN data network can be protected from unauthorized use of the device.

3. CCN staff must regularly back-up CCN data from the mobile device to the CCN network to protect the data from damage or loss.

4. All CCN corporate information must be immediately deleted from any portable media device once it is backed up to the CCN network. All Portable media devices must be password protected to control unauthorized access to any mobile device and must meet password security standards.

When working outside of CCN premises:

- **CCN employees must use Citrix to connect to CCN network.**
- **Storage of any CCN information on any computer not located at CCN is not permitted.**
- **All CCN corporate information stored on laptops or any other mobile devices should not be shared.**

Upon Your Return to the Office

If you have stored information on your CCN-issued mobile device, immediately transfer information to the appropriate network folders or collaborative workspaces when you return to the office. When transferring files, ensure they are not accidentally lost or overwritten.

Once information is properly archived and no longer required, delete electronic files and/or dispose of printed materials using CCN's secure shredding containers.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer or a designate will, on a quarterly basis, audit the CCN shared hard drive for evidence of unauthorized personal health information. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

S9 – Patch Management Policy

Developed by:	Issued by:	Policy #:
Director of Information Technology	CCN	S9
Created:	**Effective:**	**Revised:**
November 2013	November 2013	-

Overview

This policy describes the means by which CCN ensures that the latest patches and updates are being applied to the servers, computers, firewalls and routers in the network in order to make sure our servers, computers, firewalls and routers remain secure, and are not vulnerable to attacks.

Background

Patch management is an important part of maintaining the security of CCN network and systems. CCN uses a patch management program Windows Server Update Services (WSUS) to enable administrators to deploy the latest Microsoft product patches and updates to servers and computers within CCN network.

Policy

1. CCN utilizes Windows Server Update Services (a server role in Microsoft Windows Server 2012) to manage patches and updates for Microsoft products.

2. Interface Technologies' network administrators will be notified when patches and updates are downloaded to WSUS. WSUS synchronizes with Microsoft Update for patches and updates on a daily basis.

3. Interface Technologies' network administrators will review, test and approve the new patches and updates for distribution in a timely manner. Interface Technologies' network administrators will review all associated documentation, perform risk and relevancy assessments to determine whether or not the patch should be implemented. Criteria including severity, classification and applicability are used to make a determination. Interface Technologies' network administrators will document the rationale for determining that a patch should or should not be implemented. This documentation must include a description of the patch; the date that the patch became available; the severity level of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; and the rationale for the determination that the patch should not be implemented.

4. All service packs, non-critical hotfixes and non-security patches will be tested in lab environment before deployment. A rule is created in WSUS to approve automatically for updates that are classified as Security or Critical Updates. Interface Technologies' network administrators will perform post-implementation testing for the automatically approved and deployed updates.

5. CCN will audit the update reports and logs on a monthly basis. The update reports and logs include the information of a description of the patch, the date that the patch became available, the agent responsible for implementing the patch, the date of implementation, the agent responsible for testing the patch, the date of the testing of the patch, whether or not the testing was successful, the severity level and priority of the patch, the information system, technology, equipment, resource, application or program to which the patch relates, updates status, computer status, and synchronization results.

6. For non-Microsoft products:
    - CCN utilizes Symantec Endpoint Protection Manager to manage the virus definition updates for the antivirus software Symantec Endpoint Protection. Computers and servers are scheduled to check for and download the latest updates every 4 hours from Symantec Endpoint Protection Manager.
    - Interface Technologies' network administrators will download, test and apply the firmware updates to firewalls and routers in a timely manner.
    - CCN administrators will download, test and apply the patches and updates to SAP BusinessObjects in a timely manner.
    - The documentation requirement outlined in bullet #3 also apply to non-Microsoft products.
    - CCN will audit the updates reports and logs on a monthly basis.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis (in accordance with the policy "Policy and Procedures for Privacy and Security Auditing"). The Privacy Officer or a designate will, on a quarterly basis, review the update reports and logs to ensure that the above procedures have been followed. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

HUMAN RESOURCES AND ORGANIZATIONAL POLICIES AND PROCEDURES

PH1 – Privacy and Security Training

Developed by:	**Issued by:**	**Policy #:**
Director of Operations & Stakeholder Relations	CCN	PH1
Created:	**Effective:**	**Revised:**
September 2009	January 2010	July 19 2013

Overview

This policy describes the procedures governing the privacy and security training of CCN staff and other agents.

Background

It is the Cardiac Care Network's policy to ensure that appropriate procedures are in place to train staff and other stakeholders on the CCN privacy and security policies.

Policy

1. Standardized privacy and security training will be administered to new agents as part of their orientation promptly following the initiation of their employment or other relationship with CCN.

2. Privacy training will thereafter be administered to CCN agents on a biannual basis.

3. Initial and ongoing privacy and security training is mandatory.

4. All new staff, contractors and vendors must complete the online privacy and security training.

5. CCN's Administrative Assistant shall review the final mark of each participant. If an agent passes, they will obtain access to the CCN network and may continue their regular duties. If an agent fails, they must retake the privacy and security training until they pass.

6. CCN's Administrative Assistant shall maintain a list of agents who have and have not completed privacy and security training.

7. CCN's Administrative Assistant tracks attendance and provides the list to the Privacy Officer.

8. All results are communicated to the Privacy Officer immediately.

9. If staff, contract or vendors do not complete the online privacy and security, then they will not be provided access to any CCN documentation. Failure to follow any of these procedures may lead to disciplinary action and/or dismissal.

10. This process will be reviewed annually by the privacy officer.

11. CCN Data Manager and IT staff shall have appropriate training in BusinessObjects and supporting infrastructure through the knowledge transfer from the BusinessObjects vendor NexJ and Interface Technologies.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer will review the log of agents who have and have not completed privacy and security training to ensure that all agents have received adequate training in the protection of personal health information. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

PH2 - Execution of Confidentiality and Non-Disclosure Agreements

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	PH2
Created:	**Effective:**	**Revised:**
February 2010	April 1 2010	May 2 2011

Overview

This policy sets out the procedures for the execution of Confidentiality and Non-Disclosure Agreements.

Background

Confidentiality and Non-Disclosure Agreements contractually bind CCN agents to protect the personal health information in the custody of CCN to the best of their ability. The standard Agreement that all CCN agents sign is attached.

Policy

1. Upon being hired by CCN, the employee will sign an Employee Contract agreement that has the working copy of the Confidentiality and Non-Disclosure Agreement.

2. CCN employees will be required to sign the Confidentiality and Non-Disclosure Agreement on an annual basis at the start of each fiscal year, which is at the beginning of April.

3. The record and copy of the signed Confidentiality and Non-Disclosure Agreement will be kept by the CCN Privacy Officer in hard copy in a locked drawer and in a secure spot on the CCN electronic drive.

4. The Privacy Officer will maintain a log of employees who have executed Confidentiality and Non-Disclosure Agreements.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Privacy Officer on a quarterly basis. The Privacy Officer or a designate will, on a quarterly basis, review the log of agents who have signed Confidentiality and Non-Disclosure Agreements. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated.

If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

PH3 – Policy and Procedures for Discipline and Corrective Action

Developed by:	**Issued by:**	**Policy #:**
Director of Operations & Stakeholder Relations	CCN	PH2
Created:	**Effective:**	**Revised:**
May 16 2011	June 1 2011	-

Overview

This policy sets out the procedures for discipline and corrective action in respect of personal health information.

Background

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.

Policy

1. 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 shall be responsible for investigating the incident. If the Privacy Officer is under suspicion, the Director of Communications shall conduct the investigation.

2. 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.

3. 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.

4. The results of the investigation shall be communicated to the CEO in a timely manner.

5. 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.

6. Depending on the extent and seriousness of the infraction, the agent may be subject to one of the following corrective actions (in increasing order of seriousness):
    a. Verbal warning;
    b. Restriction or revocation of access rights to personal health information;
    c. Suspension with pay;
    d. Termination of employment.

7. The Privacy Officer shall be responsible for determining the seriousness of the corrective action. This determination shall be made on a case-by-case basis.

8. Any agent found to have intentionally disclosed personal health information shall be summarily fired.

9. 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.

CARDIAC CARE NETWORK

PH4 – Maintaining a Consolidated Log of Recommendations

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	PH3
Created:	**Effective:**	**Revised:**
January 2010	April 1 2010	May 3 2011

Overview

This policy describes how the CCN maintains a consolidated log of all recommendations arising from privacy impact assessments; privacy and security audits; and the investigations of privacy breaches, privacy complaints and security breaches.

Background

It is the Cardiac Care Network's policy to maintain and review the Consolidated Log of Recommendations and ensure that all recommendations are addressed in a timely manner.

Policy

1. The Consolidated Log of Recommendations shall capture all recommendations made in the following circumstances at minimum:
    - Privacy impact assessments;
    - Threat risk assessments;
    - Privacy or security audits;
    - The investigation of privacy or security breaches;
    - The investigation of privacy complaints;
    - Reviews by the Information and Privacy Commissioner of Ontario.

2. CCN's Privacy Officer shall be responsible for making all changes and additions to the Consolidated Log of Recommendations.

3. The Consolidated Log of Recommendations shall capture information about the implementation of recommendations, including necessary actions and an expected date of completion.

4. The Consolidated Log of Recommendations shall be updated every time that the implementation status of a logged recommendation changes.

5. The Consolidated Log of Recommendations shall be reviewed at least quarterly. In the course of this review, the Privacy Officer will assess the degree to which recommendations have been addressed in accordance with the prescribed timelines for completion.

6. The Consolidated Log of Recommendations shall be accessible to all CCN agents, but only changeable by CCN's Privacy Officer or a designate.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by CCN's Director of Communications on a quarterly basis. The Director of Communications shall review the timeframes and action points set out for each entry in the Consolidated Log of Recommendations and compare it to actions that have in fact been taken. The auditor shall seek to identify recommendations that have not been addressed. The auditor shall also seek to ensure that all recommendations made in any form have been added to the Log. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated. If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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

CARDIAC CARE NETWORK

PH5 – Termination and Cessation of Contractual Relationships

Developed by:	Issued by:	Policy #:
Director of Operations & Stakeholder Relations	CCN	PH5
Created:	**Effective:**	**Revised:**
May 16 2011	May 16 2011	April 22 2014

Overview

This policy describes the procedure for ending or terminating a contractual relationship with a CCN agent.

Background

It is CCN's policy to receive adequate notice of resignation from employees planning to exit the Organization. Resignations must be submitted in writing to the CEO. CCN recognizes the right of the Employee to move on and accept new opportunities and challenges for employment. Each resignation received by the organization shall be reviewed in detail to identify opportunities to improve CCN's employee retention strategy.

Policy

1. **Resignation Notice Period:**
   - Employees are encouraged to provide as much advance notice of their resignation as possible in order to minimize disruption to the organization. The recruitment process to find a replacement is lengthy and requires considerable time. In addition, time to plan for appropriate transfer of knowledge and business process should be accommodated.
   - Required Notice periods:
     - Staff positions: – minimum 2 to 4 weeks notice or as otherwise specified in the employment contract.
     - Management Staff – minimum 4 weeks' notice or as otherwise specified in employment contract.
     - Director level – minimum of 6 weeks' notice or as otherwise specified in employment contract.

2. **Termination of Contractual Relationships:**
   - A contract may be terminated either by CCN or the other party under the following circumstances:

- 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 determines on a case-by-case basis whether the other party should have the right to terminate on 30 days' notice or whether the right is CCN's alone];
- in response to a force majeure under certain circumstances; or
- on the mutual agreement of the parties to terminate the Agreement or a Service Schedule.

3. Supervisor Responsibility:

- The Supervisor must immediately advise the CEO and Director, Communications & Corporate Services of all resignations or terminations as soon as this information is available.
- The time stamp for the resignation or termination is the date that the resignation is submitted or termination notices is given in writing.
- The Director, Communications & Corporate Services will make arrangements to obtain all CCN property on last day of work, i.e. identification tags, keys, cell phones, laptop computers, passwords, etc.

4. Procedure Upon Cessation of Contactual Relationship

- The Privacy Officer maintains a check list of all required items to be returned that is completed when an employee leaves CCN. Alternatively, employees leaving CCN can may also submit property to CCN via courier.
  - There is no issue if property is not securly returned because all property pass cards, CCN e-mail and phone accounts are disabled.
- All access to the premises where PHI is retained and to the IT operational envirnoment are immediately terminated on the last day of employment.
- All access and parking cards to the main building housing CCN offices are collected and in partnership with the office building personnel, are deactivated.

Enforcement

All CCN agents must comply with this policy. Compliance with this policy will be audited by the Privacy Officer or hi/her designate on a quarterly basis. The auditor shall review that cessation of termination of contracts with CCN agents was completed according to the policy stated above. Should the Privacy Officer determine that an agent of CCN has not complied with this policy, disciplinary measures will be taken. The Privacy Officer is responsible for determining the seriousness of disciplinary measures and depending on the circumstances may recommend that an agent's relationship with CCN be terminated.

If the instance of non-compliance constitutes a violation of the agent's Confidentiality and Non-Disclosure Agreement, legal action against the agent may be pursued as per that agreement.

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