Information
and Privacy
Commissioner/
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the Cardiac Care Network of Ontario (CCN):

A Prescribed Person under the *Personal Health Information Protection Act*

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Review of the Cardiac Care Network of Ontario (CCN):
A Prescribed Person under the *Personal Health Information Protection Act*

The *Personal Health Information Protection Act, 2004* (*PHIPA*) came into effect on November 1, 2004. The Information and Privacy Commissioner of Ontario (IPC) has been designated as the oversight body responsible for ensuring compliance with *PHIPA*. *PHIPA* establishes rules for the collection, use and disclosure of personal health information by health information custodians that protect the confidentiality of, and the privacy of individuals with respect to, that personal health information. In particular, *PHIPA* provides that health information custodians may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates or as permitted or required by *PHIPA*.

Responsibilities of Prescribed Persons

Section 39(1)(c) of *PHIPA* permits health information custodians to disclose personal health information without consent to certain prescribed persons who compile or maintain registries for purposes of facilitating or improving the provision of health care or that relate to the storage or donation of body parts or bodily substances ("prescribed persons").

Section 13(2) of Regulation 329/04 to *PHIPA* requires each prescribed person to have in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information. Section 13(2) further requires each prescribed person to ensure that these practices and procedures are approved by the IPC prior to November, 1, 2005, in order for health information custodians to be able to disclose personal health information to the prescribed person without consent and for the prescribed person to:

- be able to collect personal health information from health information custodians;
- use personal health information as if it were a health information custodian for purposes of section 37(1)(j) or section 37(3) of *PHIPA*; and
- disclose personal health information as if it were a health information custodian for purposes of sections 44, 45 and 47 of *PHIPA*.

Further, section 13(3) requires prescribed persons to make publicly available a plain language description of the functions of the registry, including a summary of the practices and procedures to protect the privacy of individuals whose personal information it receives and to maintain the confidentiality of that information.

Mandate of the IPC with Respect to Prescribed Persons

Prescribed persons must ensure that their practices and procedures to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information are reviewed and approved by the IPC prior to November 1, 2005.

Review Process

The IPC met with all of the prescribed persons to outline the process that would be followed by the IPC for the review of these practices and procedures. The process was to include a review of documentation relating to the practices and procedures of the prescribed person to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of that information, as well as a visit to the primary site where personal health information was held by the prescribed person. The IPC provided the prescribed persons with a preliminary checklist of privacy and security measures that the IPC would be looking for during the course of its review. The checklist included the following:

Human Resources

- Confidentiality agreements
- Disciplinary procedures for violations
- Clearly defined roles and responsibilities
- Appointed contact persons for privacy and security
- Ongoing education and training program for all staff, employees, affiliates, volunteers, etc. on security and privacy policies and procedures
- Third party agreements (with health information custodians, researchers, etc.)

Privacy

- Privacy policies and procedures that describe how the organization adheres to each fair information practice
- Privacy brochure – available upon request to the public
- Privacy Impact Assessments – for programs/database holdings
- Internal/external privacy audits
- Privacy crisis management protocols
- Data linkage protocols

- Procedures for de-identifying data
- Retention schedules and disposal procedures
- Inventory of all data holdings of personal health information
- Protocol for reviewing proposals in terms of their privacy impacts
- Mechanism for reviewing and updating privacy policies and procedures

Security

- Comprehensive security program including physical, technical and administrative measures
- Access control procedures – authentication and authorization
- Perimeter control
- Electronic access control
- Secure transfer procedures
- Audit trails
- Internal/external security audits
- Disaster Recovery Plan
- Mechanism for reviewing and updating security policies and procedures

The prescribed persons were informed that they were required to implement privacy and security measures and safeguards commensurate with the nature of the work undertaken by the prescribed person, the amount and sensitivity (e.g., level of identifiability) of the information in the custody and control of the prescribed person, and the number and nature of the individuals who have access to personal health information. The scope of the review was to include practices and procedures relating to personal health information included in the specific registry associated with the prescribed person under section 13(1) of Regulation 329/04.

A site visit was to be scheduled within one month of the IPCs receiving the documentation from the prescribed person. The purpose of the site visit was to provide the prescribed person with an opportunity to provide additional information to the IPC and to clarify their practices and procedures, and to provide the IPC with an opportunity to:

- review the physical, technological and administrative security measures implemented;
- ask questions about the documentation provided; and
- discuss privacy and security matters with appropriate staff of the prescribed person.

Following the document review and site visit, each prescribed person was to be informed of any action that it needed to take prior to having its practices and procedures approved by the IPC. Once all necessary action had been taken or if no action was necessary, the IPC would prepare a draft report that would be submitted to the prescribed person for review and comment. If the IPC was satisfied that the prescribed person had implemented practices and procedures that were sufficient to protect the privacy and confidentiality of personal health information, a letter of approval would be issued prior to November 1, 2005.

Description of the Prescribed Person

The Cardiac Care Network of Ontario (CCN) is a prescribed person who compiles or maintains a registry under section 39 of *PHIPA*.

CCN, a non-share capital corporation with a Board of Directors, is an advisory body to the Ontario Ministry of Health and Long-Term Care (MOHLTC). It is dedicated to improving quality, efficiency, access and equity in the delivery of cardiac services in Ontario. CCN is funded primarily by the MOHLTC. Seventeen member hospitals make up CCN. The network operates the Cardiac Registry, advises the MOHLTC on adult cardiac services, and shares information about cardiac services through its website, including expert panel reports, submissions to the MOHLTC, and information on wait times for some cardiac services. CCN's role in the management and planning of the cardiac care system is still under development.

CCN collects personal health information through its member hospitals that provide cardiac care services. Where a patient at one of the 17 member hospitals requires cardiac catheterization, angioplasty or bypass surgery, the patient's information is put into the CCN computer system. This information is used to coordinate cardiac care services for the patient. In addition, this information is aggregated for the purposes of planning and improving the quality of cardiac services.

Review of the Prescribed Person

Documents Reviewed

CCN provided the IPC with a binder of documents on July 19, 2005, and further materials on Aug. 19, and Sept. 9, 2005, including:

Organizational Materials

- CCN Consultant Confidentiality Agreement
- CCN Confidentiality & Non-Disclosure Agreement for employees, agents, and contractors

- CCN Confidentiality & Non-Disclosure Agreement for standing committee members
- Job Profile, Director of Information & Information Technology with Addendum, Privacy Officer Job Description
- Contact Information for the Privacy Officer and Assistant Privacy Officer
- Staff Privacy Training PowerPoint Presentation
- CCN Regional Cardiac Care Coordinator Role Profile
- CCN Data Clerk/Analyst Job Description
- Third-party Agreements: Participation Agreement (template), Research Agreement with Institute for Clinical Evaluative Sciences (ICES)
- Schedule A for agreement between CCN and ICES
- ICES Project Approval Process/Heart and Stroke Pod
- Data Release – Accountability Transfer Form
- Copy of Letters Patent
- CCN By-Law No. 1
- Screen shots, Cardiaccess

Security Materials

- Operations Manual, Security (draft policy dealing with physical and administrative security)
- Security Incident Report form
- Network Security Report dated Spring 2004, conducted by Ainsworth Information Technology Services

Public Privacy Statements/Brochures

- Corporate Privacy Statement
- Privacy Policy, Website Version
- Operations Manual Policies:
    - P1 Accountability for Personal Health Information
    - P2 Identifying Purposes for Collecting Information

- P3 Notice/consent for Collecting, Using, or Disclosing Personal Information
- P4 Limiting Collection of Personal Information
- P5 Limiting Use, Disclosure, and Retention of Personal Information
- P6 Accuracy of Personal Information
- P7 Safeguards for Personal Information
- P8 Openness about Information Handling Policies and Practices
- P9 Individual Access to Personal Information
- P10 Challenging Compliance with Privacy Policy
- P11 Response to a breach
- P12 Opt-out

- CCN Brochure, Helping to Meet the Needs of Heart Patients
- MOHLTC Newspaper advertisement, "Your Rights Under the Personal Health Information Protection Act"
- CCN Poster, "Privacy of your Information"
- Memo to a certain doctor about provision of data for research
- Advice Access *Action*, CCN Annual Report 2005

Internal and External Audits

- Privacy Impact Assessment, CCN, May 3, 2003
- CCN Privacy Impact Assessment Compliance Plan Oct. 14, 2004, updated Dec. 7, 2004
- Institute for Clinical Evaluative Sciences Project-Specific Privacy Impact Assessment Form for CCN Stand-alone Angioplasty Pilot Project Evaluation

Site Visit

IPC representatives conducted a site visit at CCN on August 11, 2005.

IPC representatives toured CCN with the Director of Information and Information Technology and Privacy Officer. Discussions with CCN personnel focused on the following topics:

- Staff Training

- Committee Member Training
- Information Disclosure Policy and Decision Tree
- Privacy Binder materials

Findings of the Review

Human resources

CCN has clearly defined roles for privacy and security. A Privacy Officer has been appointed and is assisted by the Director of Operations and Business Affairs in implementing CCN's privacy program. The Privacy Officer is also responsible for security.

All members of the staff have undergone privacy training. It is our understanding the Committee Members and volunteers have not yet been trained on privacy and security. Privacy training for Committee Members is scheduled for the fall of 2005. Privacy training for CCN volunteers and Committee Members should be undertaken as soon as possible. Moreover, the IPC recognizes that all organizations that collect, use and disclose personal health information must develop a culture of privacy and this cannot be accomplished in one training session. In light of this, CCN should develop and implement a comprehensive program for providing ongoing privacy and security training to all staff. Details of this program should be forwarded to the IPC when they are available.

All employees, agents and contractors of CCN are required to sign a Confidentiality and Non Disclosure Agreement. By signing these agreements staff acknowledge that breaches of privacy and security will have consequences up to and including termination of employment or contract. In addition, the IPC recommends that this agreement include an acknowledgement that these individuals have read, understood, and agree to abide by CCN's privacy and security policies. In addition to signing this agreement, consultants are required to sign a separate Consulting Agreement. Also, individuals who work on CCN Standing Committees are required to sign a modified Confidentiality and Non-Disclosure Agreement.

Agreements are also signed between CCN and Participating Organizations. The Participating Organizations are 17 Ontario cardiac centres that provide selected services. It is our understanding that these agreements are in the process of being revised to reflect the requirements and terminology of *PHIPA* and that new agreements will be renegotiated in the fall of 2005. A copy of the revised template agreement between CCN and the Participating Organizations should be forwarded to the IPC after this process has been completed.

Privacy

CCN has a comprehensive privacy policy. This policy describes how CCN adheres to each of the 10 fair information practices. This privacy policy is available on CCN's website, along with

CCN's written statement of its information practices and contact information for the Privacy Officer.

CCN also has a brochure that describes its functions and what personal health information it collects and why. This brochure is published on the CCN website and is available through the 17 cardiac care centres that participate in CCN. In addition, CCN has developed a privacy notice which is posted at each of the 17 cardiac care sites. These products help to enhance the transparency of CCN's information practices for cardiac patients and other members of the public who are interested.

In 2003, an independent third party conducted a privacy impact assessment of CCN. In addition, CCN has worked with an independent third party to develop a privacy compliance plan that reflects CCN's status as a prescribed person under section 39(1)(c) of *PHIPA*.

CCN discloses personal health information to ICES. This disclosure is governed by a research agreement between CCN and ICES. The research agreement stipulates that the information will be used for a variety of research projects and for producing annual reports on cardiac services. To the extent that personal health information is disclosed for research purposes, the requirements of section 44 of *PHIPA* must be met. For example, under section 44 of *PHIPA*, before personal heath information may be disclosed without consent for research purposes, a researcher must submit to the custodian an application and a research plan, approved by a Research Ethics Board. Such requirements are not applicable where personal health information is disclosed to a prescribed entity, such as ICES, for purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, as set out under section 45(1) of *PHIPA*.

CCN does not disclose personal health information to ICES for research purposes on a study-by-study basis, in accordance with section 44 of *PHIPA*. In our view, such a process would be impractical and unnecessary. Accordingly, the IPC recommends that CCN disclose personal health information to ICES for the purposes of planning and managing the health care system, as set out under section 45 of *PHIPA*. ICES would then be permitted to use and disclose the personal health information for the purposes of planning and managing the health care system (as set out under section 45 of *PHIPA*). ICES would also be permitted to use the personal health information for research purposes, in cases where the requirements of section 44 of *PHIPA* have been met. Accordingly, the IPC recommends that the research agreement be changed to a data sharing agreement between CCN and ICES, with the disclosure of personal health information being primarily for the purposes of section 45 of *PHIPA*. The data sharing agreement should also stipulate that the personal health information may only be used and disclosed by ICES for purposes permitted under *PHIPA*.

CCN does not have a protocol for disclosing personal health information for research purposes and it is our understanding that CCN does not disclose personal health information to any third party other than ICES. All requests for access to cardiac care data for research purposes are referred to ICES. If, at some point in the future, CCN decides to use or disclose personal

health information without consent for research purposes, a policy that incorporates all of the relevant requirements of section 44 of *PHIPA* should be developed and implemented and forward the IPC.

CCN indicated, during the site visit, that data is not used internally in identifiable form and that the computer software that is used does not provide identifiable data. However, there is no formal policy for de-identifying data. A policy specifying when, how and by whom personal health information will be de-identified before it is used to carry out the day-to-day business of CCN should be developed and implemented. Such a policy would help to ensure that employees have access to the least identifiable data possible in their day-to-day work and that the least number of individuals have access to personal health information. This policy should be forwarded to the IPC when it has been completed.

CCN has a policy for dealing with privacy breaches. This policy focuses on containing the breach and taking corrective action to ensure that a similar breach does not occur in the future.

It is our understanding that CCN does not undertake any data linkages. Accordingly, a data linkage policy is not necessary.

In terms of retention, it is our understanding that the intent is to retain all data for the duration of the registry for historical statistical and research purposes. Nevertheless, CCN should develop and implement a formal policy for the destruction of data on various media, as it is unlikely that all multiple copies of data that might be made would be retained indefinitely. This policy should specify when and how personal health information should be destroyed on various media. This policy should be forwarded to the IPC when it has been completed.

Security

A summary review of CCN's information security policies, procedures and other documentation was undertaken, along with an inspection of the physical premises and interviews with relevant IT staff. On the basis of our visit, examination, and observations, we found no evidence of major security risks, threats or breaches. We are therefore broadly satisfied that CCN's information security measures are adequate for the purposes of protecting the privacy of personal health information held.

CCN has a security program that incorporates physical, technical and administrative security measures. Entry to CCN offices is controlled by security cards and video monitoring. All laptop computers are secured with cable locks in a locked office, where available. CCN has a policy of not leaving personal health information unattended on a desk or in other public places. All personal health information is stored only on the master server for which special privacy and security measures are in place. All hard copy documents containing personal health information are stored in locked filing cabinets. All new personnel are oriented to the security system and related security policies and procedures.

In terms of information system security, system administration for all 17 cardiac care sites is handled centrally. Application system access IDs and passwords are issued by the central CCN office. Passwords must be changed every 90 days. Audit logs are created for all demographic and clinical changes made to the data. Logs of network intrusion, hospital tape backups, system logs and file upload logs are checked on a daily basis.

A disaster recovery plan has been developed and implemented. Data that are transmitted over the Internet are encrypted and transmitted across a secure tunnel. All personal health information stored on CDs or other electronic media is password-protected.

In 2004, an independent third party undertook a network infrastructure security assessment. However, the consultant's report indicates that a general overview of security rather than a thorough assessment of security was requested by CCN. Although many of the recommendations arising from this assessment have been implemented, some of them have not. The IPC recommends that CCN implement the recommendations from this assessment as soon as possible and inform the IPC when this has been accomplished.

Although CCN has implemented a number of security measures, the IPC recognizes that information security requires ongoing vigilance and a commitment to continuous improvement. Given the volume and sensitivity of the personal data stores held and used by CCN and its agents, we would be more comforted by the adoption by CCN of a more comprehensive and systemic information security management program.

In this light, we encourage CCN to carry out (preferably by an independent party) a comprehensive, organization-wide threat and risk assessment (TRA). Such a TRA would help identify all risks, both external and internal, and provide a strong basis for prioritizing those risks and developing an action plan to mitigate them. Recurring TRAs are also valuable for measuring progress and ensuring continued improvement.

Summary of Recommendations

Major Recommendations

Based on the review of documentation and the site visit, there are no major recommendations that require rectification or resolution by CCN prior to November 1, 2005.

Other Recommendations

Based on the review of documentation and the site visit, the IPC is making the following recommendations that CCN is not required to act upon/resolve prior to November 1, 2005:

1. Complete privacy and security training for Committee Members and volunteers.

2. Develop and implement a comprehensive program for providing ongoing privacy and security training to all staff and forward details of this program to the IPC when they are available.

3. Amend the Confidentiality and Non-Disclosure Agreement to include an acknowledgement that the individual who signs the agreement has read, understood, and agrees to abide by CCN's privacy and security policies.

4. Amend the agreement between CCN and the Participating Organizations to reflect the requirements and terminology of *PHIPA* and forward a copy of the revised agreement to the IPC once the new agreement has been negotiated with the Participating Organizations.

5. Complete the implementation of the recommendations from the third party network security analysis and inform the IPC when this has been completed.

6. Change the title of the agreement between ICES and CCN to a data sharing agreement and amend the agreement to reflect that the disclosure of personal health information is primarily for the purposes of section 45 of *PHIPA* and that ICES will only use and disclose personal health information as permitted under *PHIPA*.

7. Should CCN decide to use or disclose personal health information without consent for research purposes, a policy that incorporates all of the relevant requirements of section 44 of *PHIPA* should be developed and implemented and forwarded to the IPC.

8. Develop and implement a formal policy for de-identifying data that ensures that employees use the least identifiable data possible in their day-to-day work and that the least number of individuals have access to personal health information and forward this policy to the IPC.

9. Develop and implement a formal policy specifying when and how personal health information will be destroyed on various media and forward this policy to the IPC when it has been completed.

10. Conduct periodic comprehensive threat and risk assessments, with emphasis on both internal and external threats to security.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that CCN has in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Accordingly, effective October 31, 2005, the practices and procedures of CCN have been approved by the IPC.