Information
and Privacy
Commissioner of
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the Cardiac Care Network of Ontario in respect of its Registry of Cardiac Services:

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

Ann Cavoukian, Ph.D.
Commissioner
October 2008

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Three-Year Review of the Cardiac Care Network of Ontario in respect of its registry of cardiac services:

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

The *Personal Health Information Protection Act, 2004* ("the *Act*") is a consent-based statute, meaning that persons or organizations in the health sector defined as "health information custodians"[1] may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates, subject to limited exceptions where the *Act* permits or requires the collection, use or disclosure to be made without consent.

One such disclosure that is permitted without consent is the disclosure of personal health information to prescribed persons that compile or maintain registries of personal health information 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 pursuant to subsection 39(1)(c) of the *Act*.

Statutory Provisions Relating to the Disclosure to Prescribed Persons

Subsection 39(1)(c) of the *Act* permits health information custodians to disclose personal health information, without consent, to a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances. The following persons have been prescribed for purposes of subsection 39(1)(c) of the *Act*:

- Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network;
- Cancer Care Ontario in respect of the Colorectal Cancer Screening Registry;
- Cardiac Care Network of Ontario in respect of its registry of cardiac services;
- INSCYTE Corporation in respect of CytoBase; and
- Hamilton Health Sciences Corporation in respect of Critical Care Information System.

In order for a health information custodian to be permitted to disclose personal health information to a prescribed person without consent, the prescribed person must have in place practices and procedures approved by the Information and Privacy Commissioner/Ontario ("IPC") to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information pursuant to subsection 13(2) of Regulation 329/04 to the *Act*.

1 Persons or organizations described in subsection 3(1) of the *Act* that have custody or control of personal health information as a result of or in connection with performing the powers, duties or work of the person or organization.

These practices and procedures must also be reviewed by the IPC every three years from the date of their initial approval, pursuant to subsection 13(2) of Regulation 329/04 to the *Act*, in order for a health information custodian to be able to continue to disclose personal health information to a prescribed person without consent, and in order for a prescribed person to be able to continue to collect, use and disclose personal health information without consent as permitted by the *Act*.

Initial Review of the Practices and Procedures of the Prescribed Persons

In 2005, the IPC reviewed the practices and procedures implemented by the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, the Cardiac Care Network of Ontario in respect of its registry of cardiac services and INSCYTE Corporation in respect of CytoBase. Following this review, the IPC approved the practices and procedures implemented by these prescribed persons to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information, effective October 31, 2005.

While the IPC was satisfied that these prescribed persons had practices and procedures in place that sufficiently protected the privacy of individuals whose personal health information they received and sufficiently protected the confidentiality of that information, the IPC did make certain recommendations to further enhance these practices and procedures. The recommendations made during the initial review of the Cardiac Care Network of Ontario in respect of its registry of cardiac services, which were the subject of an earlier report of the IPC and which are set out in Appendix "A" to this report, have all since been addressed by the Cardiac Care Network of Ontario.

Three-Year Review of the Practices and Procedures of the Prescribed Persons

Subsection 13(2) of Regulation 329/04 to the *Act* requires the IPC to review the practices and procedures implemented by each prescribed person every three years from the date that they were initially approved by the IPC. Given that the practices and procedures of the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, the Cardiac Care Network of Ontario in respect of its registry of cardiac services and INSCYTE Corporation in respect of CytoBase were all approved on October 31, 2005, the IPC was again required to review the practices and procedures implemented by each of these prescribed persons on or before October 31, 2008.

Process Followed for the Three-Year Review

By letter dated January 28, 2008, the Assistant Commissioner for Personal Health Information requested the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, the Cardiac Care Network of Ontario in respect of its registry of cardiac services and INSCYTE Corporation in respect of CytoBase to forward certain documentation to the IPC, set out in Appendix "B" to this report, to enable the IPC to commence its review of the practices and procedures implemented to protect the privacy of individuals whose personal health information is received and to protect the confidentiality of that information.

Upon receipt, the requested documentation was reviewed and additional documentation and necessary clarifications were requested. The Cardiac Care Network of Ontario submitted the requested documentation on July 10, 2008, and additional documentation on August 11, 2008.

Once the additional documentation and necessary clarifications were received, an on-site meeting was held to discuss the practices and procedures implemented by the prescribed person and to provide the IPC with an opportunity to ask questions arising from the documentation. The on-site meeting with the Cardiac Care Network of Ontario in respect of its registry of cardiac services was held on August 19, 2008.

Following the on-site meeting, each prescribed person was informed of the action that it was required to take prior to the continued approval of its practices and procedures. Once all necessary action was taken, the IPC prepared a draft report which was submitted to each prescribed person for review and comment prior to the report being posted on the IPC website.

It must be emphasized that the review by the IPC was limited to personal health information collected, used and disclosed by the prescribed person pursuant to its function as a prescribed person under subsection 39(1)(c) of the *Act* and not with respect to any other role or responsibility that the prescribed person may have assumed under the *Act*.

Description of the Cardiac Care Network of Ontario

The Cardiac Care Network of Ontario is a not-for-profit corporation established in 2003 to ensure that individuals in the Province of Ontario receive timely, equitable and appropriate access to quality advanced cardiac services, including cardiac catheterizations, coronary angioplasties and cardiac surgeries. The Cardiac Care Network of Ontario is the principal advisor to the Ministry of Health and Long-Term Care on matters related to cardiac services including the need for, the distribution of, and the resources required for cardiac services and including the implementation of best practices, quality indicators, performance measurement and continuum of care strategies.

The Cardiac Care Network of Ontario has developed and operates a registry of cardiac services to facilitate, monitor, manage and improve the quality and efficiency of cardiac services delivered in the Province of Ontario and to improve equitable access to such services. The Cardiac Care

Network of Ontario in respect of its registry of cardiac services is a prescribed person within the meaning of subsection 39(1)(c) of the *Act*.

Three-Year Review of the Cardiac Care Network of Ontario

1. Privacy and Security Governance and Accountability Framework

The Chief Executive Officer of the Cardiac Care Network of Ontario, who reports directly to the Board of Directors, is ultimately accountable for personal health information in the custody or control of the Cardiac Care Network of Ontario, including ensuring compliance with the *Act* and with the privacy and security policies, procedures and practices implemented. However, the Chief Executive Officer has delegated day-to-day responsibility for the privacy program and for maintaining the confidentiality and security of personal health information to the Privacy Officer, who reports directly to the Chief Executive Officer. The Privacy Officer is responsible for developing, implementing, maintaining and ensuring compliance with the privacy and security policies, procedures and practices implemented and for:

- Overseeing, directing and/or delivering privacy and security training;
- Initiating, facilitating and promoting activities to foster privacy and security awareness;
- Participating in the development and implementation of agreements in order to ensure that privacy and security requirements are addressed;
- Performing privacy and security reviews and conducting compliance monitoring; and
- Establishing and administering a process to receive, document, investigate and take appropriate action with respect to privacy breaches.

2. Overview of Privacy and Security Policies and Procedures

The Cardiac Care Network of Ontario has developed a privacy policy in respect of its registry of cardiac services which describes its status as a prescribed person within the meaning of subsection 39(1)(c) of the *Act* and the obligations that arise from this status. It further describes the purposes for which the Cardiac Care Network of Ontario collects, uses and discloses personal health information and the accountability framework for ensuring compliance with the *Act* and for ensuring adherence to the privacy and security policies, procedures and practices implemented.

The Cardiac Care Network of Ontario has also implemented privacy and security policies and procedures that support the privacy policy, including policies and procedures related to privacy and security training, de-identification of personal health information, retention and destruction of records of personal health information, appropriate password composition and privacy breaches.

Response to a Breach Policy

The Cardiac Care Network of Ontario has developed and implemented a *Response to a Breach Policy* to address the discovery, management and remediation of breaches. A breach is defined as the theft, loss or unauthorized use of personal health information or the disclosure of personal health information to unauthorized persons. It is recommended that a breach also be defined to include a breach of any and all privacy and security policies, procedures and practices implemented by the Cardiac Care Network of Ontario.

The *Response to a Breach Policy* requires the Privacy Officer to investigate a breach; however, it does not impose a positive duty on agents of the Cardiac Care Network of Ontario to report a breach or suspected breach to the Privacy Officer. In the absence of such a duty, there is a risk that breaches will not be identified and contained in an expeditious manner, thereby adversely impacting the privacy of individuals. It is recommended that the *Response to a Breach Policy* be amended to impose a mandatory duty on agents to notify the Privacy Officer of a breach or suspected breach and to set out what information with respect to the breach or suspected breach must be reported to the Privacy Officer and the format in which it must be reported.

In addition, the *Response to a Breach Policy* does not address containment of the breach. It is important that the process of containment be initiated immediately upon discovery of the breach or suspected breach in order to prevent further theft, loss or unauthorized access, use, disclosure, copying, modification or disposal of personal health information. It is recommended that the *Response to a Breach Policy* be amended to address containment, including who is responsible for containing the breach, the procedures to be followed in containing the breach, when containment must be commenced and the procedure for reviewing the containment measures in order to determine if the breach has been effectively contained or whether further action is required.

The *Response to a Breach Policy* requires the Privacy Officer to complete an incident report upon being notified of a breach, to ascertain the risk arising from the breach and to take any action that is deemed appropriate. The *Response to a Breach Policy*, however, does not address notification in the event of a breach. It does not set out when and in what circumstances senior management and others at the Cardiac Care Network of Ontario will be notified of a breach, including the Chief Executive Officer and Board of Directors. It also does not address the procedure for investigating and remediating the breach. It is recommended that the *Response to a Breach Policy* be amended to address notification, as well as the procedure for investigating and remediating a breach.

In addition, the *Response to a Breach Policy* states that the individuals to whom the personal health information relates will be notified of the breach. It is recommended that, as a secondary user of personal health information, the Cardiac Care Network of Ontario notify the health information custodians that provided the personal health information in order that the health information custodians may notify the individuals to whom the personal health information relates when required pursuant to subsection 12(2) of the *Act*, as opposed to notifying these individuals directly.

In revising the *Response to a Breach Policy*, the Cardiac Care Network of Ontario may wish to have regard to *What to Do When Faced with a Privacy Breach: Guidelines for the Health Sector* produced by the IPC.

Security Breach Policy

The Cardiac Care Network of Ontario does not appear to have developed a policy or implemented a procedure governing information security incidents, that is, events that compromise or potentially compromise the confidentiality, integrity or availability of personal health information. It is recommended that the Cardiac Care Network of Ontario develop a policy and associated procedures to address the identification, reporting, containment, notification, investigation and remediation of information security incidents.

Privacy Inquiries and Complaints Policy

The Cardiac Care Network of Ontario in respect of its registry of cardiac services has also not implemented policies and procedures to receive and respond to privacy complaints and inquiries from members of the public and other stakeholders. It is recommended that the Cardiac Care Network of Ontario develop a policy and implement procedures for receiving, documenting, tracking, investigating and remediating privacy complaints and for receiving, documenting, tracking and responding to privacy inquiries.

Review of Privacy and Security Policies and Procedures

The privacy policy developed and implemented by the Cardiac Care Network of Ontario in respect of its registry of cardiac services states that the privacy policy will be reviewed in the event of changes to the information practices of the Cardiac Care Network of Ontario or in the event of amendments to the *Act*. However, there is no minimum frequency articulated for this review and there are no procedures outlined for undertaking this review and for amending the privacy policy. Further, the privacy policy does not address the review of all the other privacy and security policies and procedures implemented by the Cardiac Care Network of Ontario.

It is recommended that the Cardiac Care Network of Ontario develop and implement a policy and associated procedures for the annual review of the privacy and security policies and procedures it has implemented. This policy and its associated procedures should set out the person(s) responsible for undertaking the review, the procedure to be followed in undertaking the review, the procedure to be followed in amending the policies and procedures and the time frame each year in which this review will be undertaken.

It is further recommended that the review of the privacy and security policies and procedures implemented have regard to technological advancements; to any orders, guidelines and best practices issued by the IPC; to any industry security and privacy best practices and to any new or amendments to existing privacy legislation relevant to the Cardiac Care Network of Ontario in respect of its registry of cardiac services, including amendments to the *Act* and its regulation.

3. Information Available Related to Privacy and Security Policies and Procedures

The Cardiac Care Network of Ontario makes information about its privacy and security policies, procedures and practices readily available on its website at www.ccn.on.ca including its privacy policy, an information brochure, a *Health Information Privacy Statement* and contact information for the Privacy Officer of the Cardiac Care Network of Ontario.

In addition, each individual in the registry of cardiac services receives an information brochure, *Cardiac Patients Have Options. We are Here to Help You*, which sets out the purposes for which the Cardiac Care Network of Ontario collects and uses personal health information. This brochure is either provided to individuals upon registration or shortly thereafter through regular letter mail.

The Cardiac Care Network of Ontario has also developed a poster entitled *Privacy of Your Information*, which is displayed in the cardiac areas of hospitals from which the Cardiac Care Network of Ontario collects personal health information. This poster describes the information practices of the Cardiac Care Network of Ontario, including the types of personal health information that the Cardiac Care Network of Ontario collects and the purposes for the collection, use and disclosure of the personal health information.

4. Collection, Use and Disclosure of Personal Health Information

Collection

The Cardiac Care Network of Ontario in respect of its registry of cardiac services collects personal health information related to individuals awaiting and receiving cardiac services, such as cardiac catheterizations, coronary angioplasties and cardiac surgeries.

The personal health information collected includes demographic information such as the name, gender, date of birth, address, health card number and medical record number of the individual. It also includes information relating to the cardiac service, including the type of cardiac service, the referral for a cardiac service and the cardiac service performed. The personal health information collected is reviewed by the Cardiac Care Network of Ontario every three years to ensure that the personal health information continues to be required for the identified purposes.

Personal health information is collected electronically from the eighteen cardiac care hospitals in the Province of Ontario: Hamilton Health Sciences Centre, Hôpital Régional de Sudbury, Hôtel-Dieu Grace Hospital, Kingston General Hospital, London Health Sciences Centre, Peterborough Regional Health Centre, Rouge Valley Health System, Sault Area Hospital, Southlake Regional Health Centre, St. Mary's General Hospital, St. Michael's Hospital, Sunnybrook Health Sciences Centre, Thunder Bay Regional Health Sciences Centre, Toronto East General Hospital, Trillium Health Centre, University Health Network, University of Ottawa Heart Institute and William Osler Health Centre.

This personal health information is retained in the registry of cardiac services maintained by the Cardiac Care Network of Ontario which, prior to October 1, 2008, "Cardiaccess." Effective October 1, 2008, "Cardiaccess" was replaced with the Wait Time Information System – Cardiac Care Network ("WTIS-CCN"). However, to date, a privacy impact assessment has not been conducted by the Cardiac Care Network of Ontario on the WTIS-CCN and its related applications.

It is recommended that the Cardiac Care Network of Ontario conduct a comprehensive privacy impact assessment on WTIS-CCN and its related applications in order to identify the actual or potential effects that WTIS-CCN may have on the privacy of individuals whose personal health information is contained in WTIS-CCN. In conducting this privacy impact assessment, the Cardiac Care Network of Ontario may wish to have regard to the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act* published by the IPC. It is also recommended that the privacy and security policies, procedures and practices implemented by the Cardiac Care Network of Ontario be reviewed in light of WTIS-CCN in order to ensure that they still accurately reflect the privacy and security practices of the Cardiac Care Network of Ontario.

Use

The personal health information collected by the Cardiac Care Network of Ontario in respect of its registry of cardiac services is used for purposes of facilitating or improving the provision of health care. In particular, the personal health information is used for the purpose of:

- Ensuring individuals receive timely, equitable and appropriate access to cardiac services;
- Managing and planning access to cardiac services and the delivery of cardiac services;
- Maintaining and reducing wait lists for cardiac services; and
- Providing advice on issues related to cardiac services such as the implementation of best practices, quality indicators, performance measurement and continuum of care strategies.

Currently, the Cardiac Care Network of Ontario does not use personal health information contained in its registry of cardiac services for research purposes.

Disclosure

The Cardiac Care Network of Ontario discloses personal health information contained in its registry of cardiac services for the purpose of facilitating or improving the provision of health care, namely, for the purpose of facilitating or improving the provision of cardiac services and for management of wait lists for cardiac services. This includes preparing reports for the cardiac care hospitals from which it collects personal health information, for the Ministry of Health and Long-Term Care and for Local Health Integration Networks in order to support care delivery, as well as support planning and policy development for cardiac services.

The Cardiac Care Network of Ontario also discloses personal health information to the Institute for Clinical Evaluative Sciences ("ICES"), a prescribed entity within the meaning of section 45 of the *Act*, for the purpose of analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the health system. This disclosure is subject to a *Data Sharing Agreement* between the Cardiac Care Network of Ontario and ICES which requires ICES to implement safeguards to protect the confidentiality of the personal health information and which sets out the permissible uses and disclosures that may be made of the personal health information by ICES.

The Cardiac Care Network of Ontario has indicated that it does not currently use or disclose personal health information for research purposes. It is recommended, in the event that the Cardiac Care Network of Ontario decides to use or disclose personal health information in its registry of cardiac services for research purposes, that it develop policies and procedures with respect to the use and disclosure of personal health information for research purposes in accordance with the *Act* and its regulation prior to any such use or disclosure.

5. Retention and Destruction of Personal Health Information

The Cardiac Care Network of Ontario retains records of personal health information collected pursuant to its function as a prescribed person under subsection 39(1)(c) of the *Act* for long-term analysis and reporting in order to facilitate or improve the provision of health care.

Further to the recommendation made by the IPC during the initial review of its practices and procedures in 2005, the Cardiac Care Network of Ontario developed a *Destruction of Personal Health Information Policy* that sets out the procedures to be followed in destroying records of personal health information in both paper and electronic format.

The *Destruction of Personal Health Information Policy* requires that all records of personal health information in paper format be destroyed by shredding. However, it is unclear what type of shredding is employed. It is recommended that the *Destruction of Personal Health Information Policy* be amended to set out the type of shredding that is employed and that the shredding employed be consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC and with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to the *Act*. The *Destruction of Personal Health Information Policy* further requires that all records of personal health information in electronic format, such as CD, DVD, magnetic tape or floppy diskette, be physically destroyed thereby rendering the media unusable.

6. Administrative Safeguards Implemented

In addition to its privacy and security policies and procedures, the Cardiac Care Network of Ontario has implemented the following administrative safeguards to protect personal health information in its registry of cardiac services against theft, loss and unauthorized use, disclosure, copying, modification or disposal.

Privacy and Security Training

Further to the recommendation made by the IPC during the initial review of its practices and procedures in 2005, the Cardiac Care Network of Ontario has developed a *Privacy and Security Training Policy* which requires all staff to undergo privacy and security orientation upon the commencement of their employment or contractual relationship with the Cardiac Care Network of Ontario and prior to being given access to personal health information. It further requires staff to receive annual privacy and security training.

Attendance at the initial privacy and security orientation as well as the ongoing annual privacy and security training, is mandatory and is monitored by the Privacy Officer. Confirmation of attendance is placed in the human resources file of the staff member. Further, pursuant to the *Privacy and Security Training Policy*, the failure to attend the initial privacy and security orientation and ongoing training will result in the staff member being prevented from accessing personal health information until the orientation or training has been completed.

The initial privacy and security orientation is formalized in PowerPoint presentations entitled *CCN Staff Privacy Training*, *Privacy Training: Stakeholders and Volunteers* and *CCN Security Policy*. The *CCN Staff Privacy Training* describes the status of the Cardiac Care Network of Ontario in respect of its registry of cardiac services as a prescribed person pursuant to subsection 39(1)(c) of the *Act*, indicates that the Cardiac Care Network of Ontario has implemented privacy policies and procedures, provides information as to where these policies and procedures can be found and discusses the various agreements that the Cardiac Care Network of Ontario enters into in order to protect the confidentiality of personal health information in its custody or control.

It is also recommended that the PowerPoint presentations *Staff Privacy Training* and *Privacy Training: Stakeholders and Volunteers*, be amended to discuss and explain the:

- Effect of its status as a prescribed person within the meaning of section 39(1)(c) of the *Act*;
- Privacy policy and other policies, procedures and practices implemented by the Cardiac Care Network of Ontario to protect the privacy of individuals whose personal health information it receives and to protect the confidentiality of that information;
- Requirements imposed on staff as a result of these policies, procedures and practices;
- Responsibilities imposed on staff with respect to identifying, notifying the Privacy Officer of and containing a privacy breach; and
- The roles and responsibilities of the Privacy Officer.

The PowerPoint presentation *CCN Security Policy* should also be amended to discuss and explain:

- The security policies, procedures and practices implemented by the Cardiac Care Network of Ontario to protect the security of personal health information;

- Requirements imposed on staff as a result of these policies, procedures and practices; and
- The physical, administrative and technical safeguards implemented by the Cardiac Care Network of Ontario, including the responsibilities of staff in implementing the safeguards.

It is also recommended that the ongoing annual privacy and security training include role-based training in order to ensure that staff understand how to apply the privacy and security policies, procedures and practices implemented by the Cardiac Care Network of Ontario in their day-to-day work. It should also include a discussion of any new privacy and security policies, procedures and practices implemented by the Cardiac Care Network of Ontario and significant amendments to existing privacy and security policies, procedures and practices.

Confidentiality Agreements

The privacy policy implemented by the Cardiac Care Network of Ontario in respect of its registry of cardiac services states that all employees, volunteers and members of the Board of Directors of the Cardiac Care Network of Ontario and all consultants and contractors retained by the Cardiac Care Network of Ontario must sign a *Confidentiality and Non-Disclosure Agreement*.

However, it is unclear from a review of the documentation, when the *Confidentiality and Non- Disclosure Agreement* must be signed, whether it must be signed on an annual basis, who is responsible for ensuring that the *Confidentiality and Non-Disclosure Agreement* is executed, how execution is tracked and the consequences for failing to execute the *Confidentiality and Non-Disclosure Agreement*.

It is recommended that the Cardiac Care Network of Ontario develop and implement a policy and associated procedure to formalize its practices related to the execution of the *Confidentiality and Non-Disclosure Agreement*. This policy and procedure should require the *Confidentiality and Non-Disclosure Agreement* to be executed upon the commencement of the employment or contractual relationship with the Cardiac Care Network of Ontario and prior to being given access to personal health information and emphasize that execution is mandatory. It should also describe the process that will be used to track execution, including who is responsible for tracking execution and the consequences for failing to execute the *Confidentiality and Non-Disclosure Agreement*.

The policy and procedure should also set out whether the *Confidentiality and Non-Disclosure Agreement* must be signed on an annual basis by employees, and if so, to set out the time frame each year in which the *Confidentiality and Non-Disclosure Agreement* must be executed. Annual execution of the *Confidentiality and Non-Disclosure Agreement* is one mechanism to remind employees of the sensitive nature of the information to which the Cardiac Care Network of Ontario has been entrusted and to remind them of their obligations in protecting the privacy of individuals whose personal health information is received. The annual execution of the *Confidentiality and Non-Disclosure Agreement* is also consistent with the practices implemented by other persons prescribed pursuant to subsection 39(1)(c) of the *Act*.

The *Confidentiality and Non-Disclosure Agreement* requires the person signing the *Confidentiality and Non-Disclosure Agreement* to agree that they have read, understood and agree to comply with the privacy and security policies implemented by the Cardiac Care Network of Ontario. It further requires the person to acknowledge that a breach of the *Confidentiality and Non-Disclosure Agreement* may result in disciplinary action, including termination of the relationship with the Cardiac Care Network of Ontario.

The *Confidentiality and Non-Disclosure Agreement* also addresses the uses and disclosures that may be made of the personal health information. In particular, the *Confidentiality and Non-Disclosure Agreement* requires the person signing to acknowledge that personal health information may only be used when necessary for the purpose of carrying out employment or contractual duties and for no other purpose and that personal health information may only be disclosed where permitted or required by law. It also requires the Privacy Officer to be notified immediately, in writing, upon becoming aware of a breach of the *Confidentiality and Non-Disclosure Agreement*.

Other Agreements

The Cardiac Care Network of Ontario has entered into a *Participation Agreement* with each of the cardiac care hospitals from which it collects personal health information in which the Cardiac Care Network of Ontario agrees to comply with the obligations imposed on prescribed persons under subsection 39(1)(c) of the *Act,* including the limitations imposed with respect to the collection, use and disclosure of personal health information.

However, the *Participation Agreement* does not require the Cardiac Care Network of Ontario to notify the cardiac care hospitals if personal health information is collected, used or disclosed in a manner contrary to the provisions of the *Participation Agreement* or where personal health information is stolen, lost or accessed by unauthorized persons. It is recommended that the *Participation Agreement* be amended to ensure that the cardiac care hospitals are able to fulfill their obligations under subsection 12(2) of the *Act* to notify individuals, at the first reasonable opportunity, if their personal health information is stolen, lost or accessed by unauthorized persons.

In addition, contractors retained by the Cardiac Care Network of Ontario are required to execute a *Master Services Agreement* in which the contractor acknowledges that it is an agent within the meaning of the *Act* for purposes of providing services to the Cardiac Care Network of Ontario and must comply with the duties of an agent under the *Act*. The *Master Services Agreement* further requires the contractor to acknowledge that it will not use personal health information except as necessary in the course of providing services and will not disclose the information except with the prior written consent of the Cardiac Care Network of Ontario.

Consultants retained by the Canadian Stroke Network are required to execute a *Consulting Agreement* in which the consultant acknowledges that it will not use personal health information except as necessary in the course of providing services and will not disclose the information except with the prior written consent of the Cardiac Care Network of Ontario.

It is recommended that the template *Master Services Agreement* and *Consulting Agreement* be amended to impose a positive obligation on the contractor or consultant, as the case may be, to notify the Cardiac Care Network of Ontario, in writing, at the first reasonable opportunity if the privacy and security provisions in these agreements have been breached or if the contractor or consultant uses or discloses personal health information in contravention of these agreements. It is also recommended that the *Consulting Agreement* be amended to require the consultant to acknowledge that it is an agent of the Cardiac Care Network of Ontario for purposes of the *Act* and that the consultant must comply with the duties imposed on an agent under the *Act*.

De-Identification Policy

Further to a recommendation made by the IPC during the initial review of its practices and procedures in 2005, the Cardiac Care Network of Ontario has developed a *De-identification Policy* which describes the circumstances in which personal health information must be fully de-identified and the process by which personal health information will be fully de-identified and the circumstances in which personal health information may be partially de-identified and the process by which personal health information will be partially de-identified.

Audit Program

The Cardiac Care Network of Ontario in respect of its registry of cardiac services conducts audits to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information, including reviews of eight different audit logs and conducting threat and risk assessments on its information technology infrastructure. Depending on the nature of the audit logs, the audit logs are reviewed either on a daily, weekly or monthly basis.

However, the Cardiac Care Network of Ontario has not formalized its procedures and practices for maintaining, reviewing and analyzing audit logs of its registry of cardiac services. It is recommended that the Cardiac Care Network of Ontario develop written policies and procedures governing the maintenance, review and analysis of audit logs. It is further recommended that these policies and procedures address the frequency of the review and analysis, the procedure to be used in reviewing and analyzing audit logs, the person responsible for the review and analysis and the mechanism and format for reporting the findings of the analysis and review of audit logs.

It is also recommended that the Cardiac Care Network of Ontario develop and implement a privacy and security audit program with associated policies and procedures addressing the types of privacy and security audits that will be conducted, the frequency of each audit, the procedure to be used in conducting each audit, the person responsible for conducting each audit, the mechanism and format for reporting the findings of each audit, to whom the findings of the audit will be reported and the procedure to track the findings of the audit and how each finding was addressed.

Policies Related to the Transmission of Personal Health Information

The Cardiac Care Network of Ontario has not implemented any written standards governing the transfer of personal health information from the Cardiac Care Network of Ontario. Given the potential for theft or loss of the personal health information being transferred, and the potential for unauthorized disclosure of personal health information while it is in the process of being transferred, it is recommended that the Cardiac Care Network of Ontario implement policies and procedures governing the secure transfer of personal health information.

This policy and its associated procedures should articulate the acceptable methods of transferring personal health information and prohibit all other methods of transferring personal health information. It should also set out the safeguards that must be employed to ensure that personal health information transferred through one of the acceptable methods is being transferred in a secure manner and to ensure that the acceptable methods of transferring personal health information and the safeguards employed are consistent with Order HO-004 and *Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices* issued by the IPC.

7. Physical Safeguards Implemented

The Cardiac Care Network of Ontario is located in a locked facility with twenty-four hour video and security monitoring and tracked card access which divides the facility into varying levels of security with each successive level being more secure and restricted to fewer individuals. In order to access the server room, individuals must successfully pass through multiple levels of security.

8. Technical Safeguards Implemented

The Cardiac Care Network of Ontario has implemented a number of technical safeguards to protect personal health information in its registry of cardiac services such as the use of firewalls and network encryption and intrusion detection systems and the use of multiple levels of encryption for the transfer of personal health information. The technical safeguards implemented also include the authentication of sending and receiving computer systems and restricted access to the registry of cardiac services by means of unique individual account names and passwords, account user registration, two level authentication and role-based restrictions.

The Cardiac Care Network of Ontario has also implemented backup and recovery procedures that involve daily backups of its registry of cardiac services and the creation of an off-site standby server in the event of a disaster, as well as a *Password Policy* consistent with current industry standards.

Further, the Cardiac Care Network of Ontario ensures that threat and risk assessments are conducted on the information technology infrastructure and related applications of its registry of cardiac services in order to identify real and potential threats, to assess vulnerabilities and to assess the effectiveness of proposed or existing safeguards. In June 2008, a threat and risk

assessment was performed by Cygnos I.T. Security which made a number of recommendations to minimize these threats and vulnerabilities. It is recommended that the Cardiac Care Network of Ontario implement all the recommendations arising from this threat and risk assessment.

Summary of Recommendations

It is recommended that the Cardiac Care Network of Ontario in respect of its registry of cardiac services address the recommendations detailed in this report prior to the next review of its practices and procedures. In summary, it is recommended that the Cardiac Care Network of Ontario:

1. In respect of its policies and procedures relating to the documentation, investigation and remediation of breaches:

    (a) Amend the *Response to a Breach Policy* to expand the definition of "breach," to impose a positive duty on agents to notify the Privacy Officer of a breach, to identify what information with respect to a breach must be reported and the format for this report, to address the process for containment, investigation and remediation a breach and to address notification in the event of a breach, including to the health information custodian who provided the personal health information; and

    (b) Develop written policies and procedures to address the identification, reporting, containment, notification, investigation and remediation of information security incidents.

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

3. Develop and implement a written policy and associated procedures for the annual review of the privacy and security policies and procedures implemented by the Cardiac Care Network of Ontario and review these privacy and security policies and procedures in light of the Wait Time Information System – Cardiac Care Network ("WTIS-CCN").

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

5. Develop written policies and procedures with respect to the use and disclosure of personal health information for research purposes in accordance with the *Act* and its regulation prior to any use or disclosure of personal health information for research purposes.

6. Amend the *Destruction of Personal Health Information Policy* to set out the type of shredding that is employed for records of personal health information in paper format

and ensure that the shredding employed is consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC and with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to the *Act*.

7. Amend the initial privacy and security orientation in accordance with the comments provided in this report, formalize ongoing privacy and security training, and ensure that ongoing privacy and security training includes role-based training and a discussion of any new policies, procedures and practices implemented or significant amendments to existing policies, procedures and practices implemented by the Cardiac Care Network of Ontario.

8. Develop and implement a written policy and procedure to formalize its practices and procedures related to the execution of the *Confidentiality and Non-Disclosure Agreement*.

9. Amend the *Participation Agreement*, *Master Services Agreement* and *Consulting Agreement* pursuant to the comments in this report.

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

Statement of Continued Approval of Practices and Procedures

The IPC is satisfied that the Cardiac Care Network of Ontario in respect of its registry of cardiac services continues to have in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and that sufficiently maintain the confidentiality of that information. Accordingly, effective October 31, 2008, the IPC is satisfied that the Cardiac Care Network of Ontario continues to meet the requirements of the *Act*.

APPENDIX "A"

RECOMMENDATIONS FROM THE INITIAL REVIEW

The IPC made the following recommendations during the initial review of the practices and procedures implemented by the Cardiac Care Network of Ontario in respect of its registry of cardiac services that were approved by the IPC effective October 31, 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 Cardiac Care Network of Ontario's privacy and security policies.

4. Amend the agreement between the Cardiac Care Network of Ontario and participating organizations to reflect the requirements and terminology of the *Act* and forward a copy of the revised agreement to the IPC once the new agreement has been negotiated.

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 the Institute for Clinical Evaluative Sciences and the Cardiac Care Network of Ontario 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 the *Act* and that the Institute for Clinical Evaluative Sciences will only use and disclose personal health information as permitted under the *Act*.

7. Should the Cardiac Care Network of Ontario 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 the *Act* should be developed and implemented.

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.

APPENDIX "B"

DOCUMENTATION REQUESTED

Privacy

- Privacy policies and procedures and the mechanism for reviewing and updating these policies and procedures
- Overview of privacy program and privacy audit program
- Reports on internal or external privacy audits conducted or completed
- Policies, procedures and protocols for privacy breaches and complaints
- Policies, procedures and protocols for data de-identification and data linkage including when, how, the purposes for which and by whom it will be de-identified or linked
- Information about the privacy training program for new and current employees, affiliates and volunteers including when it is provided, its content (copies of training material) and the mechanism to ensure that employees, affiliates and volunteers have been trained
- Information available to the public relating to privacy (i.e. brochures, frequently asked questions) and where it is made available
- Policies, procedures, protocols and agreements relating to research
- Privacy impact assessments for data holdings or programs including information relating to whether privacy impact assessments have been completed for all data holdings or programs, and if not, which have been completed and which remain outstanding

Security

- Security policies and procedures setting out the administrative, technical and physical safeguards and the mechanism for reviewing and updating these policies and procedures
- Policies, procedures and protocols for ensuring that personal health information is protected against theft, loss and unauthorized use or disclosure, including:
    - access control (authentication/authorization)
    - perimeter control, electronic control
    - encryption, firewalls and virus scanners

- secure transfer procedures
- password policies
- audit trails

- Information about the nature, scope and frequency of audits of access to data holdings
- Policies, procedures, protocols and agreements related to the secure retention, disposal and destruction of personal health information including retention schedules
- Policies, procedures and protocols related to sending and receiving personal health information including by facsimile, email transmission and other methods
- Policies, procedures and protocols for personal health information on portable or mobile devices such as laptop computers, personal digital assistants and flash drives
- Reports on internal or external threat and risk assessments
- Business continuity and disaster recovery plans
- Information about the security training program for new and current employees, affiliates and volunteers including when it is provided, its content (copies of training material) and the mechanism to ensure employees, affiliates and volunteers have been trained
- Reports on internal or external security audits conducted or completed

Organizational and Other Documentation

- Inventory of data holdings of personal health information
- Respective roles and responsibilities for privacy and security including information about the appointed contact persons for privacy and security and to whom they report and information about the terms of reference for privacy and security committees
- Confidentiality, non-disclosure, data sharing, research and third party agreements
- Policies, procedures and protocols relating to the execution of these agreements, including procedures to track and monitor their execution
- Disciplinary policies/procedures for violations
- Detailed documentation evidencing the completion of each recommendation set out in the report of the Information and Privacy Commissioner of Ontario dated October 2005