Information
and Privacy
Commissioner/
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the Canadian Stroke Network in respect of the Canadian Stroke Registry:

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

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Review of the Canadian Stroke Network in respect of the Canadian Stroke Registry:
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) of Regulation 329/04 to *PHIPA* 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 all 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 IPC 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 Canadian Stroke Network (CSN) is a prescribed person who compiles or maintains a registry under section 39(1) (c) of *PHIPA* for the purpose of facilitating or improving the provision of stroke care in the province of Ontario. This registry is called the Canadian Stroke Registry (the Registry).

CSN is an independent, not-for-profit corporation, established in 1999 to reduce the burden of stroke. CSN is funded by the Networks of Centres of Excellence and provides funding to research projects with the aim of reducing the effects of stroke on the lives of Canadians.

The Registry is compiled and maintained by CSN. The Registry was launched in 2001 as a tool for monitoring, assessing and evaluating the delivery of stoke care in the Province of Ontario in order to facilitate or improve the provision of stroke care in the province.

CSN in respect of the Registry collects personal health information about patients with stoke or transient ischemic attack who are treated at acute care facilities in Ontario that have been designated as Regional Stroke Centres by the Ontario Ministry of Health and Long Term Care as well from a randomly selected sample of additional acute care facilities in Ontario. Participation in the Registry is voluntary. Individuals may withdraw their consent to having their personal health information disclosed to and included in the Registry at any time by contacting a coordinator for the Registry.

The following personal health information is collected for the purposes of the Registry:

- Patient demographics (e.g., gender, date of birth, marital status and health card number);
- Information about the stroke or transient ischemic attack (e.g., date and time of onset, symptoms and signs, mode of arrival to hospital, stroke type and severity and vital signs);
- Pre-existing medical conditions and medications;
- Emergency department and in-hospital investigations, consultations, treatments, and complications; and

- Length of stay, discharge destination, follow-up arrangements, symptoms at time of discharge and medications at discharge.

The personal health information in the Registry is de-identified and used for the following purposes:

- To provide relevant up-to-date information to acute care facilities including quality of care indicators for continuous quality improvement;
- To determine the impact of the services and interventions on the outcome of patients by age, gender and stroke type; and
- To evaluate the outcomes of patients after stroke.

The Institute for Clinical Evaluative Sciences (ICES) houses the Registry and has been contracted by CSN to provide services in relation to the storage and safeguarding of personal health information in the Registry on behalf of CSN.

Review of the Prescribed Person

Documents Reviewed

CSN provided the IPC with a binder of documents in respect of the Registry on October 19, 2005, including:

Human Resources Materials

- Confidentiality Agreement Policy
- Confidentiality Agreement
- Job Descriptions for the Privacy Officer, Biostatistician and Database Programmer

Privacy Materials

- CSN Privacy Policy
- Privacy Code for the Registry
- Confidentiality and Privacy of Personal Health Information Statement
- Privacy and Opt-Out Brochure for the Registry
- Privacy Impact Assessment for the Registry
- Research Ethics Board Approvals of the Research Protocol of the Registry

- Data Flow Diagrams
- Data Destruction Policy
- Shredding Policy
- Confidentiality and Security of Data Policy
- Information Breach Policy
- Draft Letter to Chart Abstractors
- Ethics Review Process for Research Projects using Anonymized Data from the Registry

Security Materials

- Laptop Computer Security Protocol
- Laptop Encryption Software Documentation
- Instructions for Backing-Up and Deleting Data from Laptop Computers
- Security Levels Document
- Overview of Physical and Electronic Security Safeguards
- Transfer of Data for Editing Discrepancies Protocol
- Laptop Computers Servicing Protocol

Other Documents

- Letter to Ministry of Health and Long-Term Care related to the designation of prescribed persons pursuant to section 39(1) (c) of *PHIPA*
- Article "Impracticability of Informed Consent in the Registry of the Canadian Stroke Network"
- Description of the Registry – Phase 3
- Organizational Chart for the Registry

The IPC requested revisions to some of the above mentioned documentation. The revised documentation was submitted on October 24, 2005.

Site Visit

The site visit for CSN in respect of the Registry was conducted on March 14, 2005, the same day as the site visit was conducted for the review of the information practices and procedures of ICES, a prescribed entity under section 45 of *PHIPA*, given the Registry is housed at ICES

and is subject to all of the same safeguards as the personal health information received by and maintained within ICES. For further information about the practices and procedures implemented by ICES to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that personal health information, please see the IPC report entitled: *Review of the Institute for Clinical Evaluative Sciences: A Prescribed Entity under the Personal Health Information Protection Act*.

Findings of the Review

Human resources

CSN has clearly defined roles with respect to privacy and confidentiality. The Executive Director for CSN has been appointed the Privacy Officer. The Privacy Officer reports directly to the Chief Executive Officer and Scientific Director of CSN. The Privacy Officer may delegate day-to-day responsibility for administration of the privacy policies, procedures and practices to other employees but remains accountable for the handling of personal health information by CSN.

The Privacy Officer oversees all activities relating to the development, implementation, maintenance, review and compliance with CSN's policies, practices and procedures relating to privacy and security. In addition, the Privacy Officer participates in the development, implementation and monitoring of all research agreements to ensure privacy and security requirements are addressed and administers the process for receiving, documenting, investigating and taking appropriate action with respect to complaints received concerning CSN's privacy policies, procedures and practices.

CSN has a robust on-going privacy and security training program in respect of the Registry. All new staff (including scientists, adjunct scientists, fellows, students and administrative staff) are required to receive privacy orientation prior to the commencement of employment and prior to being given access to information contained in the Registry. It is our understanding that not all individuals who have access to information in the Registry have completed *PHIPA*-specific privacy training. It is recommended that CSN ensure that all individuals who are affiliated with CSN in respect of the Registry complete training on *PHIPA,* as soon as possible.

All persons affiliated with CSN in respect of the Registry (including employees, staff, scientists, adjunct scientists, fellows and students) are required to sign Confidentiality Agreements upon hiring, and thereafter, on an annual basis. In addition, all persons affiliated with CSN in respect of the Registry for business purposes (consultants, visiting scientists and research collaborators) are required to sign Confidentiality Agreements.

By signing the Confidentiality Agreement, these persons acknowledge that they have read, understood and agree to abide by CSN's policies, procedures and practices with respect to privacy and security. These persons also acknowledge that a breach will result in disciplinary action for

staff up to and including dismissal and, in the case of persons affiliated with CSN for business purposes, may result in termination of their relationship with CSN. It is our understanding that not all persons affiliated with CSN in respect of the Registry have signed Confidentiality Agreements. It is therefore recommended that CSN ensure that these Confidentiality Agreements are executed as soon as possible.

Privacy

CSN has a comprehensive *Privacy Policy* in relation to personal information about identifiable individuals that is collected, used or disclosed in relation to the funding or conduct of research related to reducing the effects of stroke on the lives of Canadians. In addition, it has developed a comprehensive *Privacy Code for the Registry of the Canadian Stroke Network* in relation to the collection, use and disclosure of personal health information by the Registry and the practices and procedures implemented by the Registry to protect the privacy of individuals whose personal health information is collected and to maintain the confidentiality of that information. These are both readily available to the public on CSN's website as well as the website of the Registry. To avoid confusion on the part of the public, the IPC recommends that CSN establish one comprehensive privacy policy that covers all personal information and personal health information collected, used and disclosed by CSN.

In addition, with respect to the Registry, CSN has developed a *Privacy and Confidentiality Statement* that sets out the types of personal health information collected by the Registry, from whom and how this information is collected, the purposes for which it is used, and the person accountable for compliance with the privacy and security policies, procedures and practices implemented by CSN in respect of the Registry. It has also developed a privacy brochure that describes: the Registry; the functions of CSN; how personal health information is collected, used and disclosed by the Registry; the physical, technical and administrative safeguards implemented to protect the privacy of individuals; and how individuals may withdraw consent to having their personal health information disclosed to or included in the Registry. These are also readily available to the public on CSN's website and the website of the Registry as well as available to the public through acute care facilities that provide stroke care.

The IPC recommends that CSN develop a privacy poster that briefly describes the Registry and CSN; the personal health information that is collected; from whom personal health information is collected; and how this information is used and disclosed. The poster should also inform individuals that they may withdraw consent to having their personal health information disclosed to or included in the Registry, provide contact information for an individual who can answer questions about the Registry, and refer individuals to the privacy brochure and *Privacy Code for the Registry of the Canadian Stroke Network* for more detailed information. This poster should be posted at all acute care facilities that disclose personal health information to CSN in respect of the Registry.

CSN has implemented a policy for managing privacy breaches and handling complaints from the public. The privacy breach policy emphasizes containment of the breach; notification of

appropriate persons; and the implementation or amendment of policies, procedures or practices to avoid similar privacy breaches in future. Staff who discover a breach are required to notify their immediate supervisor and the Privacy Officer for CSN. The Privacy Officer for CSN is then responsible for notifying members of the core breach team which include the principal investigators of the Registry, the Chief Executive Officer of CSN and the ICES Privacy Officer (given the Registry is housed at ICES). Privacy complaints and inquiries about the Registry are handled by the Privacy Officer of CSN who is responsible for administering the process of receiving, documenting, investigating, and taking appropriate action with respect to complaints and inquiries received concerning CSN's privacy policies, procedures and practices in respect of the Registry.

CSN has a protocol for de-identifying and linking data. Data is collected by specially trained chart abstractors working at the acute care facilities. Data is entered on a laptop computer and is encrypted with software that is specifically designed for this purpose. Laptop computers are password-protected so that only designated staff may view the data. Encrypted data is sent electronically on a secure telephone line to the Registry. No personal identifiers are included in the data that are transmitted to the Registry. Instead a unique patient identifier is automatically created. Information that links this unique patient identifier to the health card number of an individual is stored separately on the laptop and couriered to the Registry on a diskette.

A very limited number (4) of specified individuals have access to personal health information in the Registry and to information that links the unique patient identifier to the health card number of an individual. These individuals sign special Confidentiality Agreements and are charged with collecting all personal health information disclosed to the Registry and carrying out all required data linkages. Once the linkages are completed, all identifiers are stripped from the dataset, which is then ready for analysis for purposes of facilitating or improving the provision of stroke care in the province of Ontario. In terms of retention and destruction of data, retention schedules are set out on a project-by-project basis. A destruction policy ensures that copies of all datasets are destroyed once they are no longer needed.

Data in the Registry is analyzed regularly for purposes related to facilitating or improving the provision of stroke care. These analyses are performed by biostatisticians on-site, using a secure server and de-identified data. De-identified data is also used on-site by the Registry for approved research projects. Detailed research proposals must be submitted to the publications committee of the Registry for approval. For each research project undertaken using de-identified data contained in the Registry, a Privacy Impact Assessment is carried out. In addition, each research project must be accompanied by a research plan that fulfills the requirements of section 44 of *PHIPA* and Regulation 329/04 and by Research Ethics Board (REB) approval. To ensure the privacy of individuals, the results of all analyses and research projects are reported using aggregated data only. In addition, only data with a cell size greater than five are reported to the public.

The Registry also discloses personal health information for research purposes in accordance with the requirements of *PHIPA* and Regulation 329/04. Requests for disclosure of personal health information for research purposes must be accompanied by a written application, a detailed research plan that complies with *PHIPA* and the decision of a REB approving the research plan.

Linked data is never disclosed to external researchers. All requests for disclosure are reviewed by the Privacy Officer of CSN, the Registry Steering Committee and the Registry Data Privacy and Security Committee.

CSN in respect of the Registry has also entered into agreements with each of the acute care facilities that disclose personal health information to the Registry which governs the disclosure of personal health information to the Registry, the manner in which the personal health information is disclosed to and collected by the Registry, the use and disclosure of that personal health information by the Registry, and the safeguards implemented by the Registry to protect the privacy of individuals whose personal health information is collected by the Registry.

In addition, CSN in respect of the Registry has entered into a data sharing agreement for the sharing of personal health information with ICES for purposes of analysis and compiling statistical information with respect to the management, evaluation, monitoring, planning or allocation of resources for all or part of the health system pursuant to section 13(5) of Regulation 329/04 and section 45 of *PHIPA*.

Security

CSN, in respect of the Registry, has implemented a comprehensive security program including physical, technical and administrative measures. Access to the facility that houses the Registry and to each office in that facility is restricted with keys. Not all members of the staff have a key to enter the facility. Movement of individuals within the facility is controlled with Marlock keys. Staff are only allowed to access areas of the building that they require access to for purposes specific to their job functions. All members of staff are required to wear identification badges. All visitors to the facility must sign in and out and wear distinctive visitor badges. All keys and identification badges are tracked. Security cameras have been installed to monitor activities inside and outside the building. "Glass-break detectors" and security windows have been installed on the ground floor. The facility is also monitored by video surveillance and security services provided by Sunnybrook and Women's Health Sciences Centre.

All personal health information is stored in fireproof safes. There are no external connections to the system containing the Registry. Graded levels of access to data are provided on a need-to-know basis. Identifiers are either removed or encrypted prior to the data being used by staff. Computer systems are password-protected and password-protected screensavers are used to prevent access to information when a terminal has not been used for a specified period of time. Researchers wishing to use data must submit detailed research proposals and physically come to the building to use stripped-down, diskless terminals. Firewalls and virus protection have also been implemented. CSN has a protocol in place for the secure transfer of personal health information to the Registry.

CSN has contracted with ICES to provide services on behalf of CSN with respect to the storage and safeguarding of personal health information collected by the Registry. The agreement between CSN and ICES outlines the safeguards that must be implemented by ICES and the procedure for notifying CSN in the event of a breach of the terms of the Agreement. It is recommended

however, that this agreement be amended to clarify that, in respect of the services provided by ICES relating to the storage and safeguarding of personal health information in the Registry, ICES is an agent of CSN (as defined under *PHIPA*) and, as such, all the responsibilities of and restrictions on agents in section 17 of *PHIPA* apply to ICES.

With respect to the system where the Registry is maintained, a vulnerability/penetration assessment was undertaken by an independent third party. The results of the assessment indicated that the measures that had been put in place were successful in protecting the Registry from internal and external malicious threats.

Although the security measures that have been implemented appear to be quite extensive, one concern that was raised by the IPC is that the measures that have been put in place are not based upon a comprehensive threat and risk assessment (TRA). Although the recent "ethical hack" revealed no evidence of any major security risks, threats or breaches, the IPC recognizes that information security requires ongoing vigilance and a commitment to continuous improvement. Given the volume and sensitivity of the personal health information in the custody or control of CSN and its agents with respect to the Registry, it would be desirable for CSN to adopt a more comprehensive and systemic information security management program.

In this light, we encourage CSN to carry out a comprehensive, Registry-specific threat and risk assessment. Such a threat and risk assessment 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 threat and risk assessments 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 CSN prior to November 1, 2005.

Other Recommendations

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

1. Ensure that all individuals affiliated with CSN who have access to information in the Registry complete privacy and security training specific to *PHIPA*.

2. Ensure that all persons affiliated with CSN in respect of the Registry who have not yet signed a Confidentiality Agreement with CSN do so as soon as possible.

3. Replace the two privacy policies with a comprehensive privacy policy that covers all personal information and personal health information collected, used and disclosed by CSN.

4. Develop a privacy poster that briefly describes the Registry and CSN; the personal health information that is collected by the Registry; from whom the personal health information is collected; how this information is used and disclosed; and how individuals may withdraw consent to having their personal health information disclosed to and included in the Registry. The privacy poster should also provide contact information for the person who can answer questions about the Registry and should refer individuals to the privacy brochure *and Privacy Code for the Registry of the Canadian Stroke Network* for more detailed information. This privacy poster should be provided to the IPC for review and comment prior to being posted at all acute care facilities that disclose personal health information to CSN in respect of the Registry.

5. Amend the agreement between CSN and ICES to clarify that, in respect of the services provided by ICES relating to the storage and safeguarding of personal health information in the Registry, ICES is an agent of CSN as defined in *PHIPA* and, as such, must abide by all of the requirements and restrictions on agents set out in *PHIPA*.

6. Conduct regular 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 CSN 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 CSN have been approved by the IPC.