Information
and Privacy
Commissioner of
Ontario

Report of the Information & Privacy Commissioner/Ontario

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

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

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 Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, 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 Canadian Stroke Network.

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 Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network submitted the requested documentation on June 17, 2008, and additional documentation on August 25, 2008 and August 26, 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 Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network was held on September 3, 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 Canadian Stroke Network

The Canadian Stroke Network is a not-for-profit corporation established in 1999 to reduce the physical, social and economic consequences of stroke on the individual and society. The Canadian Stroke Network has developed and operates the Registry of the Canadian Stroke Network. The Registry of the Canadian Stroke Network collects personal health information about the care and treatment provided to individuals with stroke or transient ischemic attack across the continuum of care in order to monitor, assess, evaluate and improve the delivery of care. The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network is a prescribed person within the meaning of subsection 39(1)(c) of the *Act*.

Three-Year Review of the Canadian Stroke Network

1. Privacy and Security Governance and Accountability Framework

The Chief Executive Officer of the Canadian Stroke Network, who reports directly to the Board of Directors, is ultimately accountable for ensuring that the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network complies 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.

The Privacy Officer, who reports directly to the Chief Executive Officer, is responsible for developing, implementing, reviewing and ensuring adherence to the privacy and security policies, procedures and practices implemented and for ensuring compliance with the *Act*. The Privacy Officer is also responsible for:

- Overseeing, directing or delivering privacy and security training;
- Developing, implementing and monitoring compliance with *Confidentiality Agreements*;
- Establishing and administering a process to receive, document, track, investigate and remediate information breaches; and
- Initiating, facilitating and promoting activities to foster privacy awareness.

2. Overview of Privacy and Security Policies and Procedures

The Canadian Stroke Network has developed a privacy policy, the *Canadian Stroke Network Privacy Policy*, which describes its status in respect of the Registry of the Canadian Stroke Network as a prescribed person within the meaning of subsection 39(1)(c) of the *Act* and the obligations that arise from this status. The *Canadian Stroke Network Privacy Policy* also describes the purposes for which it 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 by the Canadian Stroke Network. The Canadian Stroke Network has also implemented privacy and security policies and procedures that support the *Canadian Stroke Network Privacy Policy*, including policies and procedures related to:

- Protecting the confidentiality and security of personal health information;
- Identifying, containing, investigating and remediating information breaches;
- Procedures respecting the execution of *Confidentiality Agreements*;
- Retention and destruction of records of personal health information; and
- Research ethics board approval.

Information Breach Policy

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network has developed and implemented an *Information Breach Policy* to address the discovery, reporting, containment, notification, investigation and remediation of information breaches. An information breach is defined as the collection, retention, use or disclosure of personal health information in contravention of the *Act* and the theft or loss of personal health information. It is recommended that an information breach also be defined to include a breach of any and all privacy and security policies, procedures and practices implemented by the Canadian Stroke Network.

The *Information Breach Policy* requires a person that discovers an information breach to commence the containment process and to notify his or her supervisor and the Privacy Officer of the breach. However, elsewhere it states that a person that discovers an information breach must report the breach to management staff of the Registry of the Canadian Stroke Network and to the Canadian Stroke Network and that management staff will begin the process of containment. It is recommended that these inconsistencies relating to the reporting and containment of an information breach be resolved and that the *Information Breach Policy* further clarify what information with respect to an information breach must be reported and the format in which it must be reported.

The Privacy Officer is then responsible for notifying other members of the Core Breach Team, including the Chief Executive Officer of the Canadian Stroke Network and the principal investigators of the Registry of the Canadian Stroke Network. The Core Breach Team will then determine the extent of the information breach and determine whether further notification is required, namely, whether the Board of Directors should be notified.

The Core Breach Team is also responsible for initiating breach documentation. However, the *Information Breach Policy* explicitly states that a breach form need not be completed for an internal breach. It is unclear what the rationale is for not documenting an internal breach. Documentation of an information breach is critically important for both managing information breaches and for preventing similar breaches in future. It is therefore recommended that the *Information Breach Policy* be amended to require that all information breaches be documented.

Further, the *Information Breach Policy* should be amended to require the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network to notify the health information custodian who provided the personal health information of the information breach, in order that the health information custodian may notify the individuals to whom the personal health information relates when required pursuant to subsection 12(2) of the *Act*. Currently, the *Information Breach Policy* states that the health information custodian will only be notified "if required."

The *Information Breach Policy* further requires that an investigation of the information breach be conducted and that following the investigation, that recommendations be made to prevent a similar information breach in future. In particular, the *Information Breach Policy* states that in the event of an external information breach, one of the recommendations may include amendments

to existing policies and procedures. It is unclear why this recommendation is limited to external information breaches. An internal information breach may nonetheless require amendments to policies and procedures in order to prevent a similar information breach in future and therefore it is recommended that the *Information Breach Policy* be amended accordingly.

Privacy Inquiries and Complaints Policy

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network has 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 a policy and associated procedures be developed 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 *Canadian Stroke Network Privacy Policy* states that the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network will review and update its privacy policies and procedures on an annual basis or more frequently as required. However, the *Canadian Stroke Network Privacy Policy* does not articulate the procedure for reviewing and updating these privacy policies and procedures, nor does it discuss how often security policies and procedures are reviewed and the procedure for reviewing and amending these security policies and procedures.

It is recommended that the Canadian Stroke Network develop and implement a policy and associated procedures for the annual review of its privacy and security policies and procedures. 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 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 privacy legislation or amendments to existing privacy legislation relevant to the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, including amendments to the *Act* and its regulation.

It is also recommended that in undertaking this review, the Canadian Stroke Network address inconsistencies between and among the various privacy and security policies and procedures it has implemented. For example, while the *Ethics Review Process Policy* states that all requests for research purposes require the completion of a *Data Request Form* and a *Project Specific Privacy Impact Assessment Form* and set out the process for submission of the *Data Request Form* and *Project Specific Privacy Impact Assessment Form*, no such reference is made in the *Confidentiality of Data Policy*. Further, the process for approving the disclosure of information for research purposes is inconsistent as between these two policies.

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

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network makes information about its privacy and security policies, procedures and practices readily available on the website of the Canadian Stroke Network at **www.canadianstrokenetwork.ca**, as well as on the website of the Registry of the Canadian Stroke Network at **www.rcsn.org**. The information made available includes the *Canadian Stroke Network Privacy Policy*, an information brochure entitled *Registry of the Canadian Stroke Network Information Brochure* and contact information for the individuals accountable for ensuring compliance with these policies, procedures and practices and to whom complaints or inquiries can be made.

The information brochure, the *Registry of the Canadian Stroke Network Information Brochure*, describes the status of the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network as a prescribed person within the meaning of subsection 39(1)(c) of the *Act*, describes the obligations that arise as a result of its status under the *Act* and sets out the administrative, technical and physical safeguards implemented by the Canadian Stroke Network to protect personal health information in the Registry of the Canadian Stroke Network.

In addition, further to a recommendation made by the IPC during the initial review of its practices and procedures in 2005, the Canadian Stroke Network makes a poster available at regional stroke centres, enhanced district stroke centres, acute care hospitals and secondary prevention clinics from which it collects personal health information. The poster describes the types of personal health information collected and the purposes for which personal health information is collected and used.

4. Collection, Use and Disclosure of Personal Health Information

Collection

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network collects personal health information about individuals with stroke or transient ischemic attack from acute care hospitals designated by the Ministry of Health and Long-Term Care as regional stroke centres or enhanced district stroke centres, from randomly selected acute care hospitals and from secondary prevention clinics. The personal health information collected includes:

- Demographic information such as gender, date of birth, province and postal code of residence, marital status, ethnic origin, health card number and medical record number;
- Information about the stroke or transient ischemic attack, including the date and time of onset, the time interval between the onset of the stroke or transient ischemic attack and the delivery of care, vital signs, symptoms, stroke type and stroke severity;
- Pre-existing medical conditions, risk factors and medications;

- In-hospital investigations, consultations, treatments and complications; and
- Length of hospital stay, discharge destination, follow-up arrangements and symptoms and medications at the time of discharge.

Personal health information is collected by one of two methods: through abstracting records of personal health information for inclusion in the Registry of the Canadian Stroke Network or through a web-based data collection tool currently known as SPIRIT (Stroke Performance Indicators for Reporting, Improvement and Translation). An electronic services provider has been retained to host, maintain and provide technical support for the web-based data collection tool and an agent, the Institute for Clinical Evaluative Sciences, has been retained to house and safeguard the Registry of the Canadian Stroke Network.

Use

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network does not use personal health information for purposes of facilitating or improving the provision of health care pursuant to subsection 39(1)(c) of the *Act*. Rather, personal health information is de-identified and the de-identified information is then used for these purposes, and in particular, for:

- Monitoring, evaluating, facilitating and contributing to the effectiveness, quality, equity, and efficiency of stroke and transient ischemic attack care;
- Decreasing the functional, economic and social consequences of stroke and transient ischemic attack on the individual, health system and society;
- Determining the characteristics of individuals with stroke and transient ischemic attack including age, gender, stroke severity and risk factors;
- Determining the impact on outcomes based on variations in age, gender, stroke type and the types of care received;
- Documenting national and provincial patterns of care following a stroke or transient ischemic attack with a specific focus on recognized quality of care indicators;
- Developing and disseminating information for use by patients, health care practitioners, policymakers and the general public about stroke and transient ischemic attack; and
- Providing advice on the quality of stroke care delivery and the performance of the Ontario Stroke System to health information custodians, the Ontario Stroke System Evaluation Advisory Committee and the Ministry of Health and Long-Term Care.

It is recommended that the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network develop and implement a policy and procedure with respect to the de-identification and anonymization of personal health information in order to clarify and ensure consistency as to the meaning ascribed by the Canadian Stroke Network to the terms “de-identified information”

and "anonymized information," and in order to clarify and ensure consistency in the process for de-identifying and anonymizing personal health information.

In particular, the policy and procedure should define the terms "de-identified information" and "anonymized information" and should clarify the distinction between these terms. It should also identify the information that must be removed, encrypted and/or truncated in order to de-identify personal health information and the information that must be removed, encrypted and/or truncated in order to anonymize personal health information. The policy and procedure should also identify those responsible for de-identifying and anonymizing personal health information.

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network also does not use personal health information for research purposes, but rather only uses de-identified information with cell sizes of five or less being suppressed. Although only de-identified information is used for research purposes, nonetheless the Canadian Stroke Network requires that the provisions in the *Act* and its regulation relating to the use of personal health information for research purposes be complied with.

In particular, the Canadian Stroke Network requires that a research plan be prepared in accordance with the requirements of the *Act* and its regulation, that a *Project-Specific Privacy Impact Assessment Form* be completed and that the research plan be approved by the Registry of the Canadian Stroke Network Publications Committee and by a research ethics board through expedited review. Semi-annual reports are sent to the research ethics board involving the use of de-identified information for research purposes. The research ethics board may randomly select projects from the semi-annual reports for expedited review. Based on these semi-annual repots, all research plans using de-identified information are considered to have research ethics board approval.

Disclosure

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network does not disclose personal health information except where required by law and except to the health information custodian who disclosed the personal health information, provided it does not contain additional identifying information. Aside from these circumstances, personal health information is not disclosed for any other purposes, including research purposes, but rather only aggregate information is disclosed with cell sizes of five or less being suppressed.

Although the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network only discloses aggregate information for research purposes, it nonetheless requires that the provisions of the *Act* and its regulation relating to the disclosure of personal health information for research purposes be complied with. In particular, the Canadian Stroke Network requires receipt of a written application in the form of a completed *Request for Data Analysis for a Stroke Evaluation or Research Project Form*, a research plan prepared in accordance with the requirements of the *Act* and its regulation and a copy of the decision of the research ethics

board approving the research plan. It further requires the completion of a *Project-Specific Privacy Impact Assessment Form*.

The *Project-Specific Privacy Impact Assessment Form* was developed in order to ensure that a researcher, through the completion of the *Project-Specific Privacy Impact Assessment Form*, addresses all the requirements in the *Act* and its regulation that must be satisfied prior to the use or disclosure of personal health information for research purposes.

The *Project-Specific Privacy Impact Assessment Form* is then reviewed by the Privacy Officer to ensure compliance with the *Act* and its regulation and subsequently by the management team of the Registry of the Canadian Stroke Network for feasibility and appropriateness. If approved by the Privacy Officer and the management team, the research plan and the *Project-Specific Privacy Impact Assessment Form* are forwarded to the Registry of the Canadian Stroke Network Research Committee for review and approval. If approved by the Registry of the Canadian Stroke Network Research Committee, the Canadian Stroke Network further requires the researcher to execute a *Confidentiality Agreement*.

An electronic project management system is maintained to follow the submission and approval of requests for the disclosure of aggregate information for research purposes.

The Canadian Stroke Network also discloses aggregate information to health information custodians, the Ontario Stroke System Evaluation Advisory Committee and the Ministry of Health and Long-Term Care in order to facilitate or improve the provision of health care. Once again, cell sizes of five or less are suppressed. Such reports include the *Quarterly Stroke Performance Indicator Reports* and the *Ontario Stroke System Annual Report*.

5. Retention and Destruction of Personal Health Information

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network 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. Records of personal health information collected for research purposes are retained for the period of time set out in the research plan approved by the research ethics board and the *Project-Specific Privacy Impact Assessment Form*.

The Canadian Stroke Network has developed and implemented a *Document Shredding Policy* which requires that all confidential information in paper format, including 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 *Document Shredding 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*.

Further, while the Canadian Stroke Network has developed and implemented policies and procedures with respect to the secure destruction of records of personal health information in paper format, it has not developed similar policies and procedures for the secure destruction of records in electronic format. It is recommended that the Canadian Stroke Network develop and implement policies and procedures with respect to the secure destruction of records of personal health information and records of health information in electronic format consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC, and consistent with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to the *Act*.

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network has developed and implemented a *Data Destruction Policy* that sets out when information will be destroyed. In particular, a log of all data destruction dates specified in agreements and in research plans approved by research ethics boards is maintained in a project management system.

The health data coordinator is responsible for monitoring these data destruction dates and for notifying the principal investigator named in the agreement or research plan of the pending destruction date. Once the date of destruction has passed, the principal investigator will be asked to sign a document attesting to destruction. It is recommended that the *Data Destruction Policy* be amended to stipulate the required content of the document attesting to destruction that must be executed, and at a minimum, that it include the date, time, location and method of secure destruction employed.

It is also recommended that the *Data Destruction Policy* be amended to establish a process for tracking whether the principal investigator has signed a document attesting to destruction within a reasonable time after the destruction date has passed in order to ensure that records are not being retained longer than necessary to fulfill the purposes for which they were collected.

6. Administrative Safeguards Implemented

In addition to privacy and security policies and procedures, the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network has implemented the following administrative safeguards to protect personal health information against theft, loss and unauthorized use, disclosure, copying, modification or disposal.

Confidentiality Agreements

The *Confidentiality Agreement Policy* requires every person affiliated with the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network for "research purposes" to sign a *Confidentiality Agreement*. This appears to suggest that only those persons affiliated for research purposes, and not those affiliated for purposes of its function as a prescribed person pursuant to subsection 39(1)(c) of the *Act*, are required to sign a *Confidentiality Agreement*.

When clarification was requested, the Canadian Stroke Network advised that every person affiliated with the Canadian Stroke Network in respect of the Registry of the Canadian Stroke

Network is required to sign a *Confidentiality Agreement*. As a result, it is recommended that the *Confidentiality Agreement Policy* be amended to ensure consistency with the actual practices of the Canadian Stroke Network.

It is also unclear when a *Confidentiality Agreement* must be executed. Currently, the *Confidentiality Agreement Policy* states that a *Confidentiality Agreement* must be signed by employees with their employment contract, however, it does not address when other affiliated persons who are not employees, such as consultants and contractors, must execute a *Confidentiality Agreement*. It is recommended that the *Confidentiality Agreement Policy* require every person affiliated with the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network to sign a *Confidentiality Agreement* upon the commencement of their employment, contractual or other relationship and prior to having access to personal health information or health information as the case may be.

The *Confidentiality Agreement Policy* also requires every person affiliated with the Canadian Stroke Network who has "routine access" to the Registry of the Canadian Stroke Network, to sign a *Confidentiality Agreement* on an annual basis. It is unclear what the basis is for the distinction between persons affiliated with the Canadian Stroke Network who have "routine access" to the Registry of the Canadian Stroke Network, who are required to sign a *Confidentiality Agreement* on an annual basis, and other affiliated persons who continue to have access to the Registry of the Canadian Stroke Network but not on a "routine" basis.

When clarification was requested, the Canadian Stroke Network advised that every person who continues to be affiliated with the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network is required to sign a *Confidentiality Agreement*. It is therefore recommended that the *Confidentiality Agreement Policy* be amended accordingly. It also recommended that the *Confidentiality Agreement Policy* be amended to emphasize that the annual execution of the *Confidentiality Agreement* is mandatory and to set out the time frame each year in which the *Confidentiality Agreement* must be executed.

Pursuant to the *Confidentiality Agreement Policy*, execution of the *Confidentiality Agreement* is recorded in a database and in a *Confidentiality Agreement and Privacy Orientation Tracking Log*. However, it is unclear who is responsible for tracking the execution of *Confidentiality Agreements*, both initially and on an annual basis, and what the consequences are for failing to execute a *Confidentiality Agreement*. It is recommended that the *Confidentiality Agreement Policy* formalize the practices and procedures related to the execution of the *Confidentiality Agreement*.

By signing the *Confidentiality Agreement*, affiliated persons acknowledge that as a result of their relationship with the Canadian Stroke Network, they may have access to personal health information, they have read and understood the privacy and security policies and procedures implemented by the Canadian Stroke Network, and any unauthorized use or disclosure of personal health information may result in disciplinary action including the termination of the relationship with the Canadian Stroke Network. However, it is recommended that the *Confidentiality Agreement* be amended in the following respects.

The *Confidentiality Agreement* requires every person affiliated with the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network to comply with the *Freedom of Information and Protection of Privacy Act*. Given that the Canadian Stroke Network is not an institution within the meaning of the *Freedom of Information and Protection of Privacy Act* nor do those signing the *Confidentiality Agreement* appear to be such institutions, it is recommended that the reference to the *Freedom of Information and Protection of Privacy Act* be deleted.

Further, while the *Confidentiality Agreement* states that affiliated persons must acknowledge that they have read and are familiar with the privacy and security policies, procedures and practices implemented by the Canadian Stroke Network, it does not require these affiliated persons to comply with the privacy and security policies, procedures and practices implemented by the Canadian Stroke Network. It is recommended that the *Confidentiality Agreement* be amended accordingly.

Also, while the *Confidentiality Agreement* states that those signing the *Confidentiality Agreement* must acknowledge that any unauthorized use or disclosure of personal health information may result in immediate dismissal or termination of the relationship with the Canadian Stroke Network, it is unclear what is meant by unauthorized use or disclosure. It is recommended that the *Confidentiality Agreement* define an unauthorized use or disclosure to include any use or disclosure in contravention of the *Act* or in contravention of the privacy and security policies, procedures and practices implemented by the Canadian Stroke Network.

In addition, the *Confidentiality Agreement* requires every person signing the *Confidentiality Agreement* to agree not to disclose personal health information to any person who has not entered into a *Confidentiality Agreement* with the Canadian Stroke Network and to agree to keep any personal health information in a physically secure location to which only those who have signed a *Confidentiality Agreement* with the Canadian Stroke Network have access. It is recommended that the *Confidentiality Agreement* be amended to also prohibit disclosure to persons who have entered into a *Confidentiality Agreement* with the Canadian Stroke Network, but who do not require the personal health information for purposes of carrying out their function. Such an amendment would ensure consistency with data minimization best practices.

Other Agreements

The Canadian Stroke Network has entered into an agreement with the Institute for Clinical Evaluative Sciences ("ICES") governing the duties and responsibilities of ICES when acting as an agent of the Canadian Stroke Network in housing and safeguarding the Registry of the Canadian Stroke Network and governing the disclosure of personal health information to ICES for purposes of analysis or compiling statistical information with respect to the health system pursuant to ICES' function as a prescribed entity under section 45 of the *Act*.

The agreement requires ICES to comply with the provisions in the *Act* and its regulation governing the conduct of agents, permits the Canadian Stroke Network to attend the offices of ICES to inspect compliance with the agreement, describes the permissible uses and disclosures that may be made of the personal health information by ICES and sets out the administrative,

technical and physical safeguards that ICES must implement in order to safeguard the personal health information. It also requires ICES to notify the Canadian Stroke Network as soon as it becomes aware of a breach of the agreement or if personal health information is stolen, lost or accessed by unauthorized persons.

The Canadian Stroke Network has also entered into an agreement with the electronic services provider it has retained to host, maintain and provide technical support for the web-based data collection tool. Given the electronic services provider does not have access to personal health information, but rather de-identified information, the agreement describes the permissible uses and disclosures of the de-identified information.

Both of the above noted agreements, however, state that the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network is not only a prescribed person within the meaning of the *Act*, but is also a health information custodian within the meaning of the *Act*.

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network has been prescribed, pursuant to section 13 of Regulation 329/04 to the *Act*, as a prescribed person that compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care. Accordingly, in respect of the Registry of the Canadian Stroke Network, the Canadian Stroke Network is a prescribed person within the meaning of subsection 39(1)(c) of the *Act* and not a health information custodian. It is therefore recommended that these agreements be amended accordingly.

A *Participation Agreement* has also been entered into with each regional stroke centre, enhanced district stroke centre and secondary prevention clinic from which the Canadian Stroke Network collects personal health information for purposes of the Registry of the Canadian Stroke Network. The agreement describes the permissible uses and disclosures of the personal health information that may be made by the Canadian Stroke Network and sets out the administrative, technical and physical safeguards that will be implemented to safeguard the personal health information. However, it does not require the Canadian Stroke Network to notify the regional stroke centre, enhanced stroke centre or secondary prevention clinic in the event of a breach of the *Participation Agreement* or in the event of an information breach.

It is recommended that the *Participation Agreement* be amended accordingly in order to ensure that health information custodians may fulfill their obligations under subsection 12(2) of the *Act* to notify individuals to whom the personal health information relates, at the first reasonable opportunity, if the personal health information is stolen, lost or accessed by unauthorized persons.

Privacy and Security Training

The *Confidentiality of Data Policy* states that all personnel of the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, including employees, staff, students and associates, must receive a formal orientation on the principles of privacy, confidentiality

and security. This orientation is formalized in a PowerPoint presentation entitled *Safeguarding Personal Health Information: Privacy Law and the Registry of the Canadian Stroke Network*.

Further, with respect to ongoing training, the *Canadian Stroke Network Privacy Policy* states that on an ongoing basis, the Canadian Stroke Network makes staff aware of the importance of maintaining the confidentiality of personal health information.

The Canadian Stroke Network also advised that it is in the process of developing web-based training for initial privacy and security orientation, as well as ongoing privacy and security training.

It is unclear however, from a review of the documentation, who is responsible for providing both the initial privacy and security orientation and the ongoing privacy and security training, when the initial privacy and security orientation is provided, how the Canadian Stroke Network keeps track of attendance at the initial privacy and security orientation and the ongoing training, who is responsible for tracking attendance and the consequences for failing to attend. Further, it is unclear whether attendance at the ongoing training is mandatory, what the frequency is of the ongoing training and what the content is of this ongoing privacy and security training.

The Canadian Stroke Network advised that with respect to the initial privacy and security orientation, the orientation is provided prior to having access to personal health information or health information, as the case may be, and that attendance is tracked using a *Confidentiality Agreement and Privacy Orientation Tracking Log*. With respect to ongoing privacy and security training, the Canadian Stroke Network advised that ongoing privacy and security training is provided every two years in the form of a workshop, however, while this training is mandatory, attendance is not documented or tracked and the content is not formalized.

It is recommended that the Canadian Stroke Network develop and implement a policy and associated procedures governing privacy and security training. The policy and associated procedures should stipulate that attendance at both the initial privacy and security orientation and the ongoing training is mandatory, to articulate when the initial privacy and security orientation will be provided and to state the frequency of the ongoing privacy and security training.

The policy and associated procedures should also articulate the person(s) responsible for delivering the initial privacy and security orientation and ongoing privacy and security training and describe the process that will be used to track attendance, including who will track attendance and the consequences for failing to attend.

Further, the content of the initial privacy and security orientation as set out in *Safeguarding Personal Health Information: Privacy Law and the Registry of the Canadian Stroke Network*, discusses and explains the status of the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network as a prescribed person within the meaning of section 39(1) (c) of the *Act*, but it also suggests that the Canadian Stroke Network is a "health information custodian" in this capacity. For the reasons set out earlier in this report, any such reference

should be removed. It is also recommended that the initial privacy and security orientation be expanded to explain the:

- Privacy and security policies and procedures implemented by the Canadian Stroke Network, including the *Canadian Stroke Network Privacy Policy*, and the obligations imposed as a result of these policies and procedures;
- Provisions in the *Confidentiality Agreement* and the duties and obligations imposed as a result of executing the *Confidentiality Agreement*,
- Responsibilities imposed by the *Information Breach Policy* with respect to the identification, notification and containment of an information breach;
- The roles and responsibilities of the Privacy Officer; and
- The physical, administrative and technical safeguards implemented by the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, including the responsibilities imposed in implementing these safeguards.

It is further recommended that the ongoing privacy and security awareness training be formalized and that it include role-based training in order to ensure that agents understand how to apply the privacy and security policies, procedures and practices in their day-to-day work, and to address any new privacy and security policies, procedures and practices implemented and significant amendments to existing privacy and security policies, procedures and practices.

Audit Program

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network conducts audits to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information, including the review of twelve different audit logs and conducting threat and risk assessments, vulnerability assessments and security reviews.

All access to the Registry of the Canadian Stroke Network is recorded in an audit log that includes the date and time of the connection, the name of the user account making the connection and the date and time of the disconnection, including invalid or failed attempts. In addition, all operations and actions that create, modify, delete or retrieve the information are recorded in an audit log. Depending on the nature of the audit log, these audit logs are reviewed either on a weekly or daily basis and any information in the audit log that is indicative of a privacy breach, attempted privacy breach or suspected privacy breach must be immediately reported to the Privacy Officer.

The reviews conducted however, are not consolidated in one document. It is further unclear from a review of the documentation, with respect to each such review, what the mechanism and format is for reporting the findings of the review, to whom the findings of the review are reported and the procedure used in tracking the findings of the review and how the findings were addressed.

It is recommended that the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network develop and implement a policy and associated procedures respecting the privacy and security audits conducted. It is further recommended that the policy or associated procedures set out the types of 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.

7. Technical Safeguards Implemented

The Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network has implemented a number of technical safeguards to protect personal health information in its custody or control.

The Registry of the Canadian Stroke Network is located on a server that is moated, meaning, that it is not networked to the local area network, it is not connected to the internet and it has no drives or peripherals that allow for duplication or copying. It also uses firewalls and network encryption and intrusion detection systems. The data centre where the web-based data collection module of the Registry of the Canadian Stroke Network is hosted uses multiple firewalls, network encryption and intrusion detection systems and an encrypted web-browser using 128-bit secure socket layer encryption.

When personal health information is collected through chart abstraction, the personal health information is entered on laptop computers which are equipped with biometric fingerprint authentication and the personal health information is encrypted as it is being entered. A program contained on each laptop computer then creates a table of personal information that is separate from the de-identified health information and automatically creates a unique Registry of the Canadian Stroke Network identification number. This table of personal information is also additionally encrypted with a decryption algorithm thereby resulting in two levels of encryption. Information from the laptop computer is electronically transferred over a secure telephone line to the Registry of the Canadian Stroke Network. The laptop computer cannot gain access to the server containing the Registry of the Canadian Stroke Network unless it is authenticated using two factor authentication.

In addition, when personal health information is collected through the web-based data collection tool, it is segmented into an anonymized subset and an encrypted subset and a unique identification number is automatically created. Both the anonymized subset and encrypted subset, which contains the personal identifiers, are transmitted to the data centre where the web-based data collection module is housed through 128-bit secure socket layer encryption. However, the electronic services provider does not have access to the encrypted subset given it does not have the encryption key to decrypt the identifiers.

Further, the Canadian Stroke Network ensures that threat risk assessments and security reviews are conducted on the information technology infrastructure and related applications of the

Registry of the Canadian Stroke Network in order to identify real and potential threats, to assess vulnerabilities and to provide mitigation strategies. The Canadian Stroke Network also requires that vulnerability assessments be conducted every two years and following any significant programming and design changes to the Registry of the Canadian Stroke Network. Since the last review of its practices and procedures in 2005, the Canadian Stroke Network retained a third party to conduct vulnerability assessments on the computing infrastructure of the Registry of the Canadian Stroke Network on two occasions - November 26, 2006 and January 3, 2007.

8. Physical Safeguards Implemented

The Registry of the Canadian Stroke Network is located in a locked facility with internal and external video monitoring, glass breakage detectors 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. Further, the data centre where the web-based data collection module is hosted is located in a locked facility with twenty-four hour security personnel, continuous video monitoring, an iris scanner biometric identification system for identity confirmation and tracked card access.

Summary of Recommendations

It is recommended that the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network address the recommendations detailed in this report prior to the next review of its practices and procedures. In summary, it is recommended that the Canadian Stroke Network:

1. Amend the *Information Breach Policy* to expand the definition of "information breach," to address inconsistencies with respect to the reporting and containment of an information breach, to identify what information with respect to an information breach must be reported to the Privacy Officer and the format for this report, to require that all information breaches be documented, to require notification to the health information custodian who provided the personal health information in the event of an information breach and to ensure that amendments to existing policies and procedures be considered for all information breaches.

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 and address inconsistencies between and among the privacy and security policies and procedures implemented.

4. Develop and implement a written policy and procedure with respect to the de-identification and anonymization of personal health information.

5. Refine its policies, procedures and practices relating to the secure destruction of records of personal health information, including:

   (a) Amending the *Document Shredding Policy* to set out the type of shredding that is employed for records of personal health information in paper format and ensuring 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*;

   (b) Developing and implementing written policies and procedures with respect to the secure destruction of records in electronic format; and

   (c) Amending the *Data Destruction Policy* to establish a process for tracking whether the principal investigator has executed a document attesting to destruction within a reasonable time after the destruction date has passed and to stipulate the required content of the document attesting to destruction that must be executed.

6. Amend the *Confidentiality Agreement Policy* and the *Confidentiality Agreement* in accordance with the comments provided in this report.

7. With respect to privacy and security training:

   (a) Develop and implement a written policy and associated procedures governing both initial privacy and security orientation and ongoing privacy and security training; and

   (b) Amend the content of the initial privacy and security orientation in accordance with the comments provided in this report;

   (c) Formalize the content of ongoing privacy and security training and ensure that it includes role-based training and that it addresses new privacy and security policies, procedures and practices implemented by the Canadian Stroke Network and significant amendments to existing privacy and security policies, procedures and practices.

8. Amend the agreement with the agent retained to safeguard the Registry of the Canadian Stroke Network and the electronic services provider retained to host, maintain and provide support services for the web-based data collection tool to clarify that the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network is a prescribed person as defined in subsection 39(1)(c) of the *Act* and not a health information custodian and amend the *Participation Agreement* to require the Canadian Stroke Network to provide notification at the first reasonable opportunity if there has been a breach of the

Participation Agreement or if personal health information is stolen, lost or accessed by unauthorized persons.

9. Develop and implement a written policy and associated procedures for the conducting of privacy and security audits.

Statement of Continued Approval of Practices and Procedures

The IPC is satisfied that the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network 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 Canadian Stroke Network 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 Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network that were approved by the IPC effective October 31, 2005:

1. Ensure that all individuals affiliated with the Canadian Stroke Network who have access to information in the Registry of the Canadian Stroke Network complete privacy and security training specific to the *Act*.

2. Ensure that all persons affiliated with the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network who have not yet signed a Confidentiality Agreement with the Canadian Stroke Network 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 the Canadian Stroke Network.

4. Develop a privacy poster that briefly describes the Registry of the Canadian Stroke Network and the Canadian Stroke Network; the personal health information that is collected; from whom the personal health information is collected; how the information is used and disclosed; and how individuals may withdraw consent to having their personal health information disclosed to and included in the Registry of the Canadian Stroke Network. 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 procedure and the privacy policy 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 the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network.

5. Amend the agreement between the Canadian Stroke Network and the Institute for Clinical Evaluative Sciences to clarify that, in respect of the services provided by the Institute for Clinical Evaluative Sciences relating to the storage and safeguarding of personal health information in the Registry of the Canadian Stroke Network, the Institute for Clinical Evaluative Sciences is an agent of the Canadian Stroke Network as defined in the *Act* and, as such, must abide by all of the requirements and restrictions on agents set out in the *Act*.

6. Conduct regular 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