Information
and Privacy
Commissioner of
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the Institute for Clinical Evaluative Sciences:

A Prescribed Entity 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 Institute for Clinical Evaluative Sciences:

A Prescribed Entity 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 entities pursuant to section 45 of the *Act*.

Statutory Provisions Relating to the Disclosure to Prescribed Entities

Subsection 45(1) of the *Act* permits health information custodians to disclose personal health information to a prescribed entity, without consent, for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system. The following entities, including registries maintained within these entities, have been prescribed for purposes of subsection 45(1) of the *Act*:

- Cancer Care Ontario;
- Canadian Institute for Health Information;
- Institute for Clinical Evaluative Sciences; and
- Pediatric Oncology Group of Ontario.

In order for a health information custodian to be permitted to disclose personal health information to a prescribed entity without consent, the prescribed entity 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 45(3) of the *Act*.

These practices and procedures must also be reviewed by the IPC every three years from the date of their initial approval, pursuant to subsection 45(4) of the *Act*, in order for a health information custodian to be able to continue to disclose personal health information to a prescribed entity without consent, and in order for a prescribed entity to be able to continue to collect, use and disclose personal health information without consent as permitted by 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.

Initial Review of the Practices and Procedures of the Prescribed Entities

In 2005, the IPC reviewed the practices and procedures implemented by each of the prescribed entities to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information. Following this review, the IPC approved the practices and procedures of each of the prescribed entities effective October 31, 2005.

While the IPC was satisfied that the prescribed entities 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 Institute for Clinical Evaluative Sciences, 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 Institute for Clinical Evaluative Sciences.

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

Subsection 45(4) of the *Act* requires the IPC to review the practices and procedures implemented by each of the prescribed entities every three years from the date that they were initially approved by the IPC, being October 31, 2005, and to advise whether the prescribed entities continue to meet the requirements of the *Act*. As a result, the IPC was again required to review the practices and procedures implemented by the prescribed entities and to advise whether they continued to meet the requirements of the *Act* 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 each prescribed entity 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 by the IPC and additional documentation and necessary clarifications were requested. The Institute for Clinical Evaluative Sciences submitted the requested documentation on March 28, 2008, and submitted additional documentation on April 22, 2008 and May 20, 2008.

Once the additional documentation and necessary clarifications were received, an on-site meeting was held. The purpose of the on-site meeting was to discuss the practices and procedures implemented by the prescribed entity and to provide the IPC with an opportunity to ask questions

arising from the documentation. The on-site meeting with the Institute for Clinical Evaluative Sciences was held on May 28, 2008.

Following the on-site meeting, each prescribed entity 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. The draft report was submitted to the prescribed entity for review and comment prior to the report being finalized and 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 entity pursuant to its function as a prescribed entity under section 45 of the *Act* and not with respect to any other role or responsibility that the prescribed entity may have assumed under the *Act*.

Description of the Institute for Clinical Evaluative Sciences

The Institute for Clinical Evaluative Sciences ("ICES") is an independent not-for-profit organization that collects personal health information in order to analyze and report on the effectiveness, quality, equity and efficiency of health care and health-related services in the Province of Ontario and in order to inform and assist policy-makers in managing, evaluating, monitoring and planning the delivery of health services and in improving outcomes of care.

At the time of the initial review of its practices and procedures in 2005, ICES was geographically located at one site. Since that time, ICES has continued as a single organization, but it is now geographically located at two sites. This evolution is referred to as "Pan-Ontario ICES." The first satellite site was opened at Queen's University in October 2007, and is known as ICES-Queen's. Other sites are currently being contemplated. Each satellite site is required to adhere to all of the privacy and security policies, procedures and practices implemented by ICES.

Three-Year Review of the Institute for Clinical Evaluative Sciences

1. Privacy and Security Governance and Accountability Framework

The President and Chief Executive Officer of ICES, who reports directly to the Board of Directors, is ultimately accountable for ensuring that ICES complies with the *Act* and with the privacy and security policies, procedures and practices implemented by ICES. The Chief Privacy Officer, who reports to the Chief Operating Officer of ICES, has been delegated the day-to-day authority to manage the privacy program.

The Chief Privacy Officer is responsible for the development, implementation, review, maintenance and adherence to the privacy policies, procedures and practices implemented by ICES and for ensuring compliance with the *Act*. In addition, the Chief Privacy Officer is responsible for:

- Developing, implementing and ensuring compliance with *Data Sharing Agreements*;
- Overseeing, directing or delivering privacy and security training;
- Facilitating and promoting activities to foster information privacy awareness; and
- Documenting, investigating and remediating privacy complaints and privacy breaches.

Each satellite site is also required to have a Privacy Officer who reports to the Chief Privacy Officer of ICES. The Privacy Officer is responsible for assisting in the development, implementation, review, maintenance and adherence of that satellite site to the privacy policies, procedures and practices implemented and for assisting the Chief Privacy Officer in ensuring that the satellite site complies with the *Act*.

Effective May 20, 2008, ICES has also retained a Chief Information Security Officer. The Chief Information Security Officer, who also reports to the Chief Operating Officer, is responsible for providing input into and oversight of the security program at ICES.

ICES has also established a Confidentiality Committee with representatives from every role group at ICES including the Director of Data Management, the Manager of Information Systems, the Director of Monitoring and Reporting, the Manager of Administration, the Director of Research Co-ordination, the Director of Programming and Biostatistics, the Privacy Officer for ICES-Queen's and the Chief Privacy Officer. The Confidentiality Committee meets bi-weekly and its mandate is to design, implement, manage and evaluate privacy and security at ICES.

2. Overview of Privacy and Security Policies and Procedures

ICES has developed a privacy policy, *Privacy Code: Protecting Personal Health Information at ICES*, that describes its status as a prescribed entity under the *Act* and the obligations that arise from this status. It further sets out the accountability framework for ensuring compliance with the *Act* and for ensuring adherence to the privacy and security policies, procedures and practices implemented by ICES. ICES has also implemented numerous privacy and security policies and procedures that support the *Privacy Code: Protecting Personal Health Information at ICES*, including policies and procedures related to:

- Receiving, documenting, tracking, investigating and remediating privacy complaints;
- Protecting the confidentiality and security of personal health information;
- Access to personal health information and de-identified information;
- Research ethics board approval;
- Protecting personal health information on mobile devices;
- Retention and destruction of records of personal health information; and
- Identifying, containing, investigating, remediating and notifying of privacy breaches.

In 2006, ICES also began developing standard operating procedures for activities involving the collection of personal health information and the use and disclosure of de-identified information in order to enhance transparency and promote accountability with respect to these activities. The Director of Data Management identified all activities that required standard operating procedures and assigned author and owner responsibilities for developing the standard operating procedures.

Pursuant to the *Annual Policy Review Policy* and the *Standard Operating Procedures for Data Management Policy*, all privacy and security policies and procedures, including standard operating procedures, must be reviewed on an annual basis and revised as required. All amended policies and procedures are forwarded to the Operations Committee for approval prior to implementation.

Information Breach Policy

ICES has developed 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 in contravention of privacy and security policies and procedures implemented.

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 Chief Privacy Officer of the information breach. However, it is unclear what information with respect to an information breach must be reported to a supervisor and the Chief Privacy Officer and the format in which it must be reported. It is recommended that this be clarified in the *Information Breach Policy.*

The Chief Privacy Officer is then responsible for notifying other members of the Core Breach Team, including the Chief Executive Officer and Chief Operating Officer. The Core Breach Team will then determine the extent of the information breach, determine the process for notification, undertake notification and determine whether the information breach should be documented. It is unclear in what circumstances an information breach will not be documented. 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 ICES 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.

Policy and Procedure for De-Identification and Anonymization

It is also recommended that ICES 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 ICES 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.

It is also recommended that ICES explore new tools that are being developed to assist in the development of de-identification policies and procedures in order to ensure that these policies and procedures are based on an assessment of the actual risk of re-identification.

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

ICES makes information about its privacy and security policies, procedures and practices readily available on its website, **www.ices.on.ca**, including the *Privacy Code: Protecting Personal Health Information at ICES,* a brochure entitled *Our Business is Research, Our Priority…Privacy*, Frequently Asked Questions entitled *Questions and Answers About Information Privacy Protection at ICES* and contact information for the individuals responsible for ensuring compliance with these policies, procedures and practices and to whom complaints or inquiries can be made. The privacy and security policies and procedures implemented by ICES are also made readily available to staff on a centralized intranet resource.

ICES collects personal health information pursuant to its function as a prescribed entity under section 45 of the *Act*. As a prescribed entity under section 45 of the *Act*, ICES is permitted to use personal health information it has collected for the purposes set out in section 45 of the *Act* and section 18 of Regulation 329/04 to the *Act*. ICES may use personal health information it has collected under section 45 of the *Act* for the purpose of analysis or compiling statistical

information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system. ICES may also use personal health information it has collected under section 45 of the *Act* for the purposes of research, provided that it complies with the applicable research requirements in the *Act* and its regulation.

It appears that the public and other stakeholders may not clearly understand the purpose for which ICES collects personal health information and the purposes for which ICES may use personal health information under the *Act* and its regulation.

It is therefore recommended that the information made available to the public and stakeholders be amended to clearly set out the purposes for which ICES, as a prescribed entity under section 45 of the *Act*, collects and uses personal health information, the statutory authority for such collection and uses and the policies, procedures and practices and the applicable statutory requirements related to the collection and uses of the personal health information.

In addition, the information currently made available to the public and stakeholders does not reflect the fact that while ICES remains a single organization, ICES is now geographically located at two sites with further sites currently being contemplated as a result of the "Pan-Ontario ICES" initiative. It is recommended that ICES amend the information available to the public and stakeholders to discuss the "Pan-Ontario ICES" initiative and the consequences of this initiative on the privacy and security policies, procedures and practices implemented by ICES and to ensure that it continues to be accurate in light of the "Pan-Ontario ICES" initiative. For example, in *Our Business is Research, Our Priority…Privacy*, it states: "data is housed on an isolated secure system that can only be accessed by ICES faculty and staff within the building." This statement is no longer accurate given ICES-Queen's is able to access information remotely.

4. Collection, Use and Disclosure of Personal Health Information

Collection

ICES collects personal health information from the Ministry of Health and Long-Term Care for the Province of Ontario as well as other health information custodians such as hospitals, laboratories and health care practitioners. It also collects personal health information from prescribed persons that compile or maintain registries under subsection 39(1)(c) of the *Act*, such as the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network and the Cardiac Care Network of Ontario in respect of its registry of cardiac services, as well as from other prescribed entities under section 45 of the *Act*, including Cancer Care Ontario.

The personal health information collected by ICES pursuant to its function as a prescribed entity, falls into one of the following categories: administrative data, registry data, survey data and data abstracted from records of personal health information.

Most of the personal health information collected by ICES is administrative data, which is collected pursuant to agreements with the Ministry of Health and Long-Term Care, such as

the Ontario Drug Benefit Program and the Registered Persons Database. ICES also collects population-based registry databases such as the registry of cardiac services of the Cardiac Care Network of Ontario and the Registry of the Canadian Stroke Network of the Canadian Stroke Network, both prescribed persons within the meaning of subsection 39(1)(c) of the *Act*, as well as provincial and national survey databases such as the Statistics Canada Canadian Community Health Survey. Information is also abstracted from records of personal health information to augment, supplement and validate administrative and registry databases.

Since the initial review of its practices and procedures in 2005, ICES has commenced web-based collection of personal health information with respect to certain data holdings, including the Implantable Cardioverter Defibrillator Database.

Use

Personal health information collected for purposes of its function as a prescribed entity under section 45 of the *Act* is de-identified prior to its use for analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the health system or for research purposes. As a first use, personal health information is de-identified by removing personal identifiers such as name, address and telephone number and by inserting an encrypted identifier, known as the ICES Key Number (IKN), which is used to link de-identified information across multiple data holdings.

ICES does not use personal health information, that is, identifying information about an individual, for analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the health system pursuant to section 45 of the *Act*. ICES only uses de-identified information. Personal health information is de-identified by persons known as Data Covenantors. Data Covenantors have access to personal health information for purposes of removing personal identifiers, for purposes of inserting an encrypted identifier and for purposes of record linkage.

Prior to the use of personal health information for research purposes, ICES requires that a research plan be prepared and that the research plan be approved by a research ethics board in accordance with the *Act* and its regulation. Prior to any use of de-identified information for analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the health system, ICES requires that a research plan be prepared. It also requires that research ethics board approval be obtained. In addition, ICES requires that a *Project Specific Privacy Impact Assessment Form* be completed which addresses all the requirements that must be satisfied for the use of this information for these purposes pursuant to the *Act*.

In this regard ICES has implemented a policy, the *Ethics Review Process Policy*, which attempts to set out the circumstances in which the approval of a research ethics board is required.

It is recommended that the *Ethics Review Process Policy* be amended to make explicit that ICES requires research ethics board approval prior to the use of personal health information for research purposes pursuant to the *Act* and its regulation, and for the use of personal health

information for the purpose described in section 45(1) of the *Act*, regardless of the fact that the personal health information is de-identified prior to use. It is also recommended that the *Ethics Review Process Policy* be amended to clarify when and in what circumstances the research ethics board approval must be a project-specific approval and when and in what circumstances expedited approval or modified expedited approval may be obtained.

Disclosure

ICES does not disclose personal health information except where required by law. Rather, ICES only discloses aggregate information with cell sizes of five or less generally being suppressed. Although ICES does not disclose personal health information for research purposes, but rather only discloses aggregate information, ICES nonetheless requires that the provisions in the *Act* and its regulation relating to the disclosure of personal health information for research purposes be complied with.

In particular, prior to the disclosure of aggregate information for research purposes, ICES requires that a research plan be prepared that meets the requirements of the *Act* and requires that the research plan be approved by a research ethics board. In addition, a *Project Specific Privacy Impact Assessment Form* must be completed that addresses all the requirements that must be satisfied prior to the disclosure of personal health information for research purposes pursuant to the *Act* and its regulation.

5. Retention and Destruction of Personal Health Information

Personal health information is only retained by ICES for as long as necessary for the fulfillment of the purposes for which it is collected as set out in the *Project Specific Privacy Impact Assessment Form* and the research plan approved by a research ethics board or as set out in a *Data Sharing Agreement*. ICES requires that a *Data Sharing Agreement* be executed prior to the collection of administrative data, population-based registry databases and survey databases.

Destruction of Records of Personal Health Information in Paper Format

ICES 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 irreversible shredding. All records of personal health information in paper format must be placed in locked bins marked "confidential" and are shredded on-site by a third-party service provider with whom ICES has entered into an agreement. A staff member from ICES is present each time that the "confidential" bins are collected and the contents shredded. The third-party service provider provides a certificate of destruction to ICES confirming that the destruction was carried out.

It is recommended however, that the agreement between ICES and the third-party service provider be amended to ensure consistency with Order HO-001 and with the provisions set out in *Fact Sheet 10: Secure Destruction of Personal Information,* issued by the IPC.

In particular, it is recommended that the agreement be amended to explicitly state that the third- party service provider shall destroy the records of personal health information in a secure manner, to provide a definition of secure destruction consistent with subsection 1(5.1) of Regulation 329/04 to the *Act* and to specify the manner in which personal health information will be securely destroyed, including under what conditions and by whom. The agreement should also require the third-party service provider to provide a certificate of destruction setting out the date, time, location and method of secure destruction employed and bearing the signature of the person who performed the secure destruction and to require the third-party service provider to agree that:

- Its services will be performed in a professional manner, in accordance with industry standards and practices and by properly trained employees and agents;
- Its employees and agents understand that a breach of the security and confidentiality of the information may lead to disciplinary measures; and
- If the services of another third-party will be engaged, that ICES will be notified in advance, that the third-party will be required by written contract to comply with all the same terms and conditions as the third-party service provider and that a copy of the written contract will be provided to ICES.

Destruction of Records of Personal Health Information in Electronic Format

ICES has developed and implemented a written policy and procedure with respect to the secure destruction of records in electronic format. The *Data Destruction Policy* and the *Destroying Hardware Standard of Procedure* require that all hard drives and tapes be wiped with a magnetizing device and be physically destroyed. The *Destroying Hardware Standard of Procedure* also requires that all other electronic media, such as CDs, DVDs, disks and memory keys, be physically destroyed thereby rendering the media unusable.

Data Destruction Policy

Pursuant to the *Data Destruction Policy*, the Director of Data Management is responsible for monitoring destruction dates and for notifying the principal investigator named in the *Data Sharing Agreement* or research plan of the pending destruction date. Once the date of destruction has passed, the principal investigator is asked to attest to the destruction. It is recommended that the *Data Destruction Policy* be amended to set out the content of the document attesting to destruction that must be signed by the principal investigator, and that the content include the date, time, location and method of secure destruction employed.

Further, the *Data Destruction Policy* states that with respect to project-level datasets, the Director of Data Management will generate a report that will be provided to the Chief Privacy Officer, the Director of Programming and Biostatistics, the Director of Research Coordination and the Manager of Information Systems if the destruction date has passed without the principal investigator "signing off" on destruction. These individuals are then responsible for following up with the principal investigator and for destroying the information within one week of the

report. It is recommended that this same procedure be adopted for information received pursuant to *Data Sharing Agreements*.

Tracking Dates of Destruction

Dates of destruction are tracked by ICES using a *Data Sharing Agreement Log* and *Primary Data Collection Tracking Log*. It is noted however, that the information in the *Data Agreement Log* and the *Primary Data Collection Tracking Log*, which are used to track the date of destruction and the date of termination of the *Data Sharing Agreements*, are not always completed by the project manager. Failure to complete this information may result in information being retained for longer than is necessary to meet the purposes for which the information was collected and in contravention of *Data Sharing Agreements* and research plans approved by a research ethics board.

It is therefore recommended that ICES implement a process to ensure that the date of destruction and the date of termination in the *Data Agreement Log* and the *Primary Data Collection Tracking Log* are completed by the project manager prior to the collection of personal health information by ICES. It is also recommended that the *Data Agreement Log* and *Primary Data Collection Tracking Log* be amended to include a column entitled "Actual Date of Destruction" to record the date that the information was actually destroyed in accordance with the *Data Sharing Agreem*ents and in accordance with the research plans approved by the research ethics boards.

6. Administrative Safeguards Implemented

In addition to privacy and security policies and procedures, ICES has implemented the following administrative safeguards to protect personal health information against theft, loss and unauthorized use, disclosure, copying, modification and disposal.

Privacy and Security Training

All staff at ICES, including scientists, fellows and students, are required to attend privacy and security orientation at the commencement of their relationship with ICES and prior to being given access to health information pursuant to the *Privacy and Security Training Policy*.

The privacy and security orientation discusses the status of ICES as a prescribed entity under the *Act* and the obligations that arise from this status. It also explains the various policies, procedures and practices implemented by ICES to protect the privacy of individuals whose personal health information it receives and to protect the security of that information, including the requirements imposed on staff as a result of these policies, procedures and practices. The role of the Chief Privacy Officer and the physical, administrative and technical safeguards implemented to protect personal health information against theft, loss and unauthorized use and disclosure, including the responsibilities of staff in implementing the safeguards, is also discussed.

With respect to ongoing privacy and security training, the *Privacy and Security Training Policy* requires all staff to undergo annual computer-based privacy and security training.

Attendance at the initial privacy and security orientation, as well as the annual computer-based privacy and security training, is tracked. With respect to the initial privacy and security orientation, attendance is logged manually using a spreadsheet setting out the name and title of the individual, the supervisor to whom the individual reports and the date that the orientation was attended. With respect to the annual computer-based training, attendance is tracked automatically through logs. Failure to attend the orientation or the annual training results in the denial of access to health information or the termination of the employment, contractual or other relationship with ICES.

Confidentiality Agreements

The *Confidentiality Agreement Policy* requires every person affiliated with ICES, including staff, scientists, fellows, students, consultants and contractors, to sign a *Confidentiality Agreement* at the commencement of their relationship with ICES and prior to being given access to health information. It further requires that the *Confidentiality Agreement* be signed on an annual basis thereafter. Execution of the *Confidentiality Agreement* is tracked and electronic logs are maintained.

Every person that signs the *Confidentiality Agreement* agrees to familiarize him or herself with and to comply with all the privacy and security policies, procedures and practices implemented by ICES. They further agree not to use health information except as necessary to perform their functions, to not disclose personal health information except as required by law, to notify the Chief Privacy Officer immediately upon becoming aware of any breach or possible breach of the *Confidentiality Agreement* and to acknowledge that a breach of the *Confidentiality Agreement* may result in disciplinary action up to and including a termination of the relationship with ICES.

Data Sharing Agreements

Prior to the collection of administrative data, population-based registry databases and provincial and national survey databases, ICES requires that a *Data Sharing Agreement* be entered into. The *Data Sharing Agreement* is required to specify the personal health information governed by the *Data Sharing Agreement*, the intended use of the information, the retention period, the projected date of destruction and the physical, administrative and technical safeguards that will be implemented.

It is recommended that the template *Data Sharing Agreement* be amended to clearly set out the purpose for which ICES is collecting the personal health information, the statutory authority for this collection and the statutory conditions, if any, that apply to the collection of the personal health information.

In addition, it is recommended that the template *Data Sharing Agreement* be amended to accurately reflect the status of the person from whom ICES is collecting personal health information, namely whether the person is a health information custodian, another prescribed entity pursuant to section 45 of the *Act* or a prescribed person that compiles or maintains a registry pursuant to subsection 39(1)(c) of the *Act*. For example, in the *Data Sharing Agreement* with the Canadian

Stroke Network it states that the Canadian Stroke Network is a health information custodian. However, the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network is a prescribed person pursuant to subsection 39(1)(c) of the *Act*.

The template *Data Sharing Agreement* should also be amended to require ICES to securely destroy records of personal health information when the terms of the *Data Sharing Agreement* require that the information be destroyed, to provide a definition of secure destruction consistent with subsection 1(5.1) of Regulation 329/04 to the *Act* and to require ICES to provide a certificate of destruction setting out the setting out the date, time, location and method of secure destruction employed and bearing the signature of the person who performed the secure destruction.

It is also recommended that the provisions in the template *Data Sharing Agreement* that restrict ICES from contacting the individual to whom the personal health information relates and from using and disclosing personal health information in a form in which the individual can be identified unless ICES has received the prior written authority of the "data custodian," be amended to further restrict the contact, use or disclosure, as the case may be, to circumstances where the contact, use or disclosure is permitted by law.

Audits

ICES has implemented a number of audits to safeguard personal health information against unauthorized use and disclosure including audits of personal computers and laptop computers to ensure that network, client operating system and Outlook passwords comply with the *Password Policy* and to ensure that personal health information, that is identifying information, is not contained on personal computers, on portable media or in email transmissions. In addition, the Director of Data Management reviews access permissions to administrative data and population- based registry databases on a monthly basis to ensure that access permissions are still appropriate.

Further, the web-based data collection applications are monitored daily to detect malicious or suspicious activities. Where an event is categorized as a "security alert," namely an attempt by an individual to access information to which the individual has no right of access, an email is automatically sent to one of two individuals and a security incident response team is engaged.

Risk Management Framework

ICES has developed an integrated risk management framework to identify corporate risks, to identify the impact of these risks, to assess the likelihood of these risks and to establish recommendations for remediation. In addition, prior the commencement of a project, the project manager is required to develop a Risk Management Plan and a Risk Register to identify, document, manage and reduce risks inherent in the project. The Risk Management Plan is required to set out:

- The process to identify, analyze, evaluate and remediate risks throughout the project;

- The process for transferring approved risk costing into the budget;
- How often the Risk Register will be reviewed, the review process and the participants;
- Who is responsible for what aspects of risk management; and
- How risk status will be reported and to whom.

The Risk Register is required to detail all identified risks for the project, to grade the risks in terms of both the likelihood of the risk occurring and the seriousness of the impact of the risk on the project, the strategy for mitigating each risk, the costs associated with the mitigation strategy for each risk and the person (s) responsible for each mitigation strategy.

7. Physical Safeguards Implemented

ICES 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.

In addition, ICES has implemented a *Building Security Policy* which requires that all staff visibly display photo identification cards at all times and a *Visitor Policy* which requires all visitors to sign in at reception noting the date and time of arrival and the number on the identification card issued. The identification cards are issued to all visitors and must be worn at all times while in the facility. Visitors must return the identification card and sign out at reception upon departure and must record the time of departure. Signs are posted in all meeting rooms and boardrooms reminding visitors to return to reception prior to their departure in order to return their identification card and sign out.

Similar physical safeguards exist at ICES-Queen's, the satellite site located at Queen's University.

8. Technical Safeguards Implemented

In addition to de-identifying personal health information and inserting an encrypted identifier prior to its use pursuant to section 45 of the *Act* for purposes of analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the health system, ICES has implemented a number of other technical safeguards to protect personal health information in its custody or control.

The technical safeguards implemented include the use of firewalls, network encryption and intrusion detection systems and audits of local area networks and secured networks. They also include placing data holdings on isolated servers with no connections to the network or internet and with no drives or peripherals thereby making them inaccessible externally except to satellites sites, including ICES-Queen's, through an encrypted and dedicated line.

ICES has also developed a policy for *Protecting Personal Health Information on Mobile Devices* which requires that personal health information collected or transmitted on mobile devices be encrypted and password protected, in addition to the mobile device either being password protected or being equipped with biometric authentication.

A mandatory, standardized and system-wide password-protected screen saver has also been implemented for all computers after a timeout period of ten minutes and a *Password Policy* has been implemented which is consistent with current industry standards.

Finally, ICES retains third parties to conduct regular penetration testing, vulnerability assessments, threat-risks assessments, security assessments and security reviews. In particular, third-party risk assessments and penetration testing are conducted on an annual basis.

Currently, the Senior Web Developer and the Manager of Information Systems each maintain their own log of recommendations arising from penetration testing, vulnerability assessments, threat-risk assessments, security assessments and security reviews and the Chief Privacy Officer maintains her own log of recommendations arising from privacy impact assessments.

It is recommended that ICES develop and maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, penetration testing, vulnerability assessments, threat-risk assessments, security assessments and security reviews. This consolidated and centralized log should be updated regularly and should set out how each recommendation was addressed, when each recommendation was addressed and by whom the recommendation was addressed. For those recommendations that have yet to be addressed, it is recommended that the log set out how each recommendation will be addressed, the date by which each recommendation will be addressed and who is responsible for addressing each recommendation.

Maintaining a consolidated and centralized log ensures transparency, promotes accountability and assists in ensuring that all recommendations are adequately addressed in a timely manner in order to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of the personal health information.

Summary of Recommendations

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

1. Amend the *Information Breach Policy* to identify what information with respect to an information breach must be reported to the Chief 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 both internal and external information breaches.

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

3. Amend the information made available to the public and stakeholders to:

   (a) Clearly set out the purposes for which ICES, as a prescribed entity under section 45 of the *Act*, collects and uses personal health information, the statutory authority for such collection and uses and the policies, procedures and practices and the applicable statutory requirements related to the collection and uses of the personal health information;

   (b) Discuss the "Pan-Ontario ICES" initiative and the consequences of this initiative on the privacy and security policies, procedures and practices of ICES; and

   (c) Ensure that it continues to be accurate in light of the "Pan-Ontario ICES" initiative.

4. Amend the *Ethics Review Process Policy* to set out when and in what circumstances research ethics board approval is required and when and in what circumstances the research ethics board approval must be project-specific and when and in what circumstances the approval may be an expedited approval or a modified expedited approval.

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

   (a) Amending the agreement with the third-party service provider retained to securely destroy records of personal health information in accordance with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC;

   (b) Amending the *Data Destruction Policy* pursuant to the comments in this report;

   (c) Implementing a process to require that the date of destruction and the date of termination in the *Data Agreement Log* and the *Primary Data Collection Tracking Log* be completed prior to the collection of personal health information by ICES; and

   (d) Amending the *Data Agreement Log* and *Primary Data Collection Tracking Log* to include a column entitled "Actual Date of Destruction" to record the date that the information was actually destroyed in accordance with the *Data Sharing Agreements* and research plans approved by the research ethics boards.

6. Amend the template *Data Sharing Agreement* with health information custodians, prescribed persons that compile or maintain registries pursuant to subsection 39(1)(c) of the *Act* and other prescribed entities under section 45 of the *Act*, from whom ICES collects personal health information, in accordance with the comments provided in this report.

7. Develop and maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, penetration testing, vulnerability assessments, threat-risk assessments, security assessments and security reviews.

Statement of Continued Approval of Practices and Procedures

The IPC is satisfied that ICES 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 ICES 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 ICES that were approved by the IPC effective October 31, 2005:

1. Amend the Confidentiality Agreement to include references to the *Act*, to reference and define personal health information, to include provisions outlining the consequences for violations of privacy and security practices and procedures and to include provisions requiring agents to familiarize themselves with and comply with the practices and procedures relating to privacy and security implemented by ICES.

2. Ensure that all agents of ICES complete privacy training and that the web-based privacy orientation module is amended to ensure that staff is advised of ICES' role as a prescribed entity and the significance and consequences of this designation.

3. Amend all documentation to replace references to Bill 31 or the *Freedom of Information and Protection of Privacy Act* with references to the *Act*.

4. Amend all internal and external documentation to reflect ICES's status as a prescribed entity under section 45 of the *Act*.

5. When completed, provide to the IPC a copy of the agreement between ICES and the Ministry of Health and Long-Term Care.

6. Clearly document follow-up on all recommendations from future internal or external privacy and security audits.

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

APPENDIX "B"

DOCUMENTATION REQUESTED

Privacy

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

Security

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

- encryption, firewalls and virus scanners
- secure transfer procedures
- password policies
- audit trails

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

Organizational and Other Documentation

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