REPORT OF THE INFORMATION AND PRIVACY COMMISSIONER

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

Responsibilities of Prescribed Entities

Section 45(1) of *PHIPA* permits health information custodians to disclose personal health information without consent to certain prescribed entities 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, including the delivery of services, provided the prescribed entities meet the requirements of section 45(3).

Section 45(3) of *PHIPA* requires each prescribed entity to have in place practices and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Section 45(3) further requires each prescribed entity to ensure that these practices and procedures are approved by the IPC prior to November 1, 2005, in order for health information custodians to be able to disclose personal health information to the prescribed entity without consent and for the prescribed entity to:

- be able to collect personal health information from health information custodians;
- use personal health information as if it were a health information custodian for purposes of section 37(1)(j) or section 37(3) of *PHIPA*;
- disclose personal health information as if it were a health information custodian for purposes of sections 44, 45 and 47 of *PHIPA*;
- disclose personal health information back to health information custodians who provided the personal health information; and
- disclose personal health information to governmental institutions of Ontario or Canada as if it were a health information custodian for purposes of section 43(1) (h).

Section 18(2) of Regulation 329/04 to *PHIPA*, further requires each prescribed entity to make publicly available a plain language description of its functions including a summary of the practices and procedures described above to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information.

Mandate of the IPC with Respect to Prescribed Entities

Prescribed entities must ensure that their practices and procedures to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information are reviewed and approved by the IPC prior to November 1, 2005. Thereafter, the IPC must review these practices and procedures every three years from the date of approval.

Review Process

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

Human Resources

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

Privacy

- Privacy policies and procedures that describe how the organization adheres to each fair information practice
- Privacy brochure – available upon request to the public
- Privacy Impact Assessments – for programs/database holdings
- Internal/external privacy audits
- Privacy crisis management protocols
- Data linkage protocols
- Procedures for de-identifying data
- Retention schedules and disposal procedures
- Inventory of all data holdings of personal health information
- Protocol for reviewing proposals in terms of their privacy impacts
- Mechanism for reviewing and updating privacy policies and procedures

Security

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

The prescribed entities were informed that they were required to implement privacy and security measures and safeguards commensurate with the nature of the work undertaken by the prescribed entity, the amount and sensitivity (e.g., level of identifiability) of the information in the custody and control of the prescribed entity and the number and nature of the individuals who have access to personal health information. The scope of the review was to include practices and procedures relating to all personal health information in the custody and control of the prescribed entity. The review was not limited to personal health information collected, used and disclosed by the prescribed entity for purposes of section 45 of *PHIPA*.

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

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

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

Description of the Prescribed Entity

The Institute for Clinical Evaluative Sciences (ICES) is a prescribed entity under section 45 of *PHIPA.*

ICES is an independent, non-profit organization that conducts analyses on health services data to enhance the effectiveness of health care for Ontarians. ICES uses population-based health information to generate knowledge that provides evidence to support health policy development and changes to the organization and delivery of health care services. The knowledge generated by ICES provides fact-based measures of health system performance; a clearer understanding of the shifting health care needs of Ontarians; and a stimulus for discussion of practical solutions to optimize scarce resources.

Key to ICES's work is its ability to link population-based health information on an individual patient basis, using unique encrypted identifiers. This allows scientists at ICES to obtain a more comprehensive view of specific health care issues than would otherwise be possible. Linked databases reflecting 12 million of 30 million Canadians allow researchers to follow patient populations through diagnosis and treatment, and to evaluate outcomes.

ICES collects five types of data: administrative, registry, survey, primary clinical, and chart abstraction. Administrative databases include hospital discharge abstracts, physician claims, and drug benefit program claims, among others. Administrative data is collected from the Ministry of Health and Long-Term Care. Registry databases include cardiovascular, stroke and cancer data. Registry data is collected from organizations such as the Cardiac Care Network, the Canadian Stroke Network and Cancer Care Ontario. Survey data include national health surveys, such as those undertaken by Statistics Canada. Clinical data are collected by ICES researchers with consent in primary clinical studies. Chart abstraction data is collected directly from the records of health service providers by ICES researchers to assess the quality and processes of health care. All uses of the data are vetted by a Research Ethics Board (REB), either through expedited review or full review by the board (i.e., clinical studies with consent).

Review of the Prescribed Entity

Documents Reviewed

ICES provided the IPC with a binder of documents on October 30, 2004, 2005, including:

Organizational Materials

- ICES Privacy and Data Security Handbook for Faculty, Staff and Students
- ICES Privacy and Data Security Handbook for Contract Workers/Abstractors
- ICES Confidentiality Agreement
- ICES Confidentiality Agreement for Designated Individuals (who have access to identifiable data)
- ICES Project-Specific Privacy Impact Assessment Form

- Current Organizational Chart
- ICES Board of Directors
- Job Description: Privacy Officer

Data Security Architecture and Related Documents

- ICES/MOHLTC Data Use Agreement Overview Diagram
- Use of Administrative Data at ICES: General Description
- Physical, Perimeter/Corridor and Electronic Security: Description
- ICES Moated Classified UNIX System Diagram
- ICES Local Area Network (LAN): Diagram
- Data Flow Diagrams for Projects (6 combinations)
- Types of Research Projects at ICES
- Procedure for Receiving External Data to be used at ICES (June 2004)
- Proposal for Data Destruction Mechanism
- De-identification of personal health information and data linkage processes: Description
- ICES Security Audit - Information Technology Infrastructure (Penetration Testing by External Experts)

Administrative, Clinical and Other Datasets Held at ICES

- Health care administrative datasets held at ICES
- Description of health care data available at ICES

Website Pages

- ICES Privacy Code: Protecting Personal Health Information at ICES
- Questions & Answers About Information Privacy Protection At ICES
- ICES Public Information Brochure ("Our Business Is Research, Our Priority….Privacy")
- Who we are
- Education and Events
- Privacy Commitment Statement ("Our business is research, our priority….Privacy")
- Named Privacy Officer/contact information (Commitment Statement page)
- ICES Research Publications (with examples)
- ICES Research in Progress (with examples)

Staff Education

- PHIPA Education for faculty and staff: Calendar of presentations, attendance lists
- Handouts for *PHIPA* orientation
- Web-based orientation: includes "Adding new users to the orientation"; "ICES web-based privacy orientation manuscript"; Staff Privacy Orientation logs by calendar year (2001-2005)

Internal and External Audits

- Privacy Impact Assessment of the Proposed Transfer of Selected Data from the Ontario Cancer Registry of Cancer Care Ontario to ICES October 2003: David Flaherty
- ICES Internal Privacy Audit Report (LAN audit, March 2004)

- DRAFT Work plan for audit: "Indications for Conducting a Review of Privacy, Confidentiality and Data Security Policies / Practices at ICES" Oct. 2001
- Internal privacy audit by role group managers/directors
- PC Audit procedure (LAN)
- Audit plan; Audit bookings; Audit of personal computers
- Privacy Audit points
- Access and Confidentiality Review: ICES Feb. 1999, Charles Burchill
- Manitoba Centre for Health Policy 2001 November Review Plan

BestCrypt™ Laptop Encryption Software Information
- Descriptions: Jetico™ about software, AES (about encryption standard/algorithm)

Risk Assessment/Disaster Recovery Plan Draft
- Risk Assessment DRAFT November 2004
- ICES Risk Assessment/Disaster Recovery Work plan

Confidentiality Committee
- Confidentiality Committee membership
- Terms of Reference
- Work plans (2001/02, 2003, 2004, 2005)

Privacy Impact Assessment Logs
- Research Ethics Board-approved administrative data use projects for 4 years (long form logs and short form logs)
- Current Research Ethics Board-cycle Privacy Impact Assessment log

List of Practices and Policies
- Privacy Breach Policy
- Challenging Compliance Policy
- Data access Policy
- Data destruction Policy
- De-identification and Linkage Process Practice
- Programming and Biostatistics Standards Practice Guide
- Passwords Policy
- Public access to Records Policy
- Public inquiry data management + Challenging Compliance Policies
- Receiving Data Practice

MOHLTC-allowed Publications with Small Cell-Size Exclusions

Site Visit

IPC representatives conducted a site visit at ICES on March 14, 2005.

IPC representatives toured ICES with the Privacy Officer, the Manager of IT/Security and the Senior Communications Officer for ICES. Focused meetings took place with ICES representatives as follows:

Administrative Safeguards	VP, Corporate Services
Access to Data	Director, Programming &Biostatistics
Physical Technical Safeguards	Manager, IT/Security
Organization of Research Projects	Director, Research Projects
Accountability, Transparency to the Public	Senior Communications Officer
Administrative: Policies & Procedures	Manager, Administration
Ethics: clinical	Hospital Liaison Coordinator (REBs)
Clinical Face of Research	Project Manager, RCSN
Research using Administrative Databases	Senior Scientist
Managing Privacy at ICES	Privacy Officer

Findings of the Review

Human resources

ICES staff (including board members, scientists, adjunct scientists, fellows, students and administrative staff) are required to sign Confidentiality Agreements upon hiring, and thereafter, on an annual basis. In addition, every person affiliated with ICES for business purposes (consultants, visiting scientists and research collaborators) is required to sign a Confidentiality Agreement.

Although the documentation states that by signing a Confidentiality Agreement each person acknowledges the consequences resulting from a breach of confidentiality, there is no clause in the Confidentiality Agreement advising a person of the consequences of a breach, namely, that a breach of confidentiality may result in discipline for staff up to and including dismissal and, in the case of third party service providers/vendors/contractors, may result in termination of their service agreement.

Further, although the documentation states that by signing the Confidentiality Agreement, each person agrees to familiarize him or herself with and agrees to comply with ICES's privacy policies, procedures and practices, there is no clause containing such a requirement in the Confidentiality Agreement.

In addition, the Confidentiality Agreement does not reference *PHIPA* nor does it reference and define personal health information, which is extremely important given the status of ICES as a prescribed entity pursuant to *PHIPA*.

As a result, it is recommended that the Confidentiality Agreement be amended to include a provision advising of the consequences of breach of the Confidentiality Agreement; a provision requiring each person signing the Confidentiality Agreement to comply with ICES's privacy policies, procedures and practices; a reference to the status of ICES as a prescribed entity under

PHIPA; and a definition of and reference to personal health information. It is our understanding that ICES is currently in the process of making these changes to the Confidentiality Agreement.

At ICES there are clearly defined roles with respect to privacy and confidentiality. A Privacy Officer has been appointed and a Confidentiality Committee established. The mandate of the Confidentiality Committee is to create a "privacy presence," to help sensitize staff to privacy and security issues and to facilitate the implementation of best privacy practices throughout ICES. Through the Privacy Officer, the Confidentiality Committee is accountable to the Vice President, Corporate and the President/CEO of ICES. Contact information for the Privacy Officer is available to the public on ICES's website. A security specialist for information technology has also been appointed and serves as a member of the Confidentiality Committee.

ICES has a robust on-going privacy and security training program. All new staff (including scientists, adjunct scientists, fellows, students and administrative staff) are required to receive privacy orientation prior to commencement of employment and prior to being given access to personal health information. The IPC was advised that in practice all new staff, after signing the Confidentiality Agreement, meet with the Privacy Officer for a privacy orientation before they receive a key and a room to work in.

Almost all of the staff at ICES have completed training on *PHIPA*. In addition, privacy presentations are scheduled regularly throughout the year. Training materials, such as privacy handbooks, have been developed and a web-based privacy orientation module is being developed. In the ICES web-based privacy orientation, ICES's role as a prescribed entity under *PHIPA* is absent. The web-based privacy orientation module should be amended to ensure that staff is advised of ICES's role as a prescribed entity under *PHIPA* and the significance and consequences of this designation. It is our understanding that ICES is in the process of making these changes.

Privacy

ICES has a comprehensive *Privacy Code* which is readily available to the public on ICES's website. Also published on the website are *Questions and Answers about Information Privacy Protection at ICES* and a Privacy Brochure. Two internal ICES documents explain how the *Privacy Code* is implemented at ICES: the *Privacy and Data Security Handbook for Faculty, Staff and Students* and the *Privacy and Data Security Handbook for Contract Workers/ Abstractors*.

In its *Privacy Code*, ICES defines itself as a "health information custodian." Since ICES is not a health information custodian, as defined under *PHIPA*, the characterization of ICES as such should be deleted given the potential for confusion on the part of the public and given that the obligations imposed on health information custodians with respect to collection, use, and disclosure of personal health information, and responding to requests for access and correction of personal information would not be applicable to ICES as a prescribed entity. Also, the *Privacy Code* should not place the onus for obtaining consent for disclosures of personal health

information to ICES on health information custodians, since health information custodians are permitted to disclose personal health information to ICES without consent under *PHIPA.*

In addition, it would be helpful to members of the public if in the *Questions and Answers about Information Privacy Protection at ICES* a reference was made to ICES's designation as a prescribed entity under section 45 of *PHIPA*, as this provides the authority for health information custodians to disclose personal health information to ICES. ICES's website would also be more user-friendly if a link to "Privacy and Confidentiality" was added to the homepage.

Various documents including the *Privacy and Data Security Handbook for Faculty, Staff and Students* (page 4), the *Privacy and Data Security Handbook for Contract Workers/Abstractors* (page 6) and the *Privacy Code* (page 1) stipulate the uses of personal health information by ICES. To enhance transparency, one of these purposes should mirror the purposes in section 45(1) of *PHIPA*.

ICES has implemented a policy for managing privacy breaches and handling complaints from the public. The privacy breach protocol emphasizes containment of the breach and notification of appropriate persons. However, this policy should be updated to include a reference to *PHIPA* rather than Bill 31. ICES also has processes in place for de-identifying personal health information and for linking databases of personal health information. A very limited number (4) of specified individuals at ICES have access to personal health information. These individuals sign special confidentiality agreements and are charged with receiving all data. All identifiable data is stripped of personal identifiers, with the exception of health card number, which is encrypted to become what is known as an ICES key number (IKN) before being used for research purposes at ICES. All data linkages are carried out using this unique identifier (IKN). Once the linkages are completed, the IKNs are also stripped from the dataset, which is then ready for its research purpose. In terms of retention and destruction of data, retention schedules are set out on a project-by-project basis. A destruction policy ensures that copies of all datasets are destroyed by researchers once they are no longer needed.

In recent years, ICES has been involved in a number of initiatives to assess the impact of its activities on privacy. For example, a comprehensive Privacy Impact Assessment was carried out when Cancer Care Ontario was considering transferring certain data from the Ontario Cancer Registry to ICES. In addition, in 1999, ICES underwent an external review of its information practices. An internal audit of its policies and procedures was initiated in 2003. Follow-up on the recommendations coming out of these privacy assessments is not well documented. Follow-ups on future activities of this nature should be clearly documented.

For each research project undertaken at ICES a Privacy Impact Assessment is carried out. This is desirable from a privacy perspective. In addition, each research project must be accompanied by a research plan that fulfills the requirements of section 44 of *PHIPA* and Regulation 329/04.

The *Privacy and Data Security Handbook For Faculty, Staff and Students* (page 19) provides that a research agreement must be in place between ICES and providers and researchers not formally affiliated with ICES for use of secondary data. The content of the research agreements does not appear to be consistent with subsection 44(5) of *PHIPA*. In the event that this

"secondary data" contains personal health information, the research agreements should be consistent with subsection 44(5) of *PHIPA*.

ICES obtains Research Ethics Board (REB) approval prior to using personal health information other than the encrypted administrative data (e.g., when they undertake medical chart abstractions). REB approval is also sought for any clinical studies contemplated. When only encrypted administrative data are used, a global REB approval process is used, whereby the ICES CEO and the Privacy Officer submit semi-annual reports on the use of administrative data to the REB to ensure the REB is aware of the work that has been done. The REB then randomly selects some of these projects for review; however, all these projects will be considered to have REB approval. Since it is not reasonably foreseeable in the circumstances that researchers at ICES could identify individuals from the encrypted administrative data, this practice is acceptable to the IPC.

To ensure the privacy of all data subjects, the results of all research projects are reported using aggregated data. Only data with a cell size greater than five are reported to the public.

With respect to third party agreements, ICES has an agreement with the Ministry of Health and Long-Term Care. This agreement sets out the conditions under which the Ministry of Health and Long Term Care will provide to ICES a copy of the Ontario Health Insurance Plan database, among others. The IPC was informed that this agreement is currently under negotiation and a copy of the agreement will be provided to the IPC when it has been finalized.

Security

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

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

been implemented. ICES has a protocol in place for the secure transfer of personal health information to ICES.

Since the site visit, ICES has reported to the IPC the results of a vulnerability/penetration assessment undertaken by an independent third party. The results of the assessment indicated that the measures that had been put in place were successful in protecting ICES from internal and external malicious threats. Based on the results of the assessment, ICES is currently in the process of or has implemented a number of recommended security enhancements (e.g., strengthening the password policy).

Although the security measures that have been implemented by ICES appear to be quite extensive, one concern that was raised by the IPC is that the measures that have been put in place are not based upon a comprehensive threat and risk assessment (TRA). Although the recent "ethical hack" revealed no evidence of any major security risks, threats or breaches at ICES, the IPC recognizes that information security requires ongoing vigilance and a commitment to continuous improvement. Given the volume and sensitivity of the personal health information in the custody or control of ICES, it would be desirable for ICES to adopt a more comprehensive and systemic information security management program. In this light, we encourage ICES to carry out a comprehensive, organization-wide threat and risk assessment. Such a threat and risk assessment would help identify all risks, both external and internal, and provide a strong basis for prioritizing those risks and developing an action plan to mitigate them. Recurring threat and risk assessments are also valuable for measuring progress and ensuring continued improvement.

Summary of Recommendations

Major Recommendations

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

Other Recommendations

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

1. Amend the Confidentiality Agreement to include references to PHIPA, 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 *PHIPA* privacy training and that the web-based privacy orientation module is amended to ensure that staff is advised of ICES's 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 *PHIPA*.

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

5. When completed, provide to the IPC a copy of the agreement between ICES and 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.

Statement of IPC Approval of Practices and Procedures

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