Information
and Privacy
Commissioner/
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the Canadian Institute for Health Information:

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

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Review of the Canadian Institute for Health Information:
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 prac-

tices and procedures described above to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information.

In addition, section 18(7) of Regulation 329/04 to *PHIPA*, permits the Canadian Institute for Health Information to disclose personal health information to a person outside Ontario where the disclosure is for the purpose of health planning or health administration; the information relates to health care provided in Ontario to a person who is a resident of another province or territory of Canada; and the disclosure is made to the government of that province or territory.

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:

<u>Human Resources</u>

- 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 Canadian Institute for Health Information (CIHI) is a prescribed entity under section 45 of *PHIPA*. CIHI is an independent, not-for-profit organization that analyzes and provides statistical information related to the performance of the Canadian health system, the delivery of health care and the status of the health of Canadians. Specifically, CIHI:

- Identifies and promotes national health indicators;
- Coordinates and promotes the development and maintenance of national health information standards;
- Develops and manages databases and registries related to health care services, health human resources and health spending;
- Examines what factors determine good health (Canadian Population Health Initiative);
- Conducts analysis and special studies;
- Participates in research;
- Publishes reports and disseminates health information; and
- Coordinates and conducts education sessions and conferences.

CIHI collects three broad categories of health information: health services information; information about health care professionals and information about health care spending. Information is collected from a variety of sources throughout Canada including various government ministries and departments of health, hospitals, prescribed entities, continuing care access centres, health professional associations, colleges and other educational institutions and other health care organizations.

As a national organization, CIHI has offices in Ottawa, Toronto, Victoria, Edmonton and Montreal.

Review of the Prescribed Entity

Documents Reviewed

CIHI provided the IPC with a binder of documents on March 7, 2005, including:

Organizational Materials

- Privacy and Confidentiality of Health Information at CIHI; Principles and Policies for the Protection of Personal Health Information and Policies for Institution-Identifiable Information, third edition, 2002.
- Privacy Toolkit

Human Resources

- Sample Confidentiality Agreement
- Information from CIHI Website on External Training Courses

Third Party Agreements

- Confidentiality and Non-Disclosure Agreement for Service Providers
- Confidentiality Agreement for Researchers Working On Site
- Service Agreement for Web-Based Reporting Tools

Privacy

- "Privacy and Confidentiality" Brochure
- Frequently-Asked Questions about Privacy and Data Protection (web page)
- List of Privacy Impact Assessments (completed or underway)
- Privacy Impact Assessment of Clinical Administrative Databases (April 2005)

- Terms of Reference – Privacy Audit Program
- List of the Health Services Databases
- *Client Information Request Form* for Record-Level Data
- Non Disclosure and Confidentiality Agreement for Record-Level Data

Security

- Security Policy
- Information Technology and Information Security (IT-IS) Procedures Manual
- Data Access Authorization

Site Visit

IPC representatives conducted a site visit at CIHI's Toronto office on April 8, 2005.

Following a welcome and introductions, IPC representatives were briefed on CIHI activities involving personal health information, and then toured the facility. Focused meetings took place with CIHI representatives as follows:

Incoming Data Demonstration	Chief Technical Officer
IT-IS Server Room	Manager, Architecture and Standards and Co-ordinator, Network Services
Physical Security	Consultant, Privacy Secretariat
Clinical Administrative Databases	Director, Health Services Information
Canadian Organ Replacement Registry	Director, Health Services Information
Distribution Room	Director, Health Services Information

In addition, presentations were made on the following topics:

- Privacy at CIHI: Administrative Protections
    - Authority, transparency
    - Disclosures and disclosure avoidance
- IT Security at CIHI: Technical Protections
    - General system architecture

- Access protections, authorization and review
- Penetration testing

Findings of the Review

Human resources

CIHI has clearly defined roles with respect to privacy and security. A Privacy Secretariat has been established to foster a culture of privacy. The Privacy, Confidentiality and Security Team includes representation from across the organization including the Vice President of Operations and directors and managers from various departments including information systems, standards, research and analysis, client relations, databases, registries, and human resources. This team works to enhance the culture of privacy throughout the organization and provides advice on operational issues as they relate to privacy. The Chief Privacy Officer is a member of the senior management team, reports directly to the Chief Executive Officer and manages the Privacy Secretariat. Contact information for the Chief Privacy Officer is available on CIHI's website.

A Privacy and Data Protection Committee, a subcommittee of the CIHI Board of Directors, has been established to provide oversight for the privacy program and report annually on the program to the Board of Directors as well as provide advice on significant developments in privacy legislation. The Chief Technology Officer is responsible for electronic security and the Manager of Corporate Administration is responsible for physical security of the facility.

In addition, CIHI has had a Chief Privacy Advisor for five years. The role of this external advisor is built into the CIHI privacy compliance program. The Chief Privacy Advisor's role is to provide advice to the Chief Privacy Officer and to serve as a resource for the Chief Executive Officer and Board of Directors on privacy complaints.

A mandatory component of the CIHI staff orientation program is a presentation, *Introduction to Privacy and Confidentiality at CIHI*, by the Chief Privacy Officer. Workshops on the application of CIHI privacy policies and procedures and Privacy Impact Assessment training are also offered. In addition, all staff have been provided with a Privacy Toolkit. CIHI advised the IPC that specialized training on the application of *PHIPA* is currently being provided and that specialized information technology security training is currently being development. All staff of CIHI must sign a Confidentiality Agreement upon employment.

Based on a review of the Confidentiality Agreement template, it is recommended that the Confidentiality Agreement be amended to reference *PHIPA*, to reference and define personal health information and to reflect CIHI's obligations as a prescribed entity under *PHIPA*. Also, the Confidentiality Agreement only regulates the disclosure of personal health information, not its use. It is important that persons signing the Confidentiality Agreement agree not to use personal health information for any purpose other than those purposes for which access was provided by CIHI, unless required by law. The Confidentiality Agreement should therefore be

amended accordingly. Finally, the Confidentiality Agreement should require persons signing the Confidentiality Agreement to notify CIHI immediately upon becoming aware of any breach of the Confidentiality Agreement.

In order to protect the privacy of individuals with respect to their personal health information and to maintain the confidentiality of this information, third parties that may have access to personal health information in the custody or control of CIHI, including third parties accessing web-based reporting tools, are subject to terms and conditions related to confidentiality and privacy contained in third party agreements. Based on a review of these third party agreements, it is recommended that these agreements be amended to require third parties to notify CIHI immediately upon becoming aware of any breach of the confidentiality and privacy protection provisions of the agreement.

In addition, data sharing agreements are in place or under negotiation with other prescribed entities and the Ontario Ministry of Health and Long Term Care. Copies of all data sharing agreements that are currently under negotiation with other prescribed entities and the Ontario Ministry of Health and Long Term Care should be forwarded to the IPC when completed.

Privacy

CIHI has a comprehensive privacy code, *Privacy and Confidentiality of Health Information at CIHI*, which is available to the public on the CIHI website. Also available on the website are *Frequently Asked Questions about Privacy and Data Protection*, a brochure on Privacy and Confidentiality and privacy impact assessments for CIHI data holdings and projects. Privacy impact assessments have been completed or are underway for most of CIHI's data holdings and projects.

Although the IPC recognizes that CIHI is a national organization, subject to the array of laws and regulations that apply to personal health information throughout Canada, it is our view that Ontarians should be aware of its special legal status as a prescribed entity under *PHIPA*. Accordingly, we recommend that all internal and external documentation should be amended to reflect CIHI's status as a prescribed entity pursuant to section 45 of *PHIPA* and to emphasize the significance and consequences of this designation.

With respect to internal and external privacy audits, CIHI has implemented an internal privacy review program that includes oversight by the Privacy and Data Protection Subcommittee of its Board of Directors. Full implementation of this privacy audit program has been delayed due to a lack of human resources and changes to the Board of Directors. The IPC recommends that the privacy audit program should be fully implemented as soon as possible in order to protect the privacy of individuals whose personal health information is in the custody or control of CIHI and to maintain the confidentiality of that information.

CIHI currently does not have a formal policy or procedure for dealing with situations in which personal health information is lost, stolen or subject to unauthorized use, disclosure, copying, modification or disposal. The documentation provided states that in the event of a privacy

breach, the staff is trained to contact the Chief Privacy Officer who would respond in a fashion tailored to the complexity and severity of the issue at hand. The IPC recommends that a formal policy and procedure be developed to outline procedures for detecting, investigating, containing and notifying relevant persons when personal health information is lost, stolen or subject to unauthorized use, disclosure, copying, modification or disposal.

With respect to linkages of personal health information with other information, these are only undertaken with the consent of individuals or in accordance with the following criteria:

- The linkage is consistent with CIHI's mandate;
- The public benefits significantly offset the public interest in protecting privacy;
- The results will not be used for any purpose that would be detrimental to individuals;
- The linkage is for a time-limited specific purpose; and
- The linkage has demonstrable savings over alternative procedures or is the only practical alternative.

Moreover, external researchers that have access to personal health information in the custody or control of CIHI must agree not to link the personal health information with other information except as approved by CIHI. In addition to these safeguards related to "data linkage," CIHI should establish a formal policy for physically linking records. For example, a minimum number of individuals should have access to identifiable personal health information for this purpose and identifiers should be stripped or encrypted in the linked dataset, immediately following the data linkage.

Staff at CIHI is provided access to data holdings on a need-to-know basis. Only those with a need for access to identifiable information have access to personal health information. Reports and published materials contain aggregate data only to minimize the risk of residual disclosure.

CIHI does not appear to have a formal policy requiring routine encryption of the health card number prior to the use of personal health information within CIHI. Although staff at CIHI do not have access to information that would allow the identification of an individual from the health card number, it is the IPC's view that the use of the health card number in an unencrypted format in the day-to-day work of CIHI poses an unnecessary risk to privacy. The implementation of a formal policy to encrypt the health card number would help to ensure that individuals cannot be identified from the health information used at CIHI.

Pursuant to the *Privacy and Confidentiality of Personal Health Information at CIHI*, in most cases, CIHI only discloses aggregated or de-identified health information to third persons who request disclosure of health information in the custody or control of CIHI. Identifiable personal health information is only disclosed to a third party who provided the personal health information, with the consent of the individual to whom the personal health information relates, if the disclosure is required by legislation or an agreement authorized by legislation, or for research

purposes provided the researcher submits a research plan and has received research ethics board approval.

Researchers and other third parties are required to complete the *Client Information Request Form* and to execute a Non-Disclosure and Confidentiality Agreement in order to obtain access to record-level data. Based on a review of the *Client Information Request Form*, this form should be amended to reflect the requirements relating to the disclosure of personal health information set out in *PHIPA*. For example, where personal health information is disclosed for research purposes without the consent of the individual to whom the personal health information relates, the *Client Information Request Form* should be amended to conform to the requirements set out in section 44 of *PHIPA* and section 16 of Regulation 329/04 to *PHIPA*. In addition, the Non-Disclosure and Confidentiality Agreement should be amended to require researchers and third parties to notify CIHI immediately in writing if there is any breach of the agreement.

Security

CIHI has implemented an array of physical, technical and administrative security measures to protect personal health information in its custody and control. Staff of CIHI are issued and must wear photo identification cards at all times. Access to CIHI facilities is controlled through a card access system and personal identification number. Visitors must register and sign in at reception and are issued and must wear visitor identification cards at all times. CIHI office doors are always locked and are alarmed and monitored outside of office hours.

Internal access to CIHI databases is restricted to staff with a need-to-know. Electronic access is controlled with user identification and password protection. CIHI uses secure firewalls, a virtual private network and other means to secure its network. CIHI has recently introduced and is enforcing a formalized patch management policy and associated procedures for all information technology based systems.

In terms of the transfer of personal health information, a number of procedures are in place to ensure security depending on the media. When CIHI receives or sends personal health information electronically, a secure system is used and data are encrypted. Where personal health information is transferred to CIHI on disk, a courier is used and the personal health information is USB key encrypted, whenever possible. CIHI generally does not send or receive personal health information by facsimile. However, where facsimile transmission is necessary, it is done as securely as possible. Where CIHI transfers health information to other organizations, in most cases, it is aggregated. However, where personal health information is required, access authorizations, user identifications and passwords are required. In those cases where paper reports are requested, they are sent by courier. Personal health information may also be sent by magnetic tape or compact disk using secure physical transportation. Data sharing agreements or arrangements with other prescribed entities and the Ontario Ministry of Health and Long Term Care set out procedures for the secure transmission of personal health information.

CIHI currently is auditing internal access to its data holdings and network access audit trails are used when necessary. It is our understanding that a more comprehensive procedure for storing, consolidating and analyzing a range of audit trails is currently under development.

New servers at CIHI go through an audit checklist and an automated security audit before being brought "on-line." In addition, an "ethical hack" is conducted on an annual basis by an independent third party to ascertain any internal, external or web vulnerabilities. Although the recent "ethical hack" revealed no evidence of any major security risks, threats or breaches at CIHI, 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 CIHI, it would be desirable for CIHI to adopt a more comprehensive and systemic information security management program. In this light, we encourage CIHI to carry out (preferably by an independent party) 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 the documentation and the site visit, there are no major recommendations that require rectification or resolution by CIHI prior to November 1, 2005.

Other Recommendations

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

1. Provide staff with specialized training on information technology security.

2. Amend the Confidentiality Agreement to include references to *PHIPA*, to reference and define personal health information, to reflect CIHI's obligations as a prescribed entity under *PHIPA*, to include provisions governing the use of personal health information and to include provisions requiring persons signing the Confidentiality Agreement to notify CIHI immediately upon becoming aware of any breach of the Confidentiality Agreement.

3. Amend third party agreements to require third parties to notify CIHI immediately upon becoming aware of any breach of the confidentiality and privacy protection provisions of the third party agreement.

4. When completed, provide to the IPC copies of all data sharing agreements that are currently under negotiation with other prescribed entities and the Ontario Ministry of Health and Long Term Care.

5. Where appropriate, amend all internal and external documentation to reflect CIHI's status as a prescribed entity under section 45 of *PHIPA*.

6. Complete the implementation of the privacy audit program.

7. Develop and implement a formal policy for dealing with the loss, theft or unauthorized use, disclosure, copying, modification or disposal of personal health information.

8. Develop and implement a formal policy for minimizing access to identifiable personal health information during the linkage of personal health information with other information.

9. Develop and implement a formal policy for de-identifying information through the encryption of health card numbers before they are used by CIHI.

10. Amend all documentation relating to the disclosure of personal health information from CIHI (e.g., for research purposes) to conform to the requirements of *PHIPA* and Regulation 329/04 to *PHIPA*.

11. Complete the development and implementation of a comprehensive procedure for storing, consolidating and analyzing a range of audit trails.

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

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that CIHI 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 CIHI have been approved by the IPC.