Information
and Privacy
Commissioner of
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 2008

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Three-Year Review of the Canadian Institute for Health Information:

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 Canadian Institute for Health Information, which were the subject of an earlier report of the IPC and which are set out in Appendix "A" to this report, have all since been addressed by the Canadian Institute for Health Information.

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 Canadian Institute for Health Information submitted the requested documentation on April 30, 2008, and submitted additional documentation on June 5, 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 Canadian Institute for Health Information was held on June 19, 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 Canadian Institute for Health Information

The Canadian Institute for Health Information ("CIHI") is an independent, not-for-profit, pan-Canadian organization whose mandate, as agreed to by the Federal, Provincial and Territorial Ministers of Health, is to analyze and provide accurate and timely information to establish sound health policy, to effectively manage the health system and to generate public awareness about factors affecting good health. Further to this mandate, CIHI collects and analyzes personal health information and reports on health system performance, health spending, health human resources and population health in order to improve health system performance and to improve the health of Canadians. In order to support its national mandate, while the main offices of CIHI are located in Ottawa and Toronto, it also has regional offices in Victoria, Edmonton, Montreal and St. John's.

Three-Year Review of the Canadian Institute for Health Information

1. Privacy and Security Governance and Accountability Framework

The President and Chief Executive Officer of CIHI is ultimately accountable for ensuring that CIHI complies with the *Act* and with the privacy and security policies, procedures and practices implemented by CIHI. However, other individuals within CIHI have been delegated the authority to act on behalf of the President and Chief Executive Officer.

The Chief Privacy Officer and General Counsel, who reports to the Vice President of Corporate Services, has been delegated the day-to-day authority to manage the privacy program. The Chief Privacy Officer and General Counsel heads the Privacy and Legal Services Secretariat which is responsible for providing privacy advice and support to program areas; for ensuring that the privacy policies, procedures and practices implemented are up to date; for developing *Data Sharing Agreements*; for providing privacy training; for conducting privacy impact assessments; and for conducting privacy audits. The Chief Privacy Officer and General Counsel is also responsible for monitoring developments in privacy legislation across Canada and for managing the Legal Services Unit, which also provides privacy and legal advice to the program areas at CIHI.

The Chief Privacy Officer and General Counsel is supported by a Privacy, Confidentiality and Security Team with representation from senior executives and from directors and managers of all program areas. The mandate of the Privacy, Confidentiality and Security Team includes providing input into the development of privacy policies, procedures and practices and providing input into amendments to existing privacy policies, procedures and practices.

The privacy program is overseen by the Privacy and Data Protection Committee of the Board of Directors. This committee is responsible for receiving reports relating to privacy breaches; for reviewing and making recommendations on the privacy audit program; for reviewing the findings of privacy audits; and for formulating recommendations on privacy policies, procedures and practices.

In addition, since 2005, an Annual Privacy Report is prepared by the Chief Privacy Officer and General Counsel and is presented to the entire Board of Directors. The Annual Privacy Report addresses any changes to the privacy program in the previous fiscal year, the initiatives undertaken by the privacy program during the previous fiscal year, the results of privacy audits undertaken during the previous fiscal year and initiatives that will be undertaken by the privacy program in the upcoming fiscal year.

The Chief Technology Officer, who reports to the President and Chief Executive Officer of CIHI, has been delegated the day-to-day authority to manage the security of personal health information at CIHI. The Chief Technology Officer is also supported by a number of committees including the Information Leadership Team, the Information Management Advisory Board, the Information Technology Operational Committee, the Patch Surveillance Committee and the Security Management Group.

2. Overview of Privacy and Security Policies, Procedures and Protocols

CIHI has developed a privacy policy, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information.* This privacy policy describes its status as a prescribed entity under the *Act* and the obligations that arise because of 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 protocols implemented by CIHI and sets out the safeguards employed by CIHI to protect personal health information.

CIHI has also implemented numerous privacy and security policies, procedures and protocols that support the *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, which will be discussed throughout this report.

Privacy Policy

CIHI developed a privacy policy, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, which describes the practices and procedures implemented by CIHI to protect the privacy of individuals whose personal

health information it receives and to protect the confidentiality of that information. CIHI has advised that it plans to undertake a comprehensive review of this privacy policy in the next fiscal year. It is recommended that in undertaking this review, that CIHI have regard to the comments below.

The practices and procedures outlined in *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, do not clearly distinguish between the collection, use and disclosure of identifiable personal health information and the collection, use and disclosure of de-identified information. This results in a lack of clarity as to the circumstances in which identifiable personal health information is collected, used and disclosed and the circumstances in which de-identified information is collected, used and disclosed.

It is recommended that the privacy policy, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, be amended to clearly distinguish between the circumstances when identifiable personal health information is collected, used and disclosed and the circumstances when de-identified information is collected, used and disclosed and to clarify the policies, procedures and practices and the statutory conditions that apply in each circumstance.

It is also recommended that the practices and procedures for the disclosure of personal health information set out in the privacy policy, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, ensure consistency with section 18 of Regulation 329/04 to the *Act*, which only permits prescribed entities to disclose personal health information in the circumstances set out in that section.

For example, Policy 5.12 and its related procedures permit CIHI to disclose personal health information to the data provider, including the health information custodian, who originally provided the personal health information to CIHI. However, section 18 of Regulation 329/04 to the *Act* only permits a prescribed entity to disclose personal health information to a health information custodian in these circumstances if the personal health information does not contain any additional identifying information. The requirement to ensure that the personal health information does not contain additional identifying information should be addressed in Policy 5.12 and its procedures.

The privacy policy, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, should also be amended to ensure that the policies and procedures enumerated therein are consistent with the actual practices of CIHI and are consistent with other policies, procedures and practices implemented by CIHI. For example, none of the policies and procedures in "Principle 5: Limiting Use, Disclosure and Retention of Personal Health Information," appear to address the disclosure of personal health information to other prescribed entities under section 45 of the *Act*, despite the fact that CIHI discloses personal health information to such entities.

It is also recommended that *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information* be amended pursuant to the comments set out

in Appendix "C." These comments include emphasizing that personal health information is only used and disclosed in compliance with applicable laws and to clearly articulate the circumstances in which identifying personal health information is disclosed for research and analysis and the circumstances in which de-identified information is disclosed for these purposes.

Privacy Breach Management Protocol

Further to the recommendation made by the IPC during the initial review of its practices and procedures in 2005, CIHI has developed and implemented a *Privacy Breach Management Protocol* that addresses the discovery, reporting, containment, notification, investigation and remediation of privacy breaches. A privacy breach is defined as the collection, access, use, disclosure or disposal of personal health information in an unauthorized manner.

The *Privacy Breach Management Protocol* requires a person that discovers a privacy breach to immediately report the privacy breach or suspected privacy breach to their supervisor and to the Chief Privacy Officer and General Counsel verbally and subsequently in writing. The report must include a description of the compromised personal health information, when the breach or suspected breach was discovered, how it was discovered, the cause of the breach or suspected breach (if known) and any steps taken to contain the breach or suspected breach. The person that discovered the privacy breach is also required to initiate the process of containment in order to prevent further theft, loss or unauthorized access, use, disclosure, copying, modification or disposal of the information.

The Chief Privacy Officer and General Counsel is then responsible for assembling other members of the Breach Response Team, including the Chief Technology Officer and the designated Vice-President(s). The Breach Response Team will then review the containment measures to ensure that they are effective, determine whether further containment measures are required and notify the President and Chief Executive Officer of CIHI of the privacy breach or suspected privacy breach.

The President and Chief Executive Officer of CIHI, in consultation with the Breach Response Team, is then responsible for determining whether a privacy breach has occurred and for establishing a process for notification, including when to notify, how to notify, who should notify and what should be included in the notification. The *Privacy Breach Management Protocol* contains an explicit acknowledgement that as a secondary user of personal health information, notification will not be provided directly to the individual to whom the personal health information relates, but rather to the health information custodian who provided the personal health information.

The Breach Response Team will then investigate the privacy breach and issue recommendations for corrective measures to prevent a similar breach in future. The recommendations will be submitted to the Executive Committee of CIHI, which includes the President and Chief Executive Officer.

Security Policies, Procedures and Protocols

CIHI has developed and implemented security policies, procedures and practices to protect personal health information against theft, loss and unauthorized use, disclosure, copying, modification and disposal. These include policies and procedures related to the acceptable use of technology, passwords, patch management, back-up procedures, information security events and the destruction of records of personal health information in electronic format.

However, these security policies and procedures have not been integrated into a centralized security policy and procedure framework. CIHI is moving toward ISO 27001 registration and as part of this process is undergoing a gap analysis and is developing information security policies and procedures. It is recommended that, as part of ISO 27001 registration, CIHI implement a centralized, integrated and comprehensive framework of security policies and procedures.

Information Security Events Policy

CIHI has developed a policy and associated procedures for the discovery, reporting, investigation and remediation of information security events, that is, identified occurrences indicating a possible breach of information security policies and procedures; identified occurrences indicating a possible failure of safeguards; previously unknown situations that may be security relevant; and weaknesses that can be exploited to gain access or to make a system or process work in an unintended way.

The *Information Security Events Policy* requires that an information security event be reported within thirty minutes of discovery to security@cihi.ca. It is unclear, however, what information with respect to the information security event must be reported. Further, the *Information Security Events Policy* does not address containment of the information security event nor does it address notification of senior management, the health information custodians that provided the personal health information to CIHI and relevant information and privacy commissioners of the information security event. It is recommended that the *Information Security Events Policy* be amended to clarify the information that must be reported with respect to the information security event and to address containment and notification of the information security event.

Further, while the *Information Security Events Policy* requires the Security Management Group to convene within five days following the reporting of the information security event to assign an owner to the event and requires the Information Technology and Services Department to investigate the information security event, the procedure does not address the investigation process. It is recommended that the *Information Security Events Policy* be amended accordingly.

The *Information Security Events Policy*, however, does require that an investigation report be written within twenty business days following the reporting of the information security event. The investigation report must include recommendations for remediating the information security event and must be provided to the person who reported the information security event, the manager of the person who reported the information security event, the Security Management Group, the Information Technology Operational Committee and the Privacy and Legal Services

Secretariat. It further requires that the recommendations for remediating the information security event be implemented within ninety days of the release of the investigation report.

Finally, within twenty days following the release of the investigation report, the *Information Security Events Policy* requires a meeting to be convened to review the information security event and to prevent a similar information security event in future. Following this meeting, the Senior Program Consultant-Security must issue a further report to the Security Management Group, the Information Technology Operational Committee and the Privacy and Legal Services Secretariat.

Review of Privacy and Security Policies, Procedures and Protocols

The privacy policy implemented by CIHI, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, states that privacy policies, procedures and protocols implemented by CIHI are subject to "ongoing review." However, the frequency for this "ongoing review" is not defined. Further, while the *CIHI Security Audit Program Schedule* states that information security policies and procedures will be reviewed on an annual basis, no framework is provided for the review of these policies and procedures.

It is recommended that CIHI develop and implement a policy and associated procedures for the annual review of its privacy and security policies, procedures and protocols. This policy and its associated procedures should set out the person(s) responsible for undertaking the review; the procedure to be followed in undertaking the review; the procedure to be followed in amending the policies, procedures and protocols; and the time frame each year in which this review will be undertaken.

It is further recommended that any review of the privacy and security policies, procedures and protocols implemented by CIHI have regard to: technological advancements; any orders, guidelines and best practices issued by provincial or federal information and privacy commissioners; any industry security and privacy best practices; and new or amendments to existing legislation.

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

CIHI makes information about its privacy and security policies, procedures and practices readily available on its website, including its privacy policy entitled *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, a brochure entitled *Privacy and Confidentiality*, Frequently Asked Questions entitled *Frequently-Asked Questions About Privacy and Data Protection* 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. Privacy impact assessments and the statement of purposes for each data holding are also made publicly available on its website.

The privacy and security policies, procedures and protocols implemented by CIHI are also made readily available to staff on a centralized intranet resource.

4. Collection, Use and Disclosure of Personal Health Information

Collection

CIHI collects three broad categories of health information from health information custodians as well as other organizations and governments throughout Canada, such as Statistics Canada:

- Health services information - information about the services provided by health information custodians;
- Health care professional information - information about the activity patterns and trends of health care practitioners; and
- Health care spending - information about the amount of money being spent on various health services.

Personal health information is retained in a variety of data holdings including: the Discharge Abstract Database, the National Ambulatory Care Reporting System, the Canadian Joint Replacement Registry, the Canadian Organ Replacement Register, the Hospital Morbidity Database, the Ontario Trauma Registry and the Ontario Mental Health Reporting System.

Prior to the collection of personal health information, CIHI drafts a "Statement of Purposes" that identifies the purposes of each new data holding. In addition, for each new data holding containing personal health information, CIHI consults with stakeholders to define the personal health information necessary for the identified purposes and, following this consultation, prepares a document listing the personal health information that will be collected and documenting the need for the personal health information. This document is reviewed annually to ensure that the personal health information continues to be required for the identified purposes of the data holding.

The "Statement of Purposes" and the document setting out the personal health information that will be collected and the need for this personal health information is given to data providers, including health information custodians, prior to the collection of personal health information. The "Statement of Purposes" for each data holding is also made publicly available on its website.

Use

Personal health information is used for purposes of analysis and 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 pursuant to section 45 of the *Act*. Personal health information is not used by CIHI for research purposes pursuant to section 44 of the *Act*.

Staff is only permitted to access and use data holdings containing personal health information on a "need-to-know basis." All staff requiring access to a data holding must complete a *CIHI Internal Data Access Authorization/Removal Request Form* and must justify why access is required, whether this requirement is ongoing or short-term, the type of access required, whether the

personal health information in the data holding will be combined or linked with other information and whether alternatives exist to providing access. The data holding "owner" assigned to the data holding will then decide whether to grant or deny access.

All requests for access that will result in combining or linking personal health information in the data holding with another data holding must also be reviewed by the Privacy, Confidentiality and Security Team prior to granting access. Further, on an annual basis, reports are prepared for data holding "owners" and managers. The data holding "owners" and managers are then required to validate all staff access within three weeks of receipt of the report. In the event that a staff member is not validated by both the data holding "owner" and the manager within three weeks of the report, the staff member's access to the data holding will be suspended.

Further, in response to a recommendation made by the IPC during the initial review of its practices and procedures in 2005, CIHI has developed and is in the process of implementing a process for the de-identification of information through the encryption of health card numbers. A three-phase de-identification project was commenced by CIHI. Work on the de-identification project was initiated shortly after the report of the practices and procedures of CIHI was finalized in 2005, and the first phase was completed in April 2007 following a review of de-identification methodologies. The second phase, completed in October 2007, involved the de-identification of health card numbers in the Discharge Abstract Database, National Ambulatory Care Report System Database and Hospital Morbidity Database for the years between 2001 and 2007. The third phase, currently underway, entails applying the de-identification methodology to the years prior to 2001 in the above noted databases and applying the de-identification methodology to the remaining data holdings.

When completed, CIHI will only use de-identified information for purposes of analysis and compiling statistical information with respect to the health system pursuant to its function as a prescribed entity under section 45 of the *Act*, subject to limited exceptions.

Disclosure

CIHI discloses personal health information in a number of circumstances where the disclosure is permitted or required by law, including in the circumstances set out below.

Personal health information is disclosed to the data providers, including the health information custodians, who provided the personal health information to CIHI. As stated earlier in this report, it is recommended that CIHI implement procedures to ensure that personal health information is only disclosed to the health information custodian in these circumstances, where it does not contain any additional identifying information.

Personal health information is also disclosed to other prescribed entities pursuant to section 45 of the *Act* for the purpose of analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the health system.

In addition, personal health information is disclosed for research purposes. Prior to the disclosure of personal health information for research purposes, CIHI requires that a *Third-Party Record-Level Data Request Form* be completed that addresses all the requirements that must be satisfied prior to the disclosure of personal health information for research purposes under section 44 of the *Act* and its regulation. CIHI also requires a copy of the research plan and a copy of the decision of the research ethics board approving the research plan. Finally, prior to the disclosure of personal health information for research purposes, CIHI requires that all individuals who will have access to the personal health information sign a *Non-Disclosure/Confidentiality Agreement*.

The *Non-Disclosure/Confidentiality Agreement* requires individuals to agree to comply with the conditions and restrictions imposed by CIHI relating to the use, security, disclosure, return or disposal of the personal health information. For instance, by signing the *Non-Disclosure/Confidentiality Agreement*, individuals agree not to use the personal health information except for the purposes described in the *Third-Party Record-Level Data Request Form*, to adhere to the enumerated security safeguards imposed by CIHI, to not make contact with the individual to whom the personal health information relates and to immediately report any actual or potential breach of the *Non-Disclosure/Confidentiality Agreement*.

The *Non-Disclosure/Confidentiality Agreement* further requires these individuals to securely destroy the records of personal health information within one year of publication or within three years from receipt of the personal health information, whichever comes first, and to provide written confirmation setting out the date, time, location and method of secure destruction employed. The *Non-Disclosure/Confidentiality Agreement* also permits CIHI to audit compliance with the *Non-Disclosure/Confidentiality Agreement* upon reasonable notice.

5. Retention and Destruction of Personal Health Information

CIHI retains records of personal health information in electronic format permanently for long-term analysis and retains records of personal health information in paper format that have been placed into electronic format for as long as is required for the electronic records to be finalized.

The Chief Technology Officer is responsible for developing policies and procedures to support the secure destruction of records of personal health information in electronic format and the Director of Human Resources and Administration is responsible for developing policies and procedures to support the secure destruction of records of personal health information in paper format. CIHI has also retained a third-party service provider to store and manage semi-active and inactive records, including records of personal health information, and to destroy inactive records, including inactive records of personal health information.

Destruction of Records of Personal Health Information in Electronic Format

CIHI has developed and implemented a policy relating to the secure destruction of personal health information in electronic format, the *Storage and Destruction of CIHI Electronic Media Policy*.

While the *Storage and Destruction of CIHI Electronic Media Policy* requires all expired or non-usable electronic media to be destroyed on a quarterly basis, it does not set out the method of secure destruction to be employed. It is recommended that the *Storage and Destruction of CIHI Electronic Media Policy* be amended to require that all expired and non-usable electronic media be destroyed in a secure manner, to provide a definition of secure destruction that is consistent with subsection 1(5.1) of Regulation 329/04 to the *Act* and to set out the method of secure destruction that will be employed for each type of electronic media. It is further recommended that the method of secure destruction that will be employed be consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC.

In addition, while the *Storage and Destruction of CIHI Electronic Media Policy* requires the third-party service provider retained to destroy the electronic media to provide a certificate of destruction, it does not set out the required content of this certificate. It is recommended that the *Storage and Destruction of CIHI Electronic Media Policy* be amended to 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.

Destruction of Records of Personal Health Information in Paper Format

While CIHI has developed and implemented policies with respect to the secure destruction of records of personal health information in electronic format, it has not developed similar policies with respect to the secure destruction of records of personal health information in paper format. Instead, it has created an information document for staff entitled *Personal Health Information Recycle or Shred?* which requires that records of personal health information be shredded.

It is recommended that CIHI develop and implement policies and procedures with respect to the secure destruction of records of personal health information in paper format that are consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC and that are consistent with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to the *Act*, in order to ensure that these policies and procedures are enforceable.

Agreement with the Third-Party Service Provider

While the agreement between CIHI and the third-party service provider addresses the secure storage and management of records of personal health information, it does not address the secure destruction of records of personal health information. It is recommended that the agreement with 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 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 CIHI 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 CIHI.

6. Administrative Safeguards Implemented

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

Privacy and Security Training

All new employees of CIHI are required to attend privacy orientation. In December 2007, an online module entitled *Privacy and Legal Services New Employee Corporate Orientation* was introduced to provide this mandatory privacy orientation. The *Privacy and Legal Services New Employee Corporate Orientation* describes the status of CIHI under data protection legislation, including its status as a prescribed entity under the *Act*. It further provides an overview of the privacy policy implemented by CIHI, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*.

With respect to current employees, CIHI advised that the Chief Privacy Officer and General Counsel or her designate prepares and delivers training on the privacy policies, procedures and practices implemented by CIHI. From a review of the documentation submitted for purposes of this review, it appears that at least one privacy training session is provided to current employees each year.

It is unclear, however, from a review of the documentation, how CIHI keeps track of attendance at the privacy orientation and ongoing privacy training, who is responsible for tracking attendance, the consequences for failing to attend the orientation and ongoing training and when the initial privacy orientation is provided, namely whether it is provided prior to being given access to personal health information. Further, the frequency of the ongoing privacy training is not documented.

With respect to security training, aside from customized security training for employees of the Information Technology and Services Department and one-time security training for all employees at CIHI, no formal and ongoing security training has been provided. A security awareness training plan, however, has been developed to provide security training on such topics as the security program; the security policies, procedures, protocols and practices implemented by CIHI; security incident management; threat-risk approaches to the management of risk; and ensuring the security of workspaces.

It is recommended that CIHI develop and implement a comprehensive privacy and security training policy that encompasses both privacy and security orientation for new employees, as well as ongoing privacy and security training for current employees.

It is recommended that this policy set out when the initial privacy and security orientation will be provided, namely prior to being given access to personal health information, and the frequency of the ongoing privacy and security training. The policy should also articulate who is required to attend the privacy and security orientation and ongoing training, namely whether it is limited to employees or whether consultants, contractors and other agents are required to attend, and the person(s) responsible for delivering the privacy and security orientation and ongoing training. The policy should also emphasize that attendance is mandatory and describe the process used to track attendance, including who will track attendance and the consequences for failing to attend.

With respect to the ongoing privacy and security training, it is recommended that it include role-based training in order to ensure that employees understand how to apply the privacy and security policies, procedures and practices implemented by CIHI in their day-to-day work. It should also address any new privacy and security policies, procedures and practices implemented by CIHI and significant amendments to existing privacy and security policies, procedures and practices. Further, in determining the content of ongoing privacy and security training, it is recommended that CIHI consider recommendations made with respect to training contained in privacy impact assessments, vulnerability assessments, security audits, threat and risk assessments and security assessments.

CIHI also communicates to staff on privacy and security matters through communiqués and publications in *CIHIlights*. Since the initial review of its practices and procedures in 2005, CIHI has issued over twenty communiqués and publications in *CIHIlights* on such topics as desktop and mobile device security, encryption, audits of access to data holdings containing personal health information and acceptable methods of disseminating personal health information. CIHI also created a Privacy Practice Group in January 2008. Comprising employees from all program

areas, the Privacy Practice Group meets on a monthly basis to discuss the privacy program implemented by CIHI and to discuss privacy legislation, privacy best practices and recent orders issued by provincial and federal information and privacy commissioners and how they impact on CIHI.

Confidentiality Agreements

All employees of CIHI must sign an *Agreement Respecting Confidential Information, Privacy, Intellectual Property Rights and CIHI's Conflict of Interest Policy* ("Confidentiality Agreement") upon the commencement of employment and an *Annual Renewal of CIHI Employee Agreement Respecting Confidential Information* ("Annual Confidentiality Agreement") every year thereafter.

It is unclear from a review of the documentation, however, who is responsible for ensuring that the Confidentiality Agreement and Annual Confidentiality Agreement have been executed, how execution is tracked and the consequences for failing to execute these agreements. It is recommended that CIHI develop and implement a policy and procedure to formalize the practices and procedures related to the execution of these agreements.

This policy and procedure should require that the Confidentiality Agreement be executed upon the commencement of employment and prior to being given access to personal health information. It should also require that the Annual Confidentiality Agreement be executed on an annual basis and to provide a time frame each year in which the Annual Confidentiality Agreement must be executed. The policy and procedure should further emphasize that execution is mandatory and should describe the process that will be used to track execution, including who is responsible for tracking execution and the consequences for failing to execute the agreements.

By signing the Confidentiality Agreement and the Annual Confidentiality Agreement, the employee agrees that he or she will not use or disclose personal health information except as permitted by the privacy policy implemented by CIHI, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, and except with the prior written consent of CIHI. The employee also acknowledges that he or she has read and agrees to comply with the privacy policy implemented by CIHI and that the failure to comply with this privacy policy may result in disciplinary action, including but not limited to the termination of employment.

It is recommended that the obligation in the Confidentiality Agreement and the Annual Confidentiality Agreement to read and comply with the privacy policy implemented by CIHI be expanded to require the employee to acknowledge that he or she has read and agrees to comply with all privacy and security policies, procedures and protocols implemented by CIHI, including any privacy and security policies, procedures and protocols implemented after execution of these agreements, and that the failure to comply may result in disciplinary action.

Standard Contract Terms and Conditions

All persons providing services to CIHI must sign a contract containing standard terms and conditions, as well as a *Confidentiality Agreement*, which collectively set out the terms and conditions with respect to the collection, retention, use, disclosure and disposal of confidential information, including personal health information, and which require CIHI to be immediately notified, in writing, upon the breach of any such term or condition.

The standard contract terms and conditions state that once the services to CIHI cease or at any time upon request, the person providing services may either immediately return the confidential information to CIHI or permanently destroy the confidential information. This provision is inconsistent with the *Confidentiality Agreement*, which provides that the person providing services to CIHI must promptly return all confidential information and provides no such option to permanently destroy the confidential information. It is recommended that the requirements imposed on persons providing services to CIHI be consistent as between the *Confidentiality Agreement* and the standard terms and conditions of the contract that must be executed.

Further, if the person providing services to CIHI will be given the option to return the confidential information, it is recommended that the *Confidentiality Agreement* and the standard terms and conditions be amended to state that the confidential information must be returned in a secure manner and to set out the secure manner in which the confidential information must be returned.

If the person providing services to CIHI will be required to permanently destroy the confidential information, it is recommended that the *Confidentiality Agreement* and the standard terms and conditions be amended to state that the confidential information must be permanently destroyed in a secure manner, to provide a definition of secure destruction that is consistent with subsection 1(5.1) of Regulation 329/04 to the *Act* and to require the person providing services to provide written confirmation that the confidential information was permanently destroyed in a secure manner. The written confirmation should also be required to set out the date, time, location and method of secure destruction employed and should be required to bear the signature of the person who performed the secure destruction.

The standard terms and conditions further state that the person providing services to CIHI must acknowledge that the privacy policies, procedures and practices are set out in the *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*. It is unclear, however, whether persons providing services to CIHI are agents of CIHI and therefore are required to comply with these privacy policies, procedures and practices. If so, this should be explicitly set out in the standard terms and conditions.

Finally, the standard terms and conditions state that the person providing services to CIHI must agree to hold all confidential information in strict confidence and must agree to prevent any "unauthorized disclosure" of the confidential information. It is unclear, from a reading of these standard terms and conditions, what constitutes an authorized disclosure and therefore what is meant by an "unauthorized disclosure." It is recommended that the standard terms and

conditions set out the circumstances in which confidential information may be disclosed, namely where required by law, in order to avoid ambiguity as to what constitutes an "unauthorized disclosure."

Privacy Audit Program

CIHI has implemented a privacy audit program that includes three types of audits: program area audits, topic audits and external audits. Each of these audits and the process used in conducting these audits, are described in the *Revised Terms of Reference for the Privacy Audit Program*.

The Chief Privacy Officer and General Counsel is responsible for conducting these privacy audits and for preparing a Privacy Compliance Review Report that is presented to the Privacy and Data Protection Committee of the Board of Directors. The Privacy Compliance Review Report sets out the audits conducted, the process followed in conducting the audits, the findings of the audit and the recommendations arising from the audits. The results of the audits are also summarized in a Privacy Audit Program Annual Report that is presented to the entire Board of Directors.

Program area audits assess the compliance of a program area or specific data holding in the program area with the privacy policy implemented by CIHI, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*. In selecting program areas for privacy audits, priority is given to program areas determined to be high-risk, that is, program areas that hold particularly sensitive personal health information or that hold personal health information from all or most provinces and territories.

Topic audits involve the review of a particular topic across the organization to verify compliance with the privacy policy implemented by CIHI, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, as it relates to that particular topic. In selecting topics for privacy audits, priority is given to activities determined to be high-risk in terms of protecting the privacy of individuals whose personal health information is received. To date, topic audits have been conducted on the destruction of records of personal health information, inadvertent release of personal health information and internal data access procedures.

External audits assess the compliance of a recipient of information, including a recipient of aggregate information and a recipient of personal health information, with the terms and conditions of the *Confidentiality Agreement* entered into with the recipient as well as the *Third-Party Record-Level Data Request Form* and the *Client Information Request Form for Aggregate Data* that recipients must complete prior to the disclosure of information by CIHI. In conducting such audits, priority is given to the sensitivity of the information provided, the amount of information provided and whether the information provided will be used to link to other information.

Based on the *Revised Terms of Reference for the Privacy Audit Program*, it appears that the program area audits and topic audits only assess compliance with the privacy policy, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of*

Health Information. It is recommended that the *Revised Terms of Reference for the Privacy Audit Program* be amended to expand the audit program to assess compliance with all privacy policies, procedures and protocols implemented by CIHI, and not simply *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, in order to ensure a more robust privacy audit program.

Security Audit Program

CIHI conducts information security audits including reviews of access rights to data holdings containing personal health information; reviews of access rights of terminated employees; reviews of new technology devices to ensure they meet the security standards implemented by CIHI; reviews of audit logs; and annual vulnerability assessments, penetration testing and ethical hacks. However, these reviews are not consolidated in one document that sets out the process for conducting each of these reviews, the mechanism and format for reporting the findings of each review, to whom the findings of the reviews are reported and the procedure used in tracking the findings of the reviews in order to ensure that these findings are addressed.

It is recommended that CIHI develop and implement a security audit program policy and procedure that sets out the types of security audits that will be conducted, the frequency of each audit, the procedure used in conducting each audit, the person responsible for conducting each audit, the mechanism and format for reporting the findings of the audit, to whom the findings will be reported and the procedure to track the findings of the audit and how each finding was addressed.

Privacy Impact Assessments

CIHI prepares privacy impact assessments for each of its data holdings, including data holdings containing personal health information. The privacy impact assessments describe the current and intended scope of the data holding, the need for the data holding, the sources of the information, the contemplated uses and disclosures of the information, the statutory authority for the collection, use and disclosure of the information, the retention and destruction of information in the data holding and the technical architecture and safeguards implemented. These privacy impact assessments are made publicly available by CIHI on its website.

Limits on Access to Data Holdings Containing Personal Health Information

As indicated previously, CIHI has implemented policies, procedures and practices to limit access to data holdings containing personal health information by requiring staff to justify why their access is necessary, using a *CIHI Internal Data Access Authorization/Removal Request Form*, and by requiring approval for access to the data holding. CIHI has also commenced a project for the de-identification of health card numbers that, when completed, will result in the use of de-identified information, as opposed to identifying personal health information, for purposes of analysis and compiling statistical information with respect to the health system pursuant to its function as a prescribed entity under section 45 of the *Act*.

In addition, CIHI has implemented procedures and practices that require the Information Technology and Services Department to be notified by a manager, through a *CIHI Internal Data Access Authorization/Removal Request Form*, as well as by the Human Resources Department, when a staff member with access to a data holding no longer requires access or is no longer employed by CIHI in order to ensure that access is terminated. Access rights will then be terminated within eight business hours.

Dissemination of Personal Health Information

CIHI has also implemented a policy and associated procedures for the secure dissemination of personal health information. The *Methods of Disseminating Record-Level Data to External Clients and Data Providers Policy* and its associated procedures require that personal health information only be disseminated through one of three methods: through restricted web-based applications accessed by encrypted and secure socket layer sessions; through encrypted and password-protected CD/DVDs sent by courier with the password being provided by an alternate medium; and through an encrypted and password-protected email transmission with the password being provided by an alternate medium. Any exceptions to the policy require the approval of the Privacy and Legal Services Secretariat in consultation with the Information Technology and Services Department.

Privacy Policy on the Use of Mobile Computing Equipment

CIHI has developed and implemented a *Privacy Policy on the Use of Mobile Computing Equipment* that prohibits personal health information from being stored on mobile computing equipment except in specific and exceptional circumstances with the prior written approval of a Vice President. When such approval is granted, only the minimum amount of personal health information required may be temporarily stored on the mobile computing equipment and any personal health information temporarily stored must be de-identified to the fullest extent possible and must be encrypted and password-protected. The *Privacy Policy on the Use of Mobile Computing Equipment* also requires that the information be removed or destroyed within five days after the purpose is accomplished.

7. Physical Safeguards Implemented

CIHI has offices located throughout Canada including two offices in Ontario, one in British Columbia, one in Alberta, one in Quebec and one in Newfoundland and Labrador. An individual can only access the offices through a photographic identification card and personal identification number. CIHI employees must visibly display photo identification cards at all times. Doors with direct access to CIHI offices are locked at all times and alarmed and monitored after hours, on weekends and on statutory holidays. Locations are equipped either with surveillance cameras at various points of entry or by a security guard who is on duty twenty-four hours a day. All visitors must sign in at reception and must be issued a visitor identification card that must be worn while on premises and that must be returned on departure.

8. Technical Safeguards Implemented

CIHI has implemented a number of technical safeguards to protect personal health information in its custody or control against theft, loss and unauthorized use, disclosure, copying, modification and disposal. The technical safeguards implemented include the use of firewalls, network encryption and intrusion detection systems and two-factor authentication of its virtual private network.

The safeguards also include a mandatory, standardized and system-wide password-protected screen saver for all computers after a timeout period of ten minutes and the implementation of a *Network Login Password Policy* in accordance with industry standards.

CIHI also conducts yearly vulnerability assessments and ethical hacks on the information processing infrastructure, conducts targeted vulnerability assessments and ethical hacks on external-facing applications, conducts annual penetration testing of internal and external systems and conducts security audits on all production servers prior to deployment. In addition, since the last review of its practices and procedures in 2005, CIHI has conducted a physical and infrastructure security threat and risk assessment, a CIHI Portal security impact assessment and an Information Technology and Services security assessment. In addition, a threat and risk assessment of the CIHI Portal is currently underway and is expected to be completed by November 1, 2008. As part of ISO 27001 registration, the Information Technology and Services Department will also be undergoing a threat and risk assessment.

The Information Technology and Services Department has developed and maintained a consolidated and centralized log of all recommendations arising from vulnerability assessments, penetration testing, security audits, threat and risk assessments and security impact assessments.

In addition, for all databases, web applications and Windows servers containing health information, CIHI logs all user access and generates monthly audit reports. These monthly reports are sent to the Senior Database Administrator, all database administrators, all data modelers and the Senior Program Consultant - Security. The Senior Database Administrator and Senior Program Consultant - Security are then responsible for reviewing these audit reports immediately upon receipt and following up with users. Intrusion detection system and intrusion prevention system logs are also maintained and reviewed on a weekly basis by the Infrastructure Technology Team Lead who manually samples and reviews the logs.

CIHI is currently in the process of finalizing plans for the installation and configuration of software that will automatically collect, manage, correlate and report on security events from multiple hardware and software sources to allow CIHI to evaluate alerts in real time and to allow for streamlined management of security events. This software was installed and configured in July 2008 to collect logs from forty devices within CIHI's network infrastructure. In September 2008, CIHI installed the software on all other devices in the network infrastructure and commenced drafting governance and compliance policies, procedures and standards in relation to this software.

Summary of Recommendations

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

1. Amend its privacy policy, *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, in accordance with the comments set out on this report, including Appendix "C" to this report.

2. Develop and implement a centralized, integrated and comprehensive framework of written security policies and procedures.

3. Amend the *Information Security Events Policy* to address what information must be reported with respect to an information security event, containment and notification of the information security event, and the process in investigating an information security event.

4. Develop and implement a written policy and associated procedures for the annual review of the privacy and security policies, procedures and protocols implemented by CIHI.

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

   (a) Amending the *Storage and Destruction of CIHI Electronic Media Policy* pursuant to the comments provided in this report;

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

   (c) 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.

6. Develop and implement a written policy and associated procedures governing both initial privacy and security orientation and ongoing privacy and security training.

7. Develop and implement a written policy and procedure to formalize the practices and procedures related to the execution of the *Agreement Respecting Confidential Information, Privacy, Intellectual Property Rights and CIHI's Conflict of Interest Policy* and the *Annual Renewal of CIHI Employee Agreement Respecting Confidential Information* and amend these agreements in accordance with the comments provided in this report.

8. Amend the standard terms and conditions that all persons providing services to CIHI must comply with, as well as the *Confidentiality Agreement* that must be executed by all

persons providing services to CIHI, in accordance with the comments provided in this report.

9. Expand the privacy audit program to assess compliance with all privacy policies, procedures and practices implemented by CIHI and develop and implement a security audit program policy and procedure.

Statement of Continued Approval of Practices and Procedures

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

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

2. Amend the Confidentiality Agreement to include references to the *Act*, to reference and define personal health information, to reflect CIHI's obligations as a prescribed entity under the *Act*, 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. 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 the *Act*.

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 the *Act* and its regulation.

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.

APPENDIX "B"

DOCUMENTATION REQUESTED

Privacy

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

Security

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

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

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

Organizational and Other Documentation

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

APPENDIX "C"

RECOMMENDED AMENDMENTS TO THE *PRIVACY POLICY*

II Legislative Framework

It is recommended that this section be amended to state that CIHI is a prescribed entity pursuant to section 45 of the *Act* and to outline the consequences of being prescribed as an entity. In particular, that health information custodians are permitted to disclose personal health information to CIHI without consent for the purposes of analysis or compiling statistical information for the planning and management of the health system, that CIHI may only collect, use and disclose personal health information as permitted by the *Act* and that CIHI 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 which are reviewed by the IPC every three years.

Principle 5 - Limiting Use of Personal Health Information

Procedure 5.1(b) states "when the proposed use is consistent with the identified purpose of the data holding, the program manager may authorize the use of the personal health information." Procedure 5.2 (a) states that the program manager must review each proposed new purpose for personal health information "to determine if the proposed new purpose falls within the approved purposes statement for the data holding." Finally, Policy 5.3 states that CIHI may conduct analyses of personal health information for external parties consistent with the identified purposes of the data holdings and subject to the disclosure policies in *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*.

It is recommended that the above statements be amended to explicitly state that the proposed use, proposed new purpose or analyses must also comply with applicable laws, including the *Act*.

Principle 5 - Limiting Disclosure of Personal Health Information

Policy 5.10 states that CIHI discloses personal health information only for identified purposes, consistent with its mandate and core functions. It should also be emphasized that CIHI only discloses personal health information consistent with applicable laws to which CIHI is subject, including but not limited to the *Act*.

Conditions under Which Personal Health Information Disclosed

It is recommended that Policy 5.12 and its associated procedures be amended to clearly distinguish between the circumstances when identifiable personal health information is disclosed and the circumstances when de-identified information is disclosed and the policies, procedures and practices and the statutory conditions pursuant to which these disclosures are made.

Disclosure to the Data Provider that Originally Provided the Personal Health Information

Policy 5.12 and its associated procedures permit CIHI to disclose personal health information to the data provider, including the health information custodian, who originally provided the information. Subsection 18(5) of Regulation 329/04 to the *Act* only permits a prescribed entity to disclose personal health information to a health information custodian in these circumstances if the personal health information does not contain additional identifying information. The requirement to ensure that the personal health information does not contain additional identifying information should be included in any policy or procedure related to the disclosure of personal health information to the health information custodian that originally provided the information.

Disclosure to or Upon Direction from the Relevant Ministry of Health

Policy 5.12 and its associated procedures permit CIHI to disclose personal health information to, or upon the direction of, the relevant ministry of health. Section 18 of Regulation 329/04 to the *Act* only permits a prescribed entity to disclose personal health information, including to or upon direction of the relevant ministry of health, in certain circumstances. It is recommended that any policy or procedure relating to the disclosure of personal health information to or upon the direction of a ministry of health be amended to ensure that prior to such disclosure it is determined that the disclosure is permitted by the *Act*.

Disclosure for Research and Analysis

The provisions related to the disclosure for research and analysis in the *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information*, require greater clarification as it relates to the circumstances in which identifying personal health information is disclosed for research and analysis, the circumstances in which de-identified information is disclosed for research and analysis and the policies, procedures and practices and statutory conditions that apply to these disclosures. For example, page iv states "CIHI supports access to de-identified personal health information in a responsible, secure manner for purposes of analysis and research." This appears to suggest that CIHI only discloses de-identified information for research and analysis. However, elsewhere, including in Procedures 5.10 to 5.13, it suggests that identifying personal health information is disclosed for purposes of research and analysis.

It is also noted that the requirements in section 44 of the *Act* that must be satisfied prior to disclosing personal health information for research purposes without consent are not referenced in the *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information* and should be so referenced.

Further, page 3 of *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Health Information* states "when researchers request CIHI data, CIHI undertakes a detailed review of the requests in relation to its privacy and confidentiality policies and also requires recipients to sign agreements covering their obligations to keep the data confidential and secure." It should be emphasized that CIHI also reviews the requests to ensure that the disclosure meets the requirements of applicable legislation, including the *Act*.

Finally, none of the policies and procedures relating to the disclosure for research and analysis appear to address the disclosure of personal health information to other prescribed entities for the purposes of section 45 of the *Act*. It is recommended that this disclosure be addressed, including the practices and procedures that apply to such disclosures.