Information
and Privacy
Commissioner/
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of Cancer Care Ontario:

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

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Review of Cancer Care Ontario:
A Prescribed Entity under the *Personal Health Information Protection Act*

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

Responsibilities of Prescribed Entities

Section 45(1) of *PHIPA* permits health information custodians to disclose personal health information without consent to certain prescribed entities for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services, provided the prescribed entities meet the requirements of section 45(3).

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

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

Section 18(2) of Regulation 329/04 to *PHIPA*, further requires each prescribed entity to make publicly available a plain language description of its functions including a summary of the

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

Mandate of the IPC with Respect to Prescribed Entities

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

Review Process

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

Human Resources

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

Privacy

- Privacy policies and procedures that describe how the organization adheres to each fair information practice
- Privacy brochure – available upon request to the public
- Privacy Impact Assessments – for programs/database holdings

- Internal/external privacy audits
- Privacy crisis management protocols
- Data linkage protocols
- Procedures for de-identifying data
- Retention schedules and disposal procedures
- Inventory of all data holdings of personal health information
- Protocol for reviewing proposals in terms of their privacy impacts
- Mechanism for reviewing and updating privacy policies and procedures

Security

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

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

A site visit was to be scheduled within one month of the IPC receiving the documentation from the prescribed entity. The purpose of the site visit was to provide the prescribed entities with

an opportunity to provide additional information to the IPC and to clarify their practices and procedures, and to provide the IPC with an opportunity to:

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

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

Description of the Prescribed Entity

Cancer Care Ontario (CCO) is a prescribed entity under section 45 of *PHIPA*.

CCO is a planning and research organization that advises the Ontario government on all aspects of provincial cancer care, provides information to health care providers and decision-makers, and motivates better cancer system performance. CCO is an operational service agency within the Management Board of Cabinet Establishment and Scheduling of Agencies Directives and as such receives its funding from the Ontario government. Cancer Care Ontario's goal is improving the performance of the cancer system by driving quality, accountability and innovation in all cancer-related services as an advisor, rather than a manager of cancer care delivery.

CCO collects personal health information for management and planning purposes from health information custodians that are directly involved in the delivery of health care, such as hospitals and laboratories. CCO also receives personal health information from organizations such as the Canadian Institute of Health Information and Statistics Canada. The personal health information collected by CCO may include name, date of birth, health insurance number, information about the cancer and related illnesses, and information about hospitalizations and medical procedures. This information is retained in a variety of registries or databases, the largest of which is the Ontario Cancer Registry. Information collected for research registries, with the consent of the individual participant, may be accompanied by blood or tissue samples and information about family members. Blood and tissue samples that are collected are not physically stored at CCO.

Review of the Prescribed Entity

Documents Reviewed

CCO provided the IPC with two binders of documents on May 31, 2005, and one additional binder on June 17, 2005 containing:

Organizational Materials

- Introduction to CCO
- CCO Organizational Chart
- Profile of CCO Board Members
- Terms of Reference for CCO Board Committees
- Template Cancer Program Integration Agreement dated June 30, 2003
- *Cancer Act* (Ontario)
- Memorandum of Understanding between CCO and the Ministry of Health and Long-Term Care dated November 8, 1999
- Vision, Mission Statement, Goals and Guiding Principles Nov. 2003
- "Vital Signs: An Annual Report on Cancer in Ontario" (public address by CCO President and CEO) April 2005
- Summary of CCO Data Holdings and Responsible Data Steward
- Overview of Information Flow at CCO (Current & Future)
- Dept. of Preventive Oncology Current Projects
- Summary of Cancer Quality Council of Ontario (CQCO) Research Projects
- List of References using Ontario Cancer Registry Data: Jan. 1997-April 2005
- The *Ontario Cancer Plan*
- CCO Data Book
- CCO Information Management Strategy Update, May 25, 2005
- CCO Annual Report 2003-04

Human Resources Materials

- Summary of employees by department (not including consultants)

- Template Employee – Statement of Confidentiality
- Template Consulting Agreement
- Template Designated Contractor Agreement
- CCO Progressive Discipline Policy
- CCO Termination of Employment Policy
- CCO Privacy Delegation Chart
- Terms of Reference for Privacy Leads
- Terms of Reference for Data Stewards
- CCO Policy, Privacy Orientation and Training Program
- CCO Employee Orientation Guidelines
- CCO Employee Exit Procedures
- Template Non-Disclosure Confidentiality Agreement (third party)
- Template Third Party Access & Confidentiality Agreement
- Custodian Agreement with Sunnybrook and Women's College Health Sciences Centre re records of clinic operated by Canadian Radiation Oncology Services Ltd. (excl. Schedules C&D)

Privacy Materials

- Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario; includes:
    - Data Use & Disclosure Policy
    - Privacy Breach Policy
    - Privacy Impact Assessment Policy
    - Data Linkage Policy
    - Data Retention Policy
- Intranet Confidentiality Policy
- Intranet Code of Conduct
- Intranet Conflict of Interest Policy
- Ontario Familial Colorectal Cancer Registry Privacy and Confidentiality Policy

- CCO Statement of Information Practices
- Completed Privacy Impact Assessments:
    - An Evaluation of Cancer Care Ontario's Management of Privacy and Data Protection Issues dated June 12, 2001, prepared by David H. Flaherty Inc., Privacy & Information Policy Consultants;
    - Privacy Impact Assessment of a proposed Electronic Pathology Reporting System for Ontario dated Nov. 4, 2002, prepared by David H. Flaherty Inc., Privacy & Information Policy Consultants;
    - Privacy Impact Assessment of the Proposed Transfer of Selected Data from the Ontario Cancer Registry of Cancer Care Ontario to the Data Holdings of the Institute of Clinical Evaluative Sciences dated Oct. 19. 2003, prepared by David H. Flaherty Inc., Privacy & Information Policy Consultants.
- Key Data Sharing Agreements:
    - Template Data Sharing Agreement between CCO and Integrated Cancer Program Hospitals dated as of Dec. 31, 2004;
    - Template Ministerial Directive dated June 30, 2003 under Section 23(a), Reg. 965 to the *Public Hospitals Act* (Ontario) in respect of the submission of data from the Integrated Cancer Program hospitals to CCO;
    - Confidentiality & Research Agreement dated Mar. 12, 1999 between CCO and the MOHLTC, Health Insurance and Related Programs re data from the Registered Persons Database;
    - Confidentiality Agreement dated May 1, 2004 between CCO and the MOHLTC re data provided to CCO by Health Information Custodians as part of CCO's Pathology Information Management System (PIMS);
    - Template Ministerial Directive under Section 23(a) Reg. 965 to the *Public Hospitals Act* (Ontario) in respect of the submission of PIMS data from Hospitals to CCO;
    - Agreement between Statistics Canada and CCO re Cancer Registry Data dated May 6, 1994;
    - Data Sharing Agreement between CCO and ICES dated as of Dec. 1, 2003;
    - Data Sharing Agreement between CCO and CIHI dated as of May 1, 2005 in respect of in-patient and same day surgery patients in Ontario and National Ambulatory Care Reporting System data.

Other Materials

- CCO Interim Data Access Process for Person-Identifiable Health Data including:
  - Data Request Form for Person-Identifiable Health Data for Research Purposes
  - Non-Disclosure/Confidentiality Agreement for Researches
  - Data Request form for Person-Identifiable Health Data (Non-Research)
- Briefing Note for IPC/O, Are Cancer Registries Important to the Public's Health?
- Briefing Note for IPC/O, Impracticality of Patient Consent for Cancer Registration

Security Materials

- Report on Security program – physical measures
- CCO Visitor Access and Courier/Delivery Policy
- Overview of computer security measures at CCO (May 17, 2005 memo from Steve Hall to Pamela Spencer) as related to:
  - Database access
  - Data transfer procedures
  - Audit practices
- Data Security Audit materials including:
  - Introductory overview, "Information Security Program at Cancer Care Ontario"
  - Self-assessment report by Ainsworth/WhiteHat Inc.
  - Summary of Action Items
  - Status report on Action Items (inc. Disaster Recovery Plan)
  - Relevant CCO security policies (on CCO intranet):
    - Security of Electronic Information Policy
    - Provision of Computer & Telephone Equipment Policy
    - Electronic Mail General Policy
    - Data Centre Access and Usage Policy
    - Declaration & Disposal of Surplus IT Equipment Policy
  - Network diagram

To enhance transparency, the IPC requested that CCO post on its website additional information about the collection, use and disclosure of person health information by CCO; a description of CCO's data holdings; and specification of which of CCO's data holdings are used for the purposes of planning and managing the health care system as set out under section 45. Additional information was provided to the IPC on September 4, 2005 and September 16, 2005.

Site Visit

IPC representatives conducted a site visit at CCO on June 21, 2005.

IPC representatives were shown presentations on the following topics by CCO personnel as follows:

Introduction to CCO	President and CEO
Managing Privacy at CCO	Vice President, Corporate Affairs, General Counsel & Chief Privacy Officer
Information Management at CCO	Vice President & Chief Information Officer
Systems Security at CCO	Director, Information Technology
Ontario Breast Screening Program	Director, Ontario Breast Screening Program
Ontario Cancer Registry	Director, Informatics Research & Development, Senior Scientist

During a tour of the CCO facilities, focused meetings took place with CCO representatives as follows:

New Drug Funding Program	Director, Provincial Drug Reimbursement Programs
Reception, Project Management Office, Finance	
IT-IS – Server Room	Director, Information Technology
Cancer Quality Council of Ontario & Clinical Programs: Surgical Oncology, Radiation Treatment, Systemic Therapy	Director, Clinical Council Secretariat

Preventive Oncology	Manager, Research Unit
Ontario Familial Colorectal Cancer Registry	Scientist & Manager, Knowledge Transfer, Preventive Oncology - Surveillance Unit;
Ontario Cancer Registry (OCR)	Director, Informatics;
	Study Manager, Ontario Cancer Genetics Network
	Manager (OCR)
Public Affairs	

Findings of the Review

Human resources

CCO has clearly defined roles and responsibilities for privacy and security. A Chief Privacy Officer has been appointed and is accountable to the Board of Directors through the President and CEO of CCO. The Chief Privacy Officer is responsible for ensuring that CCO is compliant with all applicable privacy laws and CCO's internal Privacy Policy. The security team consists of a Chief Information Officer, Director of Information Technology and a Systems Security Specialist. A Core Privacy Committee has also been established. In addition, each program area has a privacy lead that is responsible for implementing privacy and security policies and procedures that are appropriate for each program area. The privacy lead is the primary contact person for the Chief Privacy Officer on privacy matters. There is also a Data Access Committee. A Data Access Coordinator is responsible for receiving and processing all requests for access to data, both internal and external, and reports to the Data Access Committee. Further, each data holding of CCO has a responsible data steward.

Staff is oriented to CCO's privacy and security policies and expectations upon offer of employment. At that time, they are provided with copies of the Privacy Policy and other key privacy and security policies. Where new employees will be working with CCO data holdings, additional orientation is provided upon arrival at CCO. New hires meet with the Data Access Coordinator to review the privacy policies, the privacy breach policy, and the confidentiality policy. Additional training sessions are scheduled within the appropriate areas of CCO on a case-by-case basis. CCO Program Area Directors/Managers are responsible for ensuring that consultants and agents of CCO employed within their program area are familiar with and adhere to the CCO Data Use and Disclosure Policy.

All employees, consultants and contractors of CCO are required to sign confidentiality agreements. Templates of the three types of agreements were reviewed by the IPC. Employees, medical staff,

volunteers, other workers, and students are required to sign a Statement of Confidentiality. Consultants are required to sign a Consulting Agreement. Contractors are required to sign a Designated Contractor Agreement.

These agreements could be enhanced in a number ways. The documentation provided indicates that staff will be oriented to the CCO's privacy and security policies upon offer of employment and that part of the orientation is that they must agree to abide by the privacy and security policies, as a condition of employment. The documentation further states that by signing the Statement of Confidentiality, new employees acknowledge that they have read, understood and agree to abide by these policies. However, there is no statement to this effect in the Statement of Confidentiality or in the other agreements that must be signed by consultants and contractors. Further, none of the agreements inform individuals of the consequences of a breach of the agreement. Also, given the status of CCO as a prescribed entity under *PHIPA*, it is important that these agreements refer to this legislation and include a definition of and reference to personal health information.

Accordingly, it is recommended that these agreements be amended to include a provision advising of the consequences of breach of the agreement; a provision requiring each person signing the agreement to comply with CCO's privacy and security policies, procedures and practices; a reference to the status of CCO as a prescribed entity under *PHIPA;* and a definition of and reference to personal health information.

We also note that the Consulting Agreement and Designated Contractor Agreement specifically state that the person signing the agreement is not an agent of CCO's. We assume that this statement is directed toward the common law meaning of the term "agent" rather than the term "agent" as defined in PHIPA. Otherwise, with respect to consultants, this stipulation would be inconsistent with CCO's Data Use and Disclosure Policy which specifically designates consultants as Internal Data Users. If consultants and contractors are not considered to be agents of CCO, as defined under *PHIPA*, the provision of personal health information to such individuals would be considered a disclosure rather than a use of personal health information. *PHIPA* strictly limits the disclosure of personal health information by entities prescribed under section 45. CCO should revise these contractual agreements with third parties to clarify the intent of the wording dealing with agency and to ensure that the agreements and Data Use and Disclosure Policy are consistent.

CCO's Data Use and Disclosure Policy addresses the issue of privacy breaches. It states that violations of this policy will result in the loss of data access privileges as well as the imposition of applicable CCO disciplinary procedures. Violations of the policy by consultants/agents will result in the loss of data access privileges, as well as contractually defined penalties. CCO has disciplinary procedures for misconduct. Discipline may include oral warnings, written warnings, suspension, automatic termination for a single act of misconduct, or termination. However, the discipline policy is general and does not specify what constitutes misconduct or serious misconduct in the context of privacy breaches nor does it specify the potential consequences of such privacy breaches. Similarly, the template Designated Contractor Agreement does not include any mention of the consequences of privacy breaches. The Privacy Breach Policy states

that where a privacy breach is intentional or the result of negligent work practices, disciplinary action will be taken and this could result in termination of employment and/or laying charges. The consequences for privacy breaches should be clarified and harmonized in CCO's Data Use and Disclosure Policy, the policy for discipline and the confidentiality agreements that employees, consultants and contractors are required to sign. It would also be helpful to consolidate this information in one document.

The Third Party Access & Confidentiality Agreement is signed by suppliers who will have access to CCO's information systems. Although this agreement has been updated to refer to *PHIPA*, it currently only refers to personal information and should be amended to include references to personal health information. This agreement also has a clause that Supplier Co. shall notify immediately if "any known or suspected unauthorized access" by Supplier Co.'s employees or agents takes place. This clause should be expanded to require notification with respect to breaches that result in access by outsiders.

When CCO stopped providing cancer treatment services, custody and control of its records of personal health information were assumed by the Regional Cancer Centres' host hospitals. The only exception was with respect to cancer patients who received treatment at the Canadian Radiation Oncology Services Clinic located at Sunnybrook and Women's College Hospital. CCO established a Custodian Agreement with Sunnybrook and Women's College Hospital to cover the storage and access to these records. The IPC recommends that this Custodian Agreement and Schedule B to the agreement should be amended to reflect the requirements and terminology of *PHIPA* with respect to capacity and substitute decision-making.

Privacy

Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario was updated and implemented in July 2005. This document describes CCO's privacy program; legislative authority for the collection, use and disclosure of personal health information; and data holdings. It also describes how CCO complies with each of the 10 fair information principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*.

The policy should be amended to clarify that, as a prescribed entity under section 45 of *PHIPA*, CCO is not required to provide individuals with a right to access and request correction of their own personal health information and that personal health information will only be disclosed with the consent of the individual or as permitted or required by *PHIPA*. In addition, this policy should be amended to harmonize all references to CCO's data holdings.

Although CCO has made available on its website a description of its information practices and responses to a series of Frequently Asked Questions about its information practices, it does not have a privacy brochure that is available to cancer patients and other members of the general public. It is our understanding that a privacy brochure is being developed. Given that some members of the public may not have access to the Internet, a written brochure is essential to

ensure transparency. Privacy brochures should be made available wherever cancer treatment is provided and upon request from CCO.

CCO does not currently have the capability to audit internal access to its data holdings, screening programs or research registries that contain personal health information. CCO intends to commence an internal access audit program as soon as it can recruit a security specialist. This recruitment is currently in process. CCO should inform the IPC when it commences its internal access audits and provide the IPC with information about the nature, scope and frequency of the audits and copies of policies, and procedures for processes implementing and operationalizing these audits.

CCO has completed three privacy impact assessments. A general privacy impact assessment of CCO's management of privacy was undertaken in 2001. Two other privacy impact assessments were undertaken with respect to specific programs. Three privacy impact assessments are currently underway and should be provided to the IPC upon completion. Each of the privacy impact assessments relate to specific programs. In addition, a privacy review of CCO's programs and systems was commenced in November 2004. This privacy review should be completed and recommendations implemented where appropriate.

CCO has recently developed a procedure for conducting privacy impact assessments to assess a program and system's privacy risks, its compliance with *PHIPA*, and, where required, mitigating strategies and action plans. While all new programs and systems and changes to existing programs and systems now require a privacy impact assessment, by 2008, all existing programs and systems of CCO will undergo a privacy impact assessment. Reports on each of these assessments should be forwarded to the IPC as they become available.

CCO has a policy for dealing with privacy breaches. This policy involves containment of the breach, notification of appropriate individuals and remedies to ensure that a similar breach does not happen in the future. This policy offers whistleblower protection for employees who report privacy breaches.

CCO uses identifiable information to conduct analyses; however, the reports on these analyses do not contain identifiable data. It is the IPC's view that the analyses of data undertaken by CCO generally do not require the use of identifiable data. Although identifiers may be necessary for the purpose of linking data across time and sources, once any required data linkages have been made, the identifiers should either be stripped or encrypted before the data is used for conducting project-specific analyses. To address this issue, the IPC recommends that CCO develop a formal policy for routinely de-identifying data before it is used. The policy should specify when, how and by whom personal health information will be de-identified before it is used to carry out the day-to-day business of CCO. The policy should ensure that employees use the least identifiable data possible in their day-to-day work and that the least number of individuals have access to personal health information. The policy should be forwarded to the IPC when it has been completed.

CCO has a policy that governs data linkages. Data linkages are undertaken only with the consent of the individual or with consideration to the following criteria:

- The data linkage is consistent with CCO's mandate and serves the public interest;
- The results of the data linkage will not be used for any purpose that is reasonably contemplated to be detrimental to the individual;
- Agreements are in place to identify responsibility for the data and specify conditions with which the researcher must comply regarding relinking, further use and disposal of the data; and
- There are no other practical alternatives for conducting the analysis.

It is our view that these criteria should be requirements rather than considerations in determining whether or not a data linkage should be undertaken. In addition to these safeguards, CCO should expand this policy to include safeguards 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, prior to being used for project-specific analyses. Once the linked datasets have been de-identified, analysts and researchers should also agree not to use data in a manner that could re-identify an individual.

CCO has a procedure for processing requests for information from third parties, which is referred to as the *CCO Data Access Process for Personal Health Information*. This policy should explicitly state that CCO does not disclose personal health information unless the individual to whom the personal health information relates consents to the disclosure or the disclosure of personal health information is permitted or required by *PHIPA*. Specifically, with respect to disclosures for research purposes the *CCO Data Access Process for Personal Health Information* should state that CCO does not disclose personal health information without the consent of the individual to whom the personal health information relates unless the requirements of section 44 of PHIPA have been satisfied, namely, the researcher prepares a research plan and receives research ethics board approval. With respect to disclosures for non-research related purposes, the *CCO Data Access Process for Personal Health Information* should explicitly state that CCO does not disclose personal health information without the consent of the individual to whom the personal health information relates unless the disclosure is permitted by section 45 of *PHIPA* or section 18 of Regulation 329/04.

There are two request forms – one is used for research purposes and the other is used for non-research purposes. Both of these forms should clarify CCO's obligations with respect to the disclosure of personal health information under *PHIPA*.

The *Data Request Form for Person-Identifiable Data for Research Purposes*, which enables researchers to request personal health information from CCO for research purposes, should state that CCO does not disclose personal health information without the consent of the individual to whom the personal health information relates unless the requirements of section 44 of *PHIPA* have been satisfied, namely, the researcher prepares a research plan and receives research ethics

board approval. CCO should ensure that the research plan meets all of the requirements of *PHIPA* and Regulation 329/04 before disclosing personal health information to a researcher.

Further, the *Data Request Form for Person-Identifiable Data* should be amended to require individuals, corporations and organizations requesting personal health information from CCO for non-research related purposes to indicate whether consent to the disclosure of personal health information has been obtained from the individual to whom the personal health information relates. If consent has been obtained, the individual, corporation or organization requesting the personal health information must provide a copy of the consent. If consent has not been obtained, the individual, corporation or organization requesting the personal health information must provide the legislative authority for the disclosure without consent.

CCO requires all requesters to sign a Non-Disclosure/Confidentiality Agreement.

Security

A summary review of CCO's information security policies, procedures and other documentation was undertaken, along with an inspection of the physical premises and interviews with relevant IT personnel. On the basis of our visit, examination, and observations we found no evidence of major security risks, threats or breaches. We are therefore broadly satisfied that CCO's information security measures are adequate for the purposes of protecting the privacy of personal health information held.

CCO's offices are monitored by security services including video surveillance, the manual unlocking and locking of doors at the beginning and end of each work day, and security guard rounds. Offices are protected by locked doors and coded passcard entry. All confidential information is retained in locked file cabinets in locked offices. Visitors must sign in and wear an ID badge at all times.

In terms of information system security, access to CCO systems is granted to users, upon request and with the approval of the user's supervisor. Systems are password protected and passwords must be created and maintained in accordance with the CCO's password policy. Access to databases is granted on a need-to-know basis.

Data are transferred to CCO in a number of ways including physical shipment, online data entry and electronic transfer. On-line data entry and electronic transfer of data is done through an encrypted connection to CCO. For some systems, the network provided by Smart Systems for Health Agency or a virtual privacy network (VPN) is used for transferring data between health information custodians and CCO. The transmission of personal health information via e-mail is strictly prohibited by CCO's email policy. Certain data that is sent to CCO from MOHLTC is sent via magnetic tape. Other data that are physically transported are stored on password-protected CD-ROMs.

In terms of internal and external security audits, the IT Security Committee is responsible for completing an annual security assessment and/or penetration test of CCO's systems. The scope

of these assessments may vary and will be determined by the Director of IT, with the approval of the Chief Information Officer and the Chief Privacy Officer. One comprehensive security assessment was completed this year. Not all of the recommendations have been acted upon. It is recommended that CCO act upon the recommendations arising from this assessment, as soon as possible. In addition, although CCO has committed to conducting annual security assessments and threat and risk assessments (TRAs) in conjunction with project-specific PIAs, the IPC recommends that comprehensive, organization-wide TRAs, such as the one recently completed, be repeated on a periodic basis.

Although most of CCO's systems are capable of producing audit trails, this information is not routinely used to ensure that access to CCO's data holdings is restricted to authorized persons for appropriate purposes. The IPC recommends that audit trails be randomly checked for this purpose.

CCO also has a disaster recovery plan and a process for reviewing and updating its security policies on an annual basis.

Summary of Recommendations

Major Recommendations

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

Other Recommendations

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

1. Amend agreements with staff, consultants and contractors to include a provision advising of the consequences of breach of the agreement; a provision requiring each person signing the agreement to comply with CCO's privacy and security policies, procedures and practices; a reference to the status of CCO as a prescribed entity under *PHIPA;* and a definition of and reference to personal health information.

2. Amend agreements with consultants and contactors to clarify the use of the term "agent" and to ensure that these agreements and CCO's Data Use and Disclosure Policy are consistent.

3. Amend the Custodian Agreement with Sunnybrook and Women's College Health Sciences Centre and Schedule B to the agreement to reflect the requirements and terminology of *PHIPA* with respect to capacity and substitute decision making.

4. Complete the Privacy Brochure and make it available wherever cancer treatment is provided and upon request from CCO.

5. Inform the IPC when the internal access audits commence and provide the IPC with information about the nature, scope and frequency of the audits and copies of policies, procedures for processes implementing and operationalizing these audits.

6. Implement the recommendation from the November 2004 privacy review of CCO's programs and systems where appropriate.

7. Complete the privacy impact assessments of all CCO's programs and systems, as set out in CCO's PIA Policy and forward the reports to the IPC as they become available.

8. Develop and implement a formal policy for de-identifying data that ensures that employees use the least identifiable data possible in their day-to-day work and that the least number of individuals have access to personal health information and forward this policy to the IPC.

9. Amend the data linkage policy such that the physical linking of records is carried out in a manner that ensures a minimum number of individuals have access to personal health information and that identifiers are either stripped or encrypted in the subsets of CCO data holdings that are used for project-specific analyses.

10. Amend the CCO Data Access Process for Personal Health Information document and the two access request forms to reflect the requirements of *PHIPA* for the disclosure of personal health information.

11. Complete the implementation of recommendations from the most recent security assessment.

12. Implement a system for routinely checking systems audit trails.

13. Repeat comprehensive, organization-wide TRAs, such as the one recently completed, on a periodic basis.

Statement of IPC Approval of Practices and Procedures

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