Information
and Privacy
Commissioner/
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of Cancer Care Ontario in respect of the Colorectal Cancer Screening Registry:

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

Ann Cavoukian, Ph.D.
Commissioner
May 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

Review of Cancer Care Ontario in respect of the Colorectal Cancer Screening Registry :
A Prescribed Person 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 Persons

Section 39(1)(c) of *PHIPA* permits health information custodians to disclose personal health information without consent to certain prescribed persons who compile or maintain registries for purposes of facilitating or improving the provision of health care or that relate to the storage or donation of body parts or bodily substances ("prescribed persons").

Section 13(2) of Regulation 329/04 to *PHIPA* requires each prescribed person to have in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information. Section 13(2) further requires each prescribed person to ensure that these practices and procedures are approved by the IPC every three years, in order for health information custodians to be able to disclose personal health information to the prescribed person without consent and for the prescribed person 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*; and
- disclose personal health information as if it were a health information custodian for purposes of sections 44, 45 and 47 of *PHIPA*;

Further, section 13(3) requires prescribed persons to make publicly available a plain language description of the functions of the registry, including a summary of the practices and procedures to protect the privacy of individuals whose personal information it receives and to maintain the confidentiality of that information.

Mandate of the IPC with Respect to Prescribed Persons

Prescribed persons 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 every three years.

Review Process

The review process included a review of documentation relating to the practices and procedures of the prescribed person 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 is held by the prescribed person. Before commencing the review, the IPC provided the prescribed person 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 person was informed that they were required to implement privacy and security measures and safeguards commensurate with the nature of the work undertaken by the prescribed person, the amount and sensitivity (e.g., level of identifiability) of the information in the custody and control of the prescribed person, and the number and nature of the individuals who have access to personal health information. The scope of the review included practices and procedures relating to personal health information included in the specific registry associated with the prescribed person under section 13(1) of Regulation 329/04.

A site visit was scheduled within one month of the IPC's receiving the documentation from the prescribed person. The purpose of the site visit was to provide the prescribed person 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 person.

Following the document review and site visit, the prescribed person was informed of actions that it needed to take prior to having its practices and procedures approved by the IPC. Once

all necessary action had been taken, the IPC prepared a draft report that was submitted to the prescribed person for review and comment. When the IPC was satisfied that the prescribed person had implemented practices and procedures that were sufficient to protect the privacy and confidentiality of personal health information, a letter of approval was issued.

Description of the Prescribed Person

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 within Management Board of Cabinet's Agency Establishment and Accountability Directive 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.

In addition to being an entity prescribed for the purposes of section 45(1) of *PHIPA*, CCO has been prescribed as a person who compiles or maintains the Colorectal Cancer Screening Registry for the purpose of facilitating or improving the provision of health care, under section 39(1)(c) of *PHIPA*. CCO refers to the colorectal cancer screening program as ColonCancerCheck (CCC).

In January 2007, the Ministry of Health and Long-Term Care in conjunction with CCO launched a province-wide, population-based screening program for colorectal cancer. The goals of the program are to increase screening rates and thereby reduce mortality due to colorectal cancer. The program targets asymptomatic Ontarians who are 50 years and older. The method of screening and frequency of screening is determined by risk profile.

To determine the population eligible for screening, CCO collects personal health information from sources such as the Ministry of Health and Long-Term Care and CCO, in its role as a prescribed entity. Eligible participants, who have a primary care provider, are invited to participate in the screening program. All screening results will be reported to the program. The program will inform individuals about negative screening results. Positive screening results will be conveyed to patients through their primary care providers. Individuals with positive test results, who do not have a primary care provider, will be contacted by the program to arrange for follow-up care.

At any time, individuals will be able to withdraw from being contacted by CCO for the purposes of the screening program. However, all colorectal cancer screening tests results and other personal health information will continue to be collected, used and disclosed by CCO for the purposes of the Colorectal Cancer Screening Registry, as permitted under section 39(1)(c) of *PHIPA*.

Review of the Prescribed Person

Documents Reviewed

CCO provided the IPC with documents on February 8, 2008, including:

- CCC Privacy Acknowledgement Form
- CCC Privacy Training and Awareness Procedure
- CCC Privacy Breach Management Procedure
- CCC Privacy Specialist Terms of Reference
- CCC Privacy Breach Management Task Force Terms of Reference
- CCO Systems Security Specialist Job Description
- CCC Privacy Training Slides
- CCC Privacy Training and Awareness Procedure
- CCC Compliance Procedure
- CCO Corporate Privacy Training Slides
- CCO Security Training Slides
- CCO Data Access Committee Terms of Reference
- CCC Privacy Policy
- CCC Access Control Procedure
- CCC Privacy Inquiries and Complaints Procedure
- CCO's Data Quality Slides
- CCC Privacy Commitment Statement
- CCC Privacy Page of the CCO Website
- Fecal Occult Blood Test (FOBT) Kit Privacy Insert
- CCC Privacy Impact Assessment dated February 4, 2008
- CCC IPC Presentation Slides
- PIA Risk Mitigation Chart
- CCC Roles and Responsibilities Overview

CCO Media Destruction Policy and Procedure

Logical Architecture

CCO Security of Electronic Information Policy

CCO Off-Premises Access and Wireless Network Policy

CCO Acceptable Use of CCO Systems Policy

CCO Data Centre Access and Usage Policy

CCO Electronic Mail General Policy

Vulnerability Assessment Summary

CCO Data Backup Restore Policy and Procedure

Site Visit

The IPC conducted a site visit of the primary site of CCC on March 7, 2008. The following representatives of CCO participated in the site visit:

Vice President Corporate Affairs, General Counsel and Chief Privacy Officer, CCO

Privacy Director, CCO

Systems Security Specialist, CCO

Vice President, Prevention and Screening, CCO

Facilities Manager, CCO

Privacy Team Representative, ColonCancerCheck

Findings of the Review

Human resources

CCO in respect of the Colorectal Cancer Screening Registry has clearly defined roles with respect to privacy and confidentiality. The CCC Privacy Specialist coordinates that day-to-day operation of the privacy program. The CCC Privacy Specialist is supported by the Privacy Breach Management Task Force and the CCO Systems Security Specialist. The CCC Privacy Specialist reports to CCO's Privacy Director on all privacy-related matters and to the CCC Program Director on program-related matters. Information technology security-related matters are managed by CCO's Systems Security Specialist.

CCO in respect of the Colorectal Cancer Screening Registry has a robust on-going privacy and security training program. In accordance with the CCO Privacy Training and Awareness Procedure, all new staff (including employees, students, contractors, consultants, or third parties who are employed or affiliated with CCO to support CCC) are required to receive privacy training and security training, within the first two weeks of employment. All staff are responsible for reading and understanding the CCC Privacy Policy and CCO's IT Security Program polices. Upon completion of the privacy training, all staff affiliated with CCC are required to sign a Privacy Acknowledgment Form. Individuals, who breach CCC's Privacy Code either intentionally or as a result of negligent work practices, are subject to disciplinary procedures up to and including termination of employment and/or laying criminal charges.

In addition, all contractors, consultants or third parties that are not employees must sign contracts containing confidentiality provisions before they begin work with CCC.

CCO in respect of the Colorectal Cancer Screening Registry has not yet finalized its agreements with the Ministry of Health and Long-Term Care, with CCO in its capacity as a prescribed entity under section 45(1) of *PHIPA*, and with the third party mailing service provider. These agreements should be finalized as soon as possible and forwarded to the IPC.

Privacy

CCO with respect to the Colorectal Cancer Screening Registry has a comprehensive Privacy Policy which will be readily available to the public on CCC's website. CCO has also developed a statement of its commitment to privacy, frequently asked questions, and an overview of their privacy program which is posted on CCC's website.

A Fecal Occult Blood Test (FOBT) Kit Privacy Insert has also been developed, but needs to be revised to clarify that individuals will be able to obtain the results of their colon cancer screening test, even if they decide to opt out of being contacted by the program. The insert should be revised as soon as practical and forwarded to the IPC.

CCO has conducted a comprehensive privacy impact assessment regarding the registry and has mitigated or is in the process of mitigating all of the privacy risks identified. The mitigation of each risk is being tracked in a PIA Risk Mitigation Chart. CCO also indicated that it will be developing a summary of the PIA which will be made available to the public on the CCC website. This summary should be finalized, forwarded to the IPC and posted on the CCC website, as soon as possible.

CCO in respect of the Colorectal Cancer Screening Registry has implemented a CCC Privacy Breach Management Procedure which requires the CCC Privacy Specialist to appoint a Privacy Breach Management Task Force. This Task Force will support the CCO Privacy Specialist in containing, investigating and resolving privacy breaches. CCO has also developed Privacy Breach Management Task Force Terms of Reference.

CCO has also developed a CCC Privacy Inquiries and Complaints Procedure. All complaints and inquiries are directed to the CCC Privacy Specialist who must consult with the CCO Privacy Director.

Personal health information is disclosed from the Colorectal Cancer Screening Registry to third parties only for purposes related to the provision of health care to the individual; to prescribed entities under section 45(1) of *PHIPA* for the purposes of planning and managing the health care system; to researchers subject to the requirements set out in *PHIPA*; and to a health data institute for analyses of the health system. The CCO Data Access Committee must review and approve all requests from external parties for personal health information maintained in the registry and for record linkages. CCO Data Access Committee Terms of Reference were provided to the IPC; however, detailed information about the policies and procedures for granting access to third parties has not been provided in the documentation. While CCO has a use and disclosure policy in respect of its functions as a prescribed entity under section 45(1) of *PHIPA*, it also needs a use and disclosure policy in respect of its functions as the prescribed person who compiles and maintains the Colorectal Cancer Screening Registry. As soon as possible, CCO should develop the policies and procedures for reviewing and approving third party access to the registry and forward these to the IPC.

CCO has yet to develop a protocol for de-identifying personal health information, prior to its use and disclosure for secondary purposes, such as research. CCO should develop this protocol as soon as possible and forward to the IPC.

CCO in respect of the Colorectal Cancer Screening Registry has developed a CCC Compliance Procedure that describes the privacy reviews and audits that will be conducted to ensure it is meeting its obligations under *PHIPA*. At least once per year, the CCC Privacy Specialist is required to coordinate three types of reviews: Policy, Operational Effectiveness, and Physical Security. The results of the reviews are summarized in an Annual Privacy Report. The Annual Privacy Report is also submitted to the Chief Privacy Officer for sign off. A copy of the Annual Privacy Report is provided to the Privacy Director, the CCC Program Director, and the IPC and published on the CCC website.

Security

CCO in respect of the Colorectal Cancer Screening Registry has a comprehensive security program to protect personal health information in its custody and control. The CCO Systems Security Expert ensures that all CCC staff undergo security training and sign a security acknowledgement form.

In terms of physical security, CCO provides a secure environment for operating the Colorectal Cancer Screening Registry. Access to the offices is secured by locked elevators and doors, which may be access by authorized staff only. Staff are required to wear photo identification badges. Staff are required to identify, sign in and escort all visitors to the offices, in accordance with the CCO Visitor Access Policy.

Access to the data centre where the registry is housed is governed by the Data Centre Access and Usage Policy. Access to the data center is on an as needed basis and controlled with the use of proximity access cards and monitored with video surveillance. There are 3 levels of access: unrestricted, limited, and temporary. Personnel with temporary level of access must be supervised while performing any work in the data centre.

Staff are required to keep portable computers locked to immovable objects at all times when in use. When not in use, they must be stored in a secure location, such as a locked cabinet. In addition, staff must use encryption on all computers and portable media. Hard copies of personal health information also must be kept in a secure location when not in use.

All calls to participants in the screening program are made from a private office.

The physical security practices of registry staff are reviewed by the CCC Privacy Specialist on a regular basis.

Access to the Colorectal Cancer Screening Registry is strictly controlled in accordance with the CCC Access Control Procedure. Only staff that require access to the registry for the performance of their jobs are granted access. The CCO Security of Electronic Information Policy ensures that electronic information and data are accessible only to staff with authorized access. Access to the registry is governed by two-factor authentication. Passwords must be carefully constructed in accordance with strict criteria and changed every 90 days. All personal health information must be stored on CCO servers rather than on desktop computers and mobile storage devices.

Wireless computer networks are not permitted at CCO locations. The CCO Off-Premises Access and Wireless Network Policy sets out restrictions and imposes standards for remote access to CCO networks and for the use of wireless networks. The CCO Acceptable Use of CCO Systems Policy defines what is considered to be acceptable use of CCO systems and information assets. For example, staff are required to keep user identifications and passwords confidential at all times and must adhere to prohibitions against downloading or installing software. Staff are also required to use whole disk encryption on all computers and to encrypt data on portable media such as USB keys. CCO Electronic Mail General Policy prohibits the use of email to transmit personal health information. A password-protected memory key must be used to transport confidential information.

The CCO Media Destruction Policy and Procedure defines the minimum requirements to meet for the destruction of data, prior to such storage media being surplused, transferred, disposed of, or replaced by new media. When media is destroyed, this is documented for audit purposes. The CCO Data Backup Restore Policy and Procedure describes the schedule and process for backing up CCO's information assets located on the server platform. Once the technology solution for the registry has been built, a full disaster recovery plan will be developed.

In addition, CCO has implemented in 2007 (or will implement in 2008) the following advanced security measures:

- port level security to prohibit the use of unknown or untrusted personal computers or laptops on the CCO network;
- PGP whole disk encryption was introduced for personal computers and laptops (data on memory keys are also encrypted);
- RSA SecurID 700 Tokens will be implemented for all off-premises access in 2008 to create a strong two-factor authentication system.

Unfortunately, those significant improvements were not fully reflected in all of the security-related documents that were submitted to the IPC. The IPC recommends that the security policies and procedures should be updated to incorporate recent security enhancements.

In 2007, an analysis of the CCO Network Environment was conducted by an independent third party to identify potential weaknesses that could affect the security and integrity of CCO's applications. The results of this assessment are outlined in the Vulnerability Assessment Summary. CCO has implemented all of the recommendations made following this assessment and plans to conduct a follow-on assessment once the registry has been built. In addition, the IPC recommends that CCO conduct a comprehensive threat and risk assessment specific to the Colorectal Cancer Screening Registry.

CCO's Systems Security Specialist reviews CCO's IT Security Policies on an annual basis and submits revisions to the Director of Information Technology for approval.

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 prior to the IPC approving the information practices of CCO in respect of the Colorectal Cancer Screening Registry.

Other Recommendations

Based on the review of documentation and the site visit to CCO where the registry is housed, the IPC is making the following recommendations that CCO is not required to act upon/resolve prior to the approval of its information practices in respect of the Colorectal Cancer Screening Registry:

1. CCO in respect of the Colorectal Cancer Screening Registry should finalize its agreement with the Ministry of Health and Long-Term Care as soon as possible and forward a copy of the agreement to the IPC.

2. CCO as a prescribed person who compiles or maintains a registry should finalize its agreement with CCO as a prescribed entity under section 45(1) of *PHIPA* as soon as possible and forward a copy to the IPC.

3. CCO should finalize its agreement with the third party mail service provider as soon as possible and forward a copy to the IPC.

4. CCO should finalize the templates for invitation letters, screening results notification letters, and screening reminder letters as soon as possible and forward copies of these templates to the IPC.

5. CCO should develop a summary of the privacy impact assessment on the Colorectal Cancer Screening Registry and make this available on the CCC website as soon as possible.

6. CCO should revise its FOBT Kit Privacy Insert as described in this report as soon as it is practical and forward to the IPC.

7. CCO should develop policies and procedures for reviewing and approving requests from external parties for access to the data maintained within the Colorectal Cancer Screening Registry and forward to the IPC.

8. CCO should develop and forward to the IPC a protocol for de-identifying the personal health information maintained in the registry prior to its use for secondary purposes, including analysis and research.

9. CCO should update its security policies and procedures to reflect recent security enhancements.

10. CCO should conduct a comprehensive threat and risk assessment in respect of the registry, with emphasis on both internal and external threats to security.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that CCO in respect of the Colorectal Cancer Screening Registry 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 May 1, 2008, the practices and procedures of CCO with respect to the Colorectal Cancer Screening Registry have been approved by the IPC.

In order to synchronize the timing of the IPC's review of CCO in respect of the Colorectal Cancer Screening Registry with the reviews of other prescribed persons, this approval will remain in effect until October 30, 2008. Before September 1, 2008, CCO should submit to the IPC any new or revised practices and procedures so that the IPC may review and approve these practices and procedures effective October 31, 2008 for a further period of three years.