Information
and Privacy
Commissioner of
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 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 Cancer Care Ontario:

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 Cancer Care Ontario, which were the subject of an earlier report of the IPC, are set out in Appendix "A" to this report. Cancer Care Ontario has since implemented all the recommendations made during the initial review of its practices and procedures, with the exception of the recommendation respecting the review of audit trails, which will be implemented in 2009.

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. Cancer Care Ontario submitted the requested documentation on June 6, 2008, and submitted additional documentation on July 23, 2008.

Once the additional documentation and necessary clarifications were received, an on-site meeting was held 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 Cancer Care Ontario was held on July 29, 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 Cancer Care Ontario

Cancer Care Ontario ("CCO") is an operational service agency of the Government of the Province of Ontario which provides strategic direction and leadership on all aspects of cancer prevention, detection and care including the implementation of cancer prevention and screening programs, the development and implementation of quality standards and the assessment and evaluation of the effectiveness, quality, accessibility and performance of the cancer system.

In addition, since the review of its practices and procedures in 2005, CCO now operates and manages the Wait Time Information System as part of the Ontario Wait Time Strategy. In this capacity, CCO is responsible for facilitating wait time management and for providing members of the public and other stakeholders with wait time information on all provincially funded adult and pediatric surgeries and certain diagnostic procedures such as MRI/CT scans.

Three-Year Review of Cancer Care Ontario

1. Privacy and Security Governance and Accountability Framework

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

The Chief Privacy Officer, who reports directly to the President and Chief Executive Officer, has been delegated day-to-day responsibility for managing the privacy program and for ensuring compliance with the *Act* and with the privacy policies, procedures and practices implemented. In managing the privacy program, the Chief Privacy Officer is supported by a Privacy Office that is responsible for providing advice and support to program areas; for developing, implementing and ensuring compliance with the privacy policies, procedures and practices implemented; for delivering privacy training; and for developing communications related to the privacy program.

The Chief Privacy Officer is also supported by a network of other individuals and committees with specific privacy-related responsibilities including the Wait Time Information Office Privacy Lead, who is responsible for implementing the privacy program in the Wait Time Information Office, and the Core Privacy Committee and Data Access Committee. The Core Privacy Committee is responsible for providing advice and consultation to the Chief Privacy Officer on discrete privacy issues such as corporate privacy initiatives and privacy breach management and the Data Access Committee is responsible for reviewing and approving requests for the disclosure of personal health information and for ensuring that the disclosure is consistent with the *Act* and with the privacy policies and procedures implemented by CCO.

In addition, the Chief Privacy Officer presents an *Annual Privacy Report* to the Board of Directors of CCO which addresses changes to, and the initiatives undertaken by, the privacy program in the previous fiscal year and the changes to, and the initiatives to be undertaken by, the privacy program in the upcoming fiscal year. A similar annual report, the *Wait Time Information Office Annual Privacy Report*, is also prepared and presented to the Board of Directors.

A Facilities Manager, who reports to the Chief Privacy Officer, has been delegated day-to-day responsibility for the physical security of personal health information at CCO. In addition, since the initial review of its practices and procedures in 2005, CCO now employs a Chief Technology Officer who has been delegated day-to-day responsibility for managing the technological security of personal health information at CCO. The Chief Technology Officer, who reports to the Chief Information Officer, is supported by two systems security specialists and by an Information Security Committee whose responsibilities include the review of security policies and procedures, information security incident response planning and the review of information security incidents.

2. Overview of Privacy and Security Policies and Procedures

CCO has developed a privacy policy, *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario* ("*Privacy Policy*"), which is applicable to CCO in its capacity as a prescribed entity pursuant to section 45 of the *Act* and to all programs and data holdings operated pursuant to its status as a prescribed entity, with the exception of the Wait Time Information System. With respect to the Wait Time Information System, CCO has developed a separate privacy policy, the *Wait Time Information Office Privacy Policy*.

Both privacy policies describe the status of CCO as a prescribed entity under the *Act* and the obligations that arise as a result of this status, the safeguards implemented to protect personal health information and the accountability framework for ensuring compliance with the *Act* and for ensuring adherence to the privacy and security policies and procedures implemented by CCO.

CCO has also implemented numerous privacy and security policies and procedures that support the *Privacy Policy* and *Wait Time Information Office Privacy Policy*, which are discussed in this report.

Privacy Breach Management Procedure

CCO has developed and implemented *Privacy Breach Management Procedures* that address the discovery, reporting, containment, notification, investigation and resolution of privacy breaches at CCO, including the Wait Time Information Office. A privacy breach is defined in the *Privacy Breach Management Procedures* as the use or disclosure of personal health information in contravention of the *Act*, the *Privacy Policy* or the *Wait Time Information Office Privacy Policy*. It is recommended that the definition of privacy breach be broadened to include the collection, use, disclosure, retention or disposal of personal health information, not simply the use or disclosure of personal health information, in violation of the *Act* and its regulation or in violation of any and all privacy policies and procedures implemented by CCO, not simply the *Privacy Policy* or *Wait Time Information Office Privacy Policy*.

Pursuant to the *Privacy Breach Management Procedures*, agents are responsible for immediately reporting a privacy breach or suspected privacy breach to the Privacy Office or Wait Time Information Office Privacy Lead, as the case may be, in person, by telephone or by email.

In the case of the *Privacy Breach Management Procedure* applicable to CCO generally, with the exception of the Wait Time Information Office, the report must include a description of the privacy breach or suspected privacy breach, the individuals involved and any immediate steps taken to contain the breach or suspected breach. The *Privacy Breach Management Procedure* applicable to the Wait Time Information Office, however, does not specify the information that must be reported. In addition, the procedures for containing and investigating a privacy breach are inconsistent as between the *Privacy Breach Management Procedure* applicable to the Wait Time Information Office and the *Privacy Breach Management Procedure* applicable to the remainder of CCO.

It is recommended that the procedures for reporting, containing and investigating privacy breaches be consistent as between the *Privacy Breach Management Procedure* used by the Wait Time Information Office and the *Privacy Breach Management Procedure* used by the remainder of CCO.

In addition, while the *Privacy Breach Management Procedures* state that the Chief Privacy Officer is responsible for notifying senior management and others where appropriate of a privacy breach; they do not specifically address notification of the health information custodian that provided the personal health information. It is recommended that the *Privacy Breach Management Procedures* be amended to require CCO to notify the health information custodian that provided the personal health information of a privacy breach, in order that the health information custodian may notify the individuals to whom the personal health information relates pursuant to subsection 12(2) of the *Act*.

Further, the *Privacy Breach Management Procedure* used by the Wait Time Information Office states that, where appropriate, the Wait Time Information Office will notify the individuals to whom the personal health information relates of a privacy breach. It is recommended that, as a secondary collector of personal health information, CCO notify the health information

custodian that provided the personal health information in the event of a breach as opposed to notifying individuals directly.

The Privacy Office or the Privacy Breach Management Team, in the case of the Wait Time Information System, is then required to investigate the privacy breach and to issue resolutions within five business days in order to prevent a similar privacy breach from recurring. The Privacy Office or Wait Time Information Office Privacy Lead, as the case may be, is then responsible for assigning individuals to implement the resolutions, for establishing timelines for implementation of the resolutions and for ensuring that the resolutions are implemented within the relevant timelines.

Security Policies and Procedures

CCO has developed and implemented security policies and procedures 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, server and workstation security, encryption, destruction of records of personal health information and information security incidents. The *Information Security Program at Cancer Care Ontario* states that these security policies and procedures will be reviewed on a biannual basis. However, the procedure for reviewing and amending the security policies and procedures is not articulated.

It is recommended that CCO develop and implement a policy and associated procedures for the review of its security policies and procedures that sets out the person(s) responsible for undertaking the review, the procedure to be followed in undertaking the review, and the procedure to be followed in amending the security policies and procedures. It is further recommended that the review have regard to technological advancements; to any orders, guidelines and best practices issued by the IPC; to any industry security best practices; and to any new or amendments to existing privacy legislation having security implications, including amendments to the *Act* and its regulation.

Information Security Incident Response Policy

CCO has developed an *Information Security Incident Response Policy* to govern the reporting, investigation and remediation of information security incidents, that is, events that compromise or potentially compromise the confidentiality, integrity or availability of information.

With respect to the reporting of information security incidents, it is unclear to whom an information security incident must be reported. One section of the *Information Security Incident Response Policy* states that information security incidents are to be reported to the Systems Security Specialist or the Chief Technology Officer. However, elsewhere, it states that information security incidents may be reported to one of twelve individuals at CCO including the Systems Security Specialist, Chief Technology Officer, Director of Information Technology, Information Technology Helpdesk, Information Technology Manager, Network Administrator or Application Administrator.

It is recommended that this inconsistency be addressed and that the list of persons to whom agents must report an information security incident be limited in scope in order to ensure that the information security incident is contained in an expedited manner. It is also recommended that the format for reporting the information security incident and the information that must be reported be articulated in the *Information Security Incident Response Policy*.

Upon being notified of an information security incident, the Systems Security Specialist must form an "Incident Response Team" which is then responsible for determining whether the information security incident is real or perceived, to assess its impact or potential impact, to determine the nature of the information or systems threatened and to implement appropriate measures to contain or minimize the impact. It is recommended that the *Information Security Incident Response Policy* also explicitly require the Incident Response Team to consider whether the information security incident involves the unauthorized collection, use, disclosure, retention or disposal of personal health information in violation of the *Act* and its regulation or in violation of any of the privacy policies and procedures implemented by CCO.

If the information security incident involves personal health information, the *Information Security Incident Response Policy* should address notification of the Privacy Office and the roles and responsibilities as between the Office of the Chief Technology Officer and the Privacy Office. In particular, the *Information Security Incident Response Policy* should articulate the procedures that apply when the event is both an information security incident and a privacy breach or suspected privacy breach and the procedures that apply when the event is reported as an information security incident but is determined to be a privacy breach or suspected privacy breach.

The *Information Security Incident Response Policy* also does not address, in circumstances where the information security incident involves personal health information, notification to the health information custodian that provided the personal health information in order that the health information custodian may notify the individuals to whom the personal health information relates pursuant to subsection 12(2) of the *Act*. It is recommended that the *Information Security Incident Response Policy* be amended to address such notification.

The Incident Response Team is then responsible for conducting an investigation and for making recommendations to prevent a recurrence of the information security incident. The *Information Security Incident Response Policy*, however, does not address who is responsible for assigning individuals to implement the recommendations, for establishing timelines for implementation and for ensuring that the recommendations are implemented in the requisite timelines. It is recommended that the *Information Security Incident Response Policy* be amended accordingly.

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

CCO makes information about its privacy and security policies, procedures and practices readily available on its website, **www.cancercare.on.ca**, including its *Privacy Policy*, the *Annual Privacy*

Report, *Privacy Frequently Asked Questions* 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. Executive summaries of privacy impact assessments on data holdings, programs and systems involving personal health information are also posted on the website.

Pursuant to a recommendation made by the IPC during the initial review of its practices and procedures in 2005, CCO also makes available a privacy brochure entitled *Protecting Your Privacy*, which sets out the types of personal health information collected, the uses made of the personal health information and the safeguards implemented to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. This brochure has been translated into French, Italian, Spanish, Portuguese and Chinese.

In addition, the Wait Time Information Office makes further information available about its privacy and security policies, procedures and practices on the website of CCO, as well as on the website of the Ontario Wait Time Strategy, **www.ontariowaittimes.com**. This includes the *Wait Time Information Office Privacy Policy*; a brochure entitled *Protecting Your Privacy*, which has also been translated into French, Italian, Spanish, Portuguese and Chinese, the *Wait Time Information Office Frequently Asked Privacy Questions* and the *Wait Time Information Office Annual Privacy Report*.

The privacy and security policies and procedures implemented by CCO are also made readily available to agents on a centralized intranet resource.

4. Collection, Use and Disclosure of Personal Health Information

Collection

CCO collects personal health information primarily from health information custodians directly involved in the delivery of health care, such as hospitals, laboratories, physicians and independent health facilities, as well as from the Ministry of Health and Long-Term Care. It also collects personal health information from other governmental organizations, from other prescribed entities within the meaning of section 45 of the *Act* and from prescribed persons that compile or maintain registries of personal health information pursuant to subsection 39(1)(c) of the *Act*.

The personal health information collected, with the exception of that collected for purposes of the Wait Time Information System, relates to cancer. This includes the name, date of birth, address and health card number of the individual; information about the cancer and related illnesses of the individual; and information about treatments and procedures provided. This personal health information is retained in a variety of registries, the largest of which is the Ontario Cancer Registry. For purposes of the Wait Time Information System, the personal health information collected relates to wait times for adult and pediatric surgeries and certain diagnostic procedures, including:

- Identifying information such as the name, address, date of birth, health card number and medical record number of the individual to whom the information relates;

- Health care provider and facility information such as the name of the health care provider, the health provider specialty, the health care provider number and facility type;
- Prioritization information; and
- Wait time information such as the surgery or procedure for which the individual is waiting, the date of the decision to treat, the original scheduled date for the surgery or procedure, the rescheduled date and the actual date of the surgery or procedure.

CCO consults with stakeholders prior to the collection of personal health information in order to define the personal health information necessary for the identified purposes of the data holding. Following this consultation, CCO documents the personal health information that will be collected in a *Statement of Purposes* and provides a justification for why the collection is necessary for the identified purposes. This *Statement of Purposes* is reviewed every three years to ensure that the personal health information continues to be required for the identified purposes of the data holding.

Use

CCO uses personal health information for purposes of analysis and compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the health system pursuant to section 45 of the *Act*. In particular, personal health information is used to:

- Plan, manage and report on the cancer system including the incidence of cancer and the relationship between gender, age and environmental or geographical factors and cancer;
- Evaluate the effects of early diagnosis and treatment;
- Study service delivery, utilization and wait times for radiation, chemotherapy and cancer surgery and estimate current and future needs for cancer services;
- Coordinate cancer services and develop practice guidelines;
- Support cancer screening programs, such as the Ontario Breast Screening Program; and
- Manage and operate the Wait Time Information System.

Disclosure

CCO 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 health information custodians that provided the personal health information, directly or indirectly, to CCO. Prior to any such disclosure, the *CCO Decision Criteria for Data Requests* requires that an analysis be conducted of whether the disclosure complies with subsection 18(5) of Regulation 329/04 to the *Act*, namely, to ensure

that the disclosure does not include additional identifying information. Further, the *Business Process for Data Requests* requires that any report prepared for the health information custodians be reviewed to ensure that no identifying information is disclosed, other than that originally provided.

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 and to prescribed persons that compile or maintain registries of personal health information pursuant to subsection 39(1)(c) of the *Act* for purposes of facilitating or improving the provision of health care.

In addition, personal health information is disclosed for research purposes pursuant to the *Data Use and Disclosure Policy* implemented by CCO. In responding to requests for the disclosure of personal health information for research purposes, CCO considers whether the request is consistent with the *Act*. In determining consistency with the *Act*, the *Data Use and Disclosure Policy* states that a researcher requesting personal health information for research purposes must submit a research plan, a copy of the decision of the research ethics board approving the research plan and a completed *Application for Disclosure of Information from Cancer Care Ontario for Research Purposes*, which addresses the requirements that must be satisfied prior to the disclosure of personal health information for research purposes pursuant to section 44 of the *Act* and its regulation. If the request is approved, researchers and those who may have access to personal health information for research purposes must also execute a *Non-Disclosure/Confidentiality Agreement* prior to any such disclosure for research purposes.

By signing the *Non-Disclosure/Confidentiality Agreement*, the researcher and all those who may have access to the personal health information agree, among other things, to only use the personal health information for the research purposes, to comply with the conditions specified by the research ethics board, to protect the personal health information from loss and unauthorized use and disclosure, to not contact or attempt to contact the individuals to whom the personal health information relates and to not disclose the personal health information except as required by law.

5. Retention and Destruction of Personal Health Information

CCO retains records of personal health information in electronic format permanently for long-term analysis and reporting and retains records of personal health information in paper format for as long as necessary to place the records into electronic format and for financial audit purposes. 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 Privacy Office is responsible for ensuring that there are appropriate resources available to support the secure destruction of records of personal health information in paper format.

Destruction of Records of Personal Health Information in Paper Format

The *Privacy Policy* states that records of personal health information that are no longer required must be securely destroyed by shredding. However, it is unclear from a review of the *Privacy Policy*, what type of shredding is employed. It is recommended that the *Privacy Policy* be amended to set out the type of shredding employed and that the shredding employed be consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC and with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to the *Act*.

Destruction of Records of Personal Health Information in Electronic Format

CCO has developed and implemented a *Media Destruction Policy and Procedure* that governs the secure destruction of personal health information in electronic format.

The *Media Destruction Policy and Procedure* requires that if electronic storage media is to be reused or returned to a leasing company, that all personal health information be securely erased with a wipe product using a minimum of seven passes. A completion report attesting to the fact that the electronic storage media was wiped and the date and time that it was wiped is then signed and retained for seven years for audit purposes. If electronic storage media is not to be reused or returned, the *Media Destruction Policy and Procedure* requires that it be physically destroyed. Physical destruction is defined to mean disintegration, incineration, pulverization, shredding or melting. Once destroyed, a certificate of destruction must be prepared by the third-party service provider and the certificate of destruction is held for seven years for audit purposes.

Agreement with Third-Party Service Providers

It is recommended that the agreements between CCO and the third-party service providers retained to securely destroy records of personal health information in paper and electronic format be amended to ensure consistency with Order HO-001, and with the provisions in *Fact Sheet 10: Secure Destruction of Personal Information*, issued by the IPC.

In particular, it is recommended that the agreements be amended to explicitly state that the third-party service providers shall destroy 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 the records of personal health information will be securely destroyed, including under what conditions and by whom.

It is also recommended that the agreements be amended to require the third-party service providers to provide a certificate of destruction signed by the person who performed the secure destruction and to set out the required content of the certificate of destruction. In particular, the certificate of destruction should set out the date, time, location and method of secure destruction employed. The agreements should also require the third-party service providers to agree that:

- Their services will be performed in a professional manner, in accordance with industry standards and practices and by properly trained employees and agents;

- Their 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 CCO 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 providers and that a copy of the written contract will be provided to CCO.

6. Administrative Safeguards Implemented

In addition to the privacy and security policies and procedures, CCO has implemented the following administrative safeguards to protect the privacy of individuals with respect to the personal health information received by CCO and to protect the confidentiality of that personal health information.

Privacy Training

CCO has developed and implemented a *Privacy Training and Awareness Procedure* for the Wait Time Information Office and a *Privacy Training and Awareness Procedure* for the remainder of CCO. The *Privacy Training and Awareness Procedures* require all new agents of CCO, including employees, staff, consultants and contractors, to attend privacy training.

With respect to new employees and staff, the *Privacy Training and Awareness Procedures* state that the privacy training must be provided within two weeks of their start date, in the case of the Wait Time Information Office, and within four weeks of their start date in all other circumstances. However, it is unclear from a review of the *Privacy Training and Awareness Procedures* whether this privacy training is provided prior to the employee or staff member having access to personal health information and when this privacy training is provided to consultants and contractors. The template *Consulting Agreement* appears to suggest that the privacy training must be provided to consultants prior to granting access to personal health information. It is recommended that the *Privacy Training and Awareness Procedures* be amended to make explicit that agents must receive privacy training prior to being given access to personal health information.

The privacy training provided to new agents of the Wait Time Information Office is entitled *Protecting Personal Health Information: Privacy Orientation for the WTIS Project* and the initial privacy training provided to new agents of the remainder of CCO is entitled *Cancer Care Ontario Privacy Orientation.* This privacy training explains the statutory authority pursuant to which CCO collects, uses and discloses personal health information, the privacy obligations imposed on agents, the consequences imposed for failing to fulfill the privacy obligations, the safeguards implemented to protect the confidentiality of personal health information and the responsibilities imposed on agents to identify, contain and report privacy breaches or suspected privacy breaches.

In addition, the *Privacy Training and Awareness Procedures* require employees and staff to attend privacy training on an annual basis. A similar requirement to attend annual privacy training does

not appear, based on the *Privacy Training and Awareness Procedures*, to be imposed on contractors and consultants. However, the documentation provided for purposes of this review appears to suggest that contractors also receive privacy training on an annual basis. It is recommended that the application of annual privacy training to contractors and consultants be clarified in the *Privacy Training and Awareness Procedures*.

Attendance by employees and staff at both the initial and annual privacy training is tracked using a *Privacy Acknowledgement* or *Wait Time Information Office Privacy Acknowledgement*, as the case may be. The *Privacy Training and Awareness Procedure* applicable to CCO generally, with the exception of the Wait Time Information Office, states that receipt of the *Privacy Acknowledgement* is recorded and reconciled against a list of new employees, in the case of the initial privacy training, and against a list of employees and staff that were required to be in attendance, in the case of the annual privacy training. No similar procedure exists in the *Privacy Training and Awareness Procedure* applicable to the Wait Time Information Office. It is recommended that CCO ensure consistency as between the *Privacy Training and Awareness Procedure* applicable to the Wait Time Information Office and that applicable to the remainder of CCO.

It is also unclear whether consultants and contractors are required to sign a *Privacy Acknowledgement* or *Wait Time Information Office Privacy Acknowledgement* upon the completion of privacy training, given that this is not addressed in the *Privacy Training and Awareness Procedures*. The template *Consulting Agreement*, however, appears to suggest that such a requirement is imposed on consultants and contractors. It is recommended that the *Privacy Training and Awareness Procedures* be amended to require consultants and contractors to sign a *Privacy Acknowledgement* or *Wait Time Information Office Privacy Acknowledgement* upon the completion of privacy training consistent with the actual practices of CCO.

The *Privacy Acknowledgement* and *Wait Time Information Office Privacy Acknowledgement* require the persons signing to acknowledge that personal health information will not be used or disclosed except as necessary to perform their duties, that they will comply with the *Privacy Policy*, the *Wait Time Information Office Privacy Policy* and all policies and procedures implemented that give effect thereto and that the failure to comply may result in the termination of the employment or contractual relationship with CCO as well as possible legal action. It is also recommended that the *Privacy Acknowledgement* and *Wait Time Information Office Privacy Acknowledgement* be amended to require immediate notification of the Privacy Office or the Wait Time Information Office Privacy Lead upon becoming aware of a breach or suspected breach of the *Privacy Acknowledgement* or *Wait Time Information Office Privacy Acknowledgement*.

The failure of employees and staff to attend privacy training or execute a *Privacy Acknowledgement* or *Wait Time Information Office Privacy Acknowledgement* may, pursuant to the terms of the *Privacy Training and Awareness Procedures*, result in the revocation of access rights. However, the consequences imposed on consultants and contractors for failing to attend privacy training and for failing to execute a *Privacy Acknowledgement* or *Wait Time Information Office Privacy Acknowledgement* are not addressed. It is recommended that this be addressed in the *Privacy Training and Awareness Procedures*.

Security Training

The *Privacy Training and Awareness Procedure* for the Wait Time Information Office and the *Privacy Training and Awareness Procedure* for the remainder of CCO states that the Systems Security Specialist is responsible for training all new employees and staff on the security policies and procedures implemented by CCO. The security training is formalized in a presentation entitled *Security Awareness*, and is aimed at raising awareness of the importance of systems security and the obligations imposed in order to protect the confidentiality of personal health information.

However, it is unclear from a review of the *Privacy Training and Awareness Procedures*, when this security training is provided, whether this security training is provided to consultants and contractors, whether attendance at this security training is mandatory, who is responsible for ensuring that security training has been attended, how attendance is tracked and the consequences for failing to attend. It is also unclear whether ongoing security training is provided, to whom it is provided, whether this ongoing security training is mandatory and the practices and procedures that apply to ongoing security training. At the on-site meeting on July 29, 2008, CCO advised that annual security training is provided.

It is recommended that CCO develop and implement a comprehensive security training policy that encompasses both initial security training for all new employees, staff, consultants and contractors, as well as ongoing security training. This policy should emphasize that attendance at security training is mandatory and the policy should set out when the initial security training will be provided, namely prior to being given access to personal health information, the frequency of the ongoing training, to whom the initial and ongoing security training will be provided and the person(s) responsible for delivering the security training. It should also describe the process that will be used to track attendance at both the initial and ongoing security training and to set out the person(s) responsible for tracking attendance and the consequences for failing to attend.

Further, although the *Privacy Training and Awareness Procedures* do not address whether an acknowledgement similar to the *Privacy Acknowledgement* or *Wait Time Information Office Privacy Acknowledgement* must be executed following security training, it appears that a *Security Acknowledgement Form* must be executed and returned to the Systems Security Specialist.

The *Security Acknowledgement Form* requires the persons signing to acknowledge that they must attend security training and that they have read and understood the *Security of Electronic Information Policy*, *Acceptable Use of CCO Systems Policy*, *Password Policy*, *Email Policy* and *Off-Premises Access and Wireless Network Policy*.

There is no requirement in the *Security Acknowledgement Form* for the persons signing to acknowledge that they have not only read and understood, but agree to comply, with the security policies implemented by CCO. Further, the *Security Acknowledgement Form* only appears to require the persons signing to read and understand the security policies enumerated in the *Security Acknowledgement Form*. The security policies listed in the *Security Acknowledgement Form*, however, are only a small subset of the security policies and procedures implemented by CCO.

It is recommended that the *Security Acknowledgement Form* be amended to require persons signing the *Security Acknowledgement Form* to not only read and understand, but to comply with, all the security policies and procedures implemented by CCO and not simply those enumerated in the *Security Acknowledgement Form*. It is also recommended that the *Security Acknowledgement Form* be amended to require that the Chief Technology Officer or Systems Security Specialist be notified in the event of a breach or suspected breach of the *Security Acknowledgement Form*.

Further, at the on-site meeting, CCO advised that the ongoing security training provided to agents has the same content as the initial security training. It is recommended that the ongoing security training include role-based training in order to ensure that agents understand how to apply the security policies, procedures and practices implemented in their day-to-day work and that the ongoing security training address any new security policies, procedures and practices implemented by CCO and significant amendments to existing security policies, procedures and practices. It is also recommended that in determining the content of ongoing security training, CCO have regard to recommendations made with respect to training contained in security reviews, vulnerability assessments and threat and risk assessments.

Confidentiality Agreements

Pursuant to the *Confidentiality Policy* and *Privacy Training and Awareness Procedures*, all agents of CCO must sign a *Statement of Confidentiality* upon the commencement of their employment or contractual relationship with CCO. It is unclear, however, who is responsible for ensuring that *Statements of Confidentiality* have been executed, how execution of the *Statement of Confidentiality* is tracked and the consequences for failing to execute the *Statement of Confidentiality*.

It is recommended that CCO formalize its practices and procedures with respect to the execution of the *Statement of Confidentiality*. In particular, it is recommended that the *Confidentiality Policy* or *Privacy Training and Awareness Procedure* be amended to make explicit that the *Statement of Confidentiality* must be executed upon the commencement of the relationship with CCO and prior to being given access to personal health information and to set out the process that will be used to track execution of the *Statement of Confidentiality*, including the person(s) responsible for tracking execution and the consequences for failing to execute the *Statement of Confidentiality*.

By signing the *Statement of Confidentiality*, agents acknowledge that they have read, understood and agree to comply with all the policies implemented by CCO and acknowledge that a breach of the *Statement of Confidentiality* may result in disciplinary action up to and including a termination of the relationship with CCO. They further agree not to use personal health information for any purpose other than that for which it was provided and agree not to disclose the personal health information except as authorized by CCO in writing. It is recommended, however, that the *Statement of Confidentiality* be amended to require agents to immediately notify the Privacy Office in the event of a breach or suspected breach of the *Statement of Confidentiality*.

It is also recommended that the provisions in the *Statement of Confidentiality* which require the return or destruction of records of personal health information upon the cessation of the

employment or contractual relationship with CCO, or upon request by CCO, be amended to state that either the personal health information must be returned in a secure manner and to set out the secure manner in which the personal health information must be returned, or to state that the personal health information must be destroyed in a secure manner and to provide a definition of secure destruction that is consistent with subsection 1(5.1) of Regulation 329/04 to the *Act*. The *Statement of Confidentiality* should also require the agent to provide written and signed confirmation that the personal health information was permanently destroyed in a secure manner and which sets out the date, time, location and method of secure destruction employed.

Consulting Agreement

All consultants providing services to CCO must execute a *Consulting Agreement* containing standard privacy terms and conditions. The *Consulting Agreement* requires the consultant to acknowledge that it is acting as the "agent" of CCO for purposes of any collection, use, disclosure, retention or disposition of personal health information. It further requires the consultant to agree to use personal health information in accordance with the *Act* and the privacy and security policies and procedures implemented by CCO, to agree not to disclose personal health information except with the prior written consent of CCO or where required by law and to immediately advise CCO of any unauthorized access to the personal health information by the consultant and its agents.

The obligation to immediately advise CCO of unauthorized access to personal health information by the consultant and its agents is too narrow in its scope. It does not require the consultant, for example, to notify CCO of any unauthorized disclosure of personal health information to third parties. The obligation is limited to unauthorized uses of personal health information by the consultant and its agents. It is recommended that the *Consulting Agreement* be amended to require the consultant to notify CCO of any breach or suspected breach of the standard privacy terms and conditions in the *Consulting Agreement* in order to prevent further theft, loss and unauthorized use and disclosure of the personal health information.

The *Consulting Agreement* also requires the consultant to securely destroy records of personal health information upon request or when it is no longer required to perform the consulting services and to provide a written statement attesting to destruction, upon the request of CCO. It is recommended that the *Consulting Agreement* be amended to impose a positive duty on the consultant to provide a written statement attesting to destruction each time personal health information is securely destroyed, as opposed to solely upon request, and that the *Consulting Agreement* describe the required content of the written statement attesting to destruction. In particular, it should set out the date, time, location and method of secure destruction employed and should bear the signature of the person who performed the secure destruction.

Privacy Audit Program

CCO has implemented a privacy audit program that requires three types of audits to be conducted on an annual basis: policy reviews, operational effectiveness reviews and physical

security reviews. The Privacy Office or Wait Time Information Office Privacy Lead, as the case may be, is responsible for conducting the audits and for summarizing the results in the *Annual Privacy Report* or *Wait Time Information Office Annual Privacy Report* presented to the Board of Directors.

The *Privacy Audit and Compliance Procedure* requires the Privacy Office to review the *Privacy Policy* implemented by CCO and its supporting procedures on an annual basis to ensure that they continue to reflect the requirements in the *Act* and privacy best practices. In the event that amendments are required, the amendments will be made by the Privacy Office and approved by the Chief Privacy Officer and the revised *Privacy Policy* or procedure will be distributed to agents along with an explanation of the amendments.

With respect to the Wait Time Information Office, the *Wait Time Information Office Privacy Compliance Procedure* requires the Wait Time Information Office Privacy Lead to review the *Wait Time Information Office Privacy Policy* and its supporting procedures on an annual basis to ensure they continue to reflect the requirements in the *Act* and privacy best practices. In the event that amendments are required, the amendments will be made by the Wait Time Information Office Privacy Lead and approved by the Chief Privacy Officer and Chief Information Officer and the revised *Wait Time Information Office Privacy Policy* or procedure will then be distributed to agents, along with an explanation of the relevant amendments.

Based on a review of the *Privacy Audit and Compliance Procedure* and the *Wait Time Information Office Privacy Compliance Procedure*, it appears that policy reviews are limited to a review of the *Privacy Policy* and the *Wait Time Information Office Privacy Policy* and their supporting procedures and do not include a review of all the other privacy policies implemented by CCO. It is recommended that the *Privacy Audit and Compliance Procedure* and the *Wait Time Information Office Privacy Compliance Procedure* be amended to expand the privacy audit program to review all privacy policies and procedures implemented by CCO on an annual basis.

CCO also requires that operational effectiveness reviews be conducted on an annual basis. Operational effectiveness reviews involve ensuring that "clean desk" practices are implemented, ensuring privacy breaches are promptly identified and managed, surveying agents to determine their compliance with privacy policies and procedures, monitoring the implementation of recommendations arising from privacy impact assessments and ensuring Data Stewards associated with each data holding are fulfilling their responsibilities.

CCO further requires that a physical security review be conducted on an annual basis, in conjunction with the Manager of Facilities, to assess the physical safeguards implemented and to ensure that the safeguards implemented are adequate, such as ensuring that printers and fax machines are located in secure areas, that shredding bins are available, that computer screens are locked when desks are left unattended and logging physical entry by visitors.

However, the *Privacy Audit and Compliance Procedure* and *Wait Time Information Office Privacy Compliance Procedure* do not set out the procedures and processes that are used in undertaking the operational effectiveness and physical security reviews. It is recommended that the *Privacy*

Audit and Compliance Procedure and the *Wait Time Information Office Privacy Compliance Procedure* be amended to document the procedures that are to be used in conducting these reviews.

Privacy Impact Assessments

The *Privacy Impact Assessment Policy* requires that privacy impact assessments be conducted on all new programs, data holdings or systems that involve personal health information and on all activities that involve the linkage of personal health information that will result in the creation of a permanent registry of personal health information. It further requires that privacy impact assessments be conducted on existing programs, data holdings and systems that are being re-engineered and involve changes in functionality, access or technology. CCO has advised that by the end of 2008, it will have completed privacy impact assessments on all existing programs, data holdings and systems involving personal health information for which no changes are proposed.

Limits and Audits of Access to Data Holdings Containing Personal Health Information

CCO has implemented a policy and procedures to limit access to data holdings containing personal health information. Pursuant to the *Data Use and Disclosure Policy* and *CCO Direct Data Access Procedures*, all agents requiring access to a data holding must complete and sign a *Direct Data Access Request Form* identifying the data holding to which they are requesting access, setting out the reason they require access, stating the type of access required and justifying why access is required. The *Direct Data Access Request Form* must also be signed by the supervisor of the agent, who is required to confirm that access is required.

The executed *Direct Data Access Request Form* is then sent to the Data Steward for the data holding who will determine whether to grant or deny access to the data holding. If approved, access will be valid until the date specified on the *Direct Data Access Request Form* to a maximum of twelve months. One month prior to expiry, a notice of pending access termination will be sent to the agent. To maintain access, the agent must re-apply for access to the data holding.

Audits of access to data holdings containing personal health information are conducted annually on a minimum of four data holdings in order to ensure that the *Data Use and Disclosure Policy* and its associated procedures are being followed, that agents with access to the data holding continue to have an employment or contractual relationship with CCO, that agents continue to have a current and valid business need for access and that access is given to the least amount of personal health information required to meet the business purpose. These audits are conducted by the Systems Security Specialist, with the exception of audits of access to the Wait Time Information System, which are conducted by the Wait Time Information Office Privacy Lead.

De-Identification

Further to a recommendation made during the initial review of its practices and procedures in 2005, CCO has developed and implemented *De-Identification Guidelines* to assist agents in

determining whether the information presented in reports or reporting tools developed by CCO is personal health information, and to provide guidance to agents in deciding when small cells may be disclosed or made available and to whom, without increasing the risk of re-identification.

Prior to disclosure, all data elements must be classified according to identifiability. "Immediately identifiable elements" are data elements that pose a high risk of identification and are defined to include name, date of birth, address and health card number. "Potentially identifiable elements," which pose a moderate risk of identification, are defined as data elements that may be combined with other similar elements or with data that is generally available to re-identify an individual, such as admission dates. "Non-identifiable elements," which pose a low risk of identification, are defined as data elements that cannot, in and of themselves or in combination with other information, be used to re-identify an individual without special knowledge or special access.

Finally, a determination is made of the risk level for the report or data set as a whole using a decision grid contained in the *De-Identification Guidelines*. Based on this determination, if the risk level for the report or data set is high, the report will be treated as personal health information. If the risk level is moderate, the *De-Identification Guidelines* state that consideration must be given to treating the report or data set as personal health information. If the risk level is low, the information will not be treated as personal health information.

Where the risk level is moderate, it is unclear on the basis of what criteria agents will make the decision as to whether or not to treat the report or data set as personal health information and with whom agents must consult in making such a determination. It is also unclear what procedures are in place in order to ensure consistency in the decision-making as to whether or not to treat a report or data set as personal health information when the risk level is moderate.

The *De-Identification Guidelines* also do not address, in circumstances where the risk level for a report or data set is moderate and a decision is made not to treat the report or data set as personal health information, the safeguards that must be implemented to ensure that persons or organizations to whom the report or data set is disclosed will not use the information, either alone or in combination with other information, to identify the individual to whom the information relates or to contact or attempt to contact the individual. The *De-Identification Guidelines* merely state that agents must ensure administrative controls are in place but do not identify the administrative controls that should be implemented.

It is recommended that the criteria for making the determination as to whether or not to treat the report or data set as personal health information, in circumstances where the risk of identification is moderate, be outlined in the *De-Identification Guidelines*, including identifying the person(s) with whom agents must consult in making this determination. Further, the *De-Identification Guidelines* should address the safeguards that must be implemented where the risk level is moderate and a decision has been made not to treat the report or data set as personal health information.

It is also recommended that the *De-Identification Guidelines* be amended to require agents to ensure that personal health information is not disclosed if other information, such as de-

identified information or aggregate information, will serve the purpose of the disclosure and to ensure that no more personal health information is disclosed than is reasonably necessary to meet the purpose.

The *De-Identification Guidelines* further state that staff are "encouraged" to identify "incidental or accidental" disclosures to the Privacy Office to ensure that such disclosure is minimized. A mandatory obligation should be imposed on staff to report privacy breaches or suspected privacy breaches to the Privacy Office in accordance with the *Privacy Breach Management Procedure* implemented by CCO as opposed to a discretion to report a limited subset of privacy breaches or suspected privacy breaches, namely those related to "incidental" or "accidental" disclosures.

Further, CCO has advised that in order to ensure that agents use the least identifiable information possible, that information provided to programs and projects is stripped of identifying fields, is aggregated or small cell suppression is used. In addition, CCO has constructed an information infrastructure known as the Enterprise Data Warehouse to which all data holdings, including the Ontario Cancer Registry, will be migrated. The Enterprise Data Warehouse is split between a database layer, which is accessible to only those agents who require access to personal health information to build, test and maintain the Enterprise Data Warehouse, and a presentation layer, which limits access to personal health information based on approved access levels.

Policies Related to the Transmission of Personal Health Information

CCO has implemented guidelines governing the use of facsimile transmission, which are documented in the *Guideline on Fax Transmission*, and has implemented policies prohibiting the use of e-mail to transfer personal health information, documented in the *Electronic Mail Policy*.

The *Guideline on Fax Transmission*, given that it is a guideline as opposed to a policy or procedure, does not clearly articulate the expectations of CCO relating to the acceptable use of facsimile transmission as it relates to personal health information and the standard operating procedures and safeguards that apply to sending or receiving personal health information by facsimile transmission.

It is recommended that CCO develop and implement a policy in which the acceptable methods of transferring personal health information are articulated and all other methods of transferring personal health information are prohibited. It is further recommended that CCO implement standard operating procedures to set out the safeguards that must be employed to ensure that personal health information transferred through one of the acceptable methods is being transferred in a secure manner and to ensure that the acceptable methods of transferring personal health information and the safeguards employed are consistent with Order HO-004, *Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices* and the *Guidelines on Facsimile Transmission Security* issued by the IPC.

7. Physical Safeguards Implemented

CCO is located in premises with internal video monitoring and tracked card access that divides the premises into varying levels of security with each successive level being more secure and restricted to fewer individuals. In order to access the server room, individuals must successfully pass through multiple levels of security. CCO has also implemented *Visitor Access Procedures* that require all visitors to sign in at reception noting their name, the date and time of their arrival and the name of the person being visited. Identification cards are issued to all visitors and must be worn at all times while on the premises. Visitors must return the identification card and sign out at reception upon departure and must record the time of departure.

8. Technical Safeguards Implemented

CCO has implemented a number of technical safeguards to protect personal health information against theft, loss and unauthorized use, disclosure, copying, modification and disposal. The technical safeguards implemented include the use of firewalls, two-factor authentication and the implementation of a *Password Policy* in accordance with industry standards. The safeguards also include a mandatory, standardized and system-wide password-protected screen saver for all desktop and laptop computers after a timeout period of twenty minutes, the installation of anti-virus software on all servers and workstations connected to the CCO network and the encryption of all desktop and laptop computers as well as USB memory keys.

CCO also requires, pursuant to the *Systems Risk Assessment Policy*, that threat and risk assessments be carried out on all new or significantly revised information systems. Since the review of its practices and procedures in 2005, threat and risk assessments have been completed for the Wait Time Information System, the Provincial Palliative Care Integration Project, the Computerized Physician Order Entry database, the Stage Capture Project, the Registered Nurse Performed Flexible Sigmoidoscopy Project of Colorectal Cancer Screening and the Annotated Tumour Project.

In addition, biannual general systems security reviews are conducted. In March of 2005, an assessment of system security measures was completed by Ainsworth/White Hat and a similar security posture assessment was completed by Deloitte Consulting in May 2008. In addition, a vulnerability assessment was completed by Cygnos IT Security in March 2007.

During the initial review of its practices and procedures in 2005, the IPC recommended that CCO implement a system for routinely checking system audit trails.

To date, CCO has implemented procedures to limit access by agents to data holdings containing personal health information and procedures to audit whether agents with access to data holdings continue to have an employment or contractual relationship with CCO, continue to have a current and valid business need for access and that access is given to the least amount of personal health information required to meet the business purpose.

In addition, audit trails are currently retained within systems that support CCO data holdings where technically supported. CCO has advised that its practice is to provide for audit capability in all newly built or acquired systems that will contain personal health information. This capability, for example, has been provided in the Wait Time Information System and iPort.™ These audit logs are then used for investigation purposes pursuant to the *Information Security Incident Response Policy* and *Privacy Breach Management Procedures*. CCO does not currently review system audit trails on a frequent basis in order to detect unauthorized access to data holdings containing personal health information and in order to detect information security incidents.

In response to the recommendation made by the IPC during the initial review of its practices and procedures, CCO has undertaken to implement a policy and associated procedures for the frequent review of system audit trails, consistent with industry standards, in order to detect unauthorized access to data holdings containing personal health information and in order to detect information security incidents in a timely manner. CCO has further undertaken to commence this review of system audit trails in 2009 and to submit a proposal to the IPC for review and comment in the first quarter of 2009 to outline its proposed strategy for implementation.

It is recommended that CCO develop and implement a comprehensive policy and associated procedures for the frequent review of system audit trails, consistent with industry standards and commensurate with the amount and sensitivity of the personal health information collected, with the number and nature of individuals with access to personal health information and with the threats and risks associated with the personal health information. It is further recommended that a proposal be submitted to the IPC for comment outlining the strategy for the implementation of such reviews prior to April 30, 2009.

Summary of Recommendations

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

1. In respect of its policies to document, contain, investigate, remediate and provide notification in respect of privacy breaches and information security incidents:

    (a) Amend the *Privacy Breach Management Procedures* to expand the definition of "privacy breach," to identify what information with respect to an information breach must be reported, to require notification to the health information custodian that provided the personal health information in the event of a privacy breach and to ensure consistency between the *Privacy Breach Management Procedure* applicable to the Wait Time Information Office and the *Privacy Breach Management Procedure* applicable to the remainder of CCO; and

    (b) Amend the *Information Security Incident Response Policy* to clarify the reporting obligations with respect to an information security incident; to address the interplay between an information security incident and a privacy breach; to require

notification to the health information custodian that provided the personal health information when the information security incident involves personal health information and to address responsibility for assigning individuals to implement the recommendations arising from an investigation, for establishing timelines for the implementation of recommendations and for ensuring that recommendations are implemented.

2. Develop and implement a written policy and associated procedures for the review of security policies and procedures and for the secure transfer of personal health information.

3. Refine its policies, procedures and practices relating to the secure destruction of records of personal health information in both paper and electronic format, by:

   (a) Amending the *Privacy Policy* to set out the type of shredding employed for records of personal health information in paper format and ensuring the shredding employed is consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC and with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to the *Act*; and

   (b) Amending the agreement with the third-party service providers 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.

4. Refine its policies and procedures in respect to privacy and security training by:

   (a) Amending the *Privacy Training and Awareness Procedures* pursuant to the comments provided in this report in order to clarify the actual practices of CCO;

   (b) Amending the *Privacy Acknowledgement* and *Wait Time Information Office Privacy Acknowledgement* to require agents to immediately notify the Privacy Office or Wait Time Information Office Privacy Lead in the event of a breach or suspected breach;

   (c) Developing and implementing a comprehensive security training policy that encompasses both initial security training as well as ongoing security training;

   (d) Amending the *Security Acknowledgement Form* to require agents to read, understand and comply with the security policies and procedures implemented by CCO; and

   (e) Ensuring that the ongoing security training includes role-based training and addresses new security policies, procedures and practices implemented by CCO and significant amendments to existing security policies, procedures and practices.

5. Formalize the practices and procedures implemented by CCO in relation to the execution of the *Statement of Confidentiality* and amend the *Statement of Confidentiality* and *Consulting Agreement* pursuant to the comments provided in this report, including to require agents to immediately notify the Privacy Office upon becoming aware of a breach of the *Statement of Confidentiality* or the privacy terms and conditions of the *Consulting Agreement*.

6. Amend the *Privacy Audit and Compliance Procedure* and the *Wait Time Information Office Privacy Compliance Procedure* to expand the policy reviews to include a review of all privacy policies and procedures implemented by CCO and to set out the procedures that are used in undertaking operational effectiveness and physical security reviews.

7. Amend the *De-Identification Guidelines* in accordance with the comments provided in this report, including as it relates to formalizing the procedures and criteria used when the risk level associated with a report or data set is moderate and a decision is required as to whether or not to treat the report or data set as personal health information.

8. Develop and implement a comprehensive policy and associated procedures for the frequent review of system audit trails consistent with industry standards and commensurate with the amount and sensitivity of the personal health information collected, the number and nature of individuals who have access to personal health information and the threats and risks associated with the personal health information, in order to detect unauthorized access to data holdings containing personal health information and to detect information security incidents in a timely manner. It is further recommended that CCO submit a proposal to the IPC for review and comment prior to April 30, 2009, outlining its proposed strategy for the implementation of frequent review of system audit trails.

Statement of Continued Approval of Practices and Procedures

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

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

2. Amend agreements with consultants and contractors 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 Agreement with Sunnybrook and Women's College Health Sciences Centre to reflect the requirements of the *Act* with respect to capacity and substitute decision making.

4. Complete the Privacy Brochure and make it available wherever cancer treatment is provided.

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 so that physical linking is carried out in a manner that ensures a minimum number of individuals have access to personal health information and identifiers are stripped or encrypted in subsets of data holdings used for project-specific analyses.

10. Amend the CCO Data Access Process for Personal Health Information and the access request forms to reflect the requirements of the *Act* 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 threat and risk assessments on a periodic basis.

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