

2009 ANNUAL PRIVACY REPORT

**CCO Privacy & Access Office
January 22, 2010**



Table of Contents

GLOSSARY	3
Introduction	4
Purpose of the Report.....	5
Achievements for 2009.....	6
People, Process and Technology	8
I.People	8
Privacy Governance at CCO	8
CCO Privacy Office	9
Privacy Support Network.....	9
II.Process.....	10
Privacy Policy Framework	10
Privacy Assessments	10
Training and Awareness.....	12
Communications	13
Breach Management	13
Data Requests	15
Patient Recruitment for Cancer Research	17
III.Technology	17
Enterprise Information Security Office	17
PHI Access Monitoring and Auditing Project.....	19
Year in Review - Privacy Updates for CCO Programs	21
1.Ontario Health Study (OHS).....	21
2.Ontario Renal Network (ORN)	21
3.Interactive Symptom Assessment and Collection (ISAAC).....	21
4.Ontario Breast Screening Program (OBSP)	22
5.RN Performed Flexible Sigmoidoscopy (FSIG) Pilot Project	22
6.ColonCancerCheck (CCC).....	22
7.Aboriginal Data Indicators Pilot	23
8.Cancer Stage (CS) Project.....	23
9.Access to Care (ATC)	23
CONCLUSION.....	26
New Legislative Requirements	27
Freedom of Information and Protection of Privacy Act.....	27
Goals for 2010.....	29

GLOSSARY

CCAC.....	Community Care Access Centre
CCC.....	ColonCancerCheck
CCO.....	Cancer Care Ontario
CIHI	Canadian Institute of Health Information
CIO	Chief Information Officer
CIRT	Colonoscopy Interim Reporting Tool
CKD.....	Chronic Kidney Disease
CPO.....	Chief Privacy Officer
CPRO	Client Profile Database
CS.....	Cancer Stage
CT.....	Computed Tomography
CTO.....	Chief Technology Office
DSA	Data Sharing Agreement
EDRS.....	Emergency Department Reporting System
EDW	Enterprise Data Warehouse
EISO.....	Enterprise Information Security Office
ER/ALC.....	Alternate Level of Care
ESAS	Edmonton Symptom Assessment System
FIPPA	Freedom of Information and Protection of Privacy Act
HINP	Health Information Network Provider
IM/IT	Information Management/ Information Technology
IPC.....	Office of the Information and Privacy Commissioner (Ontario)
ISAAC.....	Interactive Symptom Assessment and Collection
LHIN	Local Health Integration Network
MOHLTC.....	Ministry of Health and Long-Term Care
NACRS	National Ambulatory Care Reporting System
OBSP.....	Ontario Breast Screening Program
OHS.....	Ontario Health Study
ORN.....	Ontario Renal Network
PHI.....	Personal Health Information
PHIPA.....	Personal Health Information Protection Act
PIA.....	Privacy Impact Assessment
PPAF	Preliminary Privacy Assessment Tool
PPCIP	Provincial Palliative Care Integration Project
PRM.....	Provincial Reference Model
RM&R	Resource Matching & Referral
SETP	Surgical Efficiency Targets Program
TRA	Threat and Risk assessment
WTIO	Wait Time Information Organization
WTIP.....	Wait Time Information Program

Introduction

Cancer Care Ontario (CCO) is the provincial agency responsible for continually improving cancer services. Formally launched and funded by the Ontario government in 1997, CCO is governed by the *Cancer Act*.

As the government's cancer advisor, CCO:

- Directs and oversees close to 700 million public healthcare dollars to hospitals and other cancer care providers to deliver high quality, timely cancer services;
- Implements provincial cancer prevention and screening programs designed to reduce cancer risks and raise screening participation rates;
- Works with cancer care professionals and organizations to develop and implement quality improvements and standards;
- Uses electronic information and technology to support health professionals and patient self-care and to continually improve the safety, quality, efficiency, accessibility and accountability of cancer services;
- Plans cancer services to meet current and future patient needs, and works with healthcare providers in every Local Health Integration Network (LHIN) to continually improve cancer care for the people they serve; and
- Rapidly transfers new research into improvements and innovations in clinical practice and cancer service delivery.

As an operational service agency of the Ontario government, CCO is accountable to the Minister of Health and Long-Term Care (MOHLTC).

In order to fulfill its mandate, CCO requires access to personal health information (PHI) from across Ontario. CCO derives its authority to collect, use, and disclose this information from its designations under Ontario's *Personal Health Information Protection Act, 2004* (PHIPA).

CCO is designated as a "prescribed entity" under PHIPA and the large majority of CCO's programs operate under this statutory privacy authority. As a prescribed entity, CCO is authorized to collect, use, and disclose PHI for the purpose of *health system planning and management*. In this capacity, CCO collects PHI from health care organizations that are directly involved in the care and treatment of patients, and from government institutions and agencies, such as the MOHLTC or the Canadian Institute for Health Information (CIHI).

CCO is also designated as a “prescribed registry” under PHIPA with respect to CCO’s role in compiling and maintaining the Colorectal Cancer Screening Registry as part of Ontario’s colorectal cancer screening program – ColonCancerCheck (CCC). This designation grants CCO the authority to collect, use, and disclose PHI for purposes of *facilitating or improving the provision of colorectal cancer care*.

Finally, CCO also provides the Interactive Symptom Assessment and Collection (“ISAAC”) tool to health care providers at cancer hospitals to enable them to access and electronically share palliative care information about their patients. CCO operates as a “health information network provider” under PHIPA while providing this tool and must comply with specific privacy requirements set out in the PHIPA Regulation with respect to this role.

Purpose of the Report

This is CCO’s fourth Annual Privacy Report. The purpose of this report is to describe the CCO Privacy Program and highlight the privacy milestones for 2009. The Annual Privacy Report concludes with a summary of the privacy goals for 2010.

Achievements for 2009

CCO's Privacy Office is committed to meeting the high level of privacy protection that allows CCO to meet its goals of improving quality, accountability and innovation in all cancer-related services in Ontario. In 2009, the Privacy Office focused on achieving the following five goals.

- (1) The Privacy Office was restructured in 2009 to improve its efficiency and effectiveness in providing privacy advice and guidance to CCO departments and programs. The Privacy Office is comprised of a Director, Privacy, three Senior Privacy Specialists and a Privacy Analyst.

As part of the Privacy Office's activities to streamline CCO's Privacy Programs, the WTIO Privacy Policy has been integrated into the CCO Privacy Policy. The next stage of the CCO - WTIO Privacy Program integration will include a review of the WTIS procedures to ensure that the essence of the WTIS procedures are captured appropriately within the corresponding CCO procedures.

- (2) The Privacy Office has worked closely with the CCO Project Management Office to ensure that project managers can identify the key stages within a project where privacy consultation is required or when a privacy deliverable, such as a Privacy Impact Assessment (PIA), must be completed. The Privacy Office will continue to enhance the privacy gating process to ensure that it is effectively operationalized into CCO's project management life cycle.

- (3) The privacy infrastructure has been strengthened to allow easier access to privacy services by new and existing CCO programs and projects through:

- the development and enhancement of privacy access controls to PHI;
- a single point of contact for work intake (Director, Privacy), to allow for more efficiency and less duplication of efforts over similar projects;
- the assignment of a dedicated Privacy Specialist to each program area to become a privacy subject matter expert for the business unit; and
- the standardization and application of Preliminary Privacy Impact Assessments that provide project managers with initial insight into privacy impacts.

- (4) In collaboration with the CCO Enterprise Information Security Office (EISO), the Privacy Office launched the *PHI Access Monitoring and Auditing* project in 2009 in response to the IPC's recommendation arising from its 2008 review of CCO's information practices and procedures. In early 2010, a new log management solution shall be piloted for one of CCO's system applications. Based on the lessons learned from this pilot, the log management solution will be rolled out to a minimum of 5 other CCO systems applications in 2010. These 5 applications will be chosen based on a risk rating that considers the amount of PHI retained in the system, the level of sensitivity of the information as well as the number of authorized internal and external users.

- (5) The PHIPA Regulation (O. Reg. 329/04) was amended in 2009, permitting CCO to disclose PHI for out-of-province patients to CCO's counterpart organizations in other provinces for the purpose of health planning or health administration. CCO may now disclose PHI if:
- the disclosure is for the purpose of health planning or health administration;
 - the information relates to health care provided in Ontario to a person who is a resident of another province or territory; and
 - the disclosure is made to a body responsible for the provision, planning, analysis or payment of cancer services in that province or territory.

People, Process and Technology

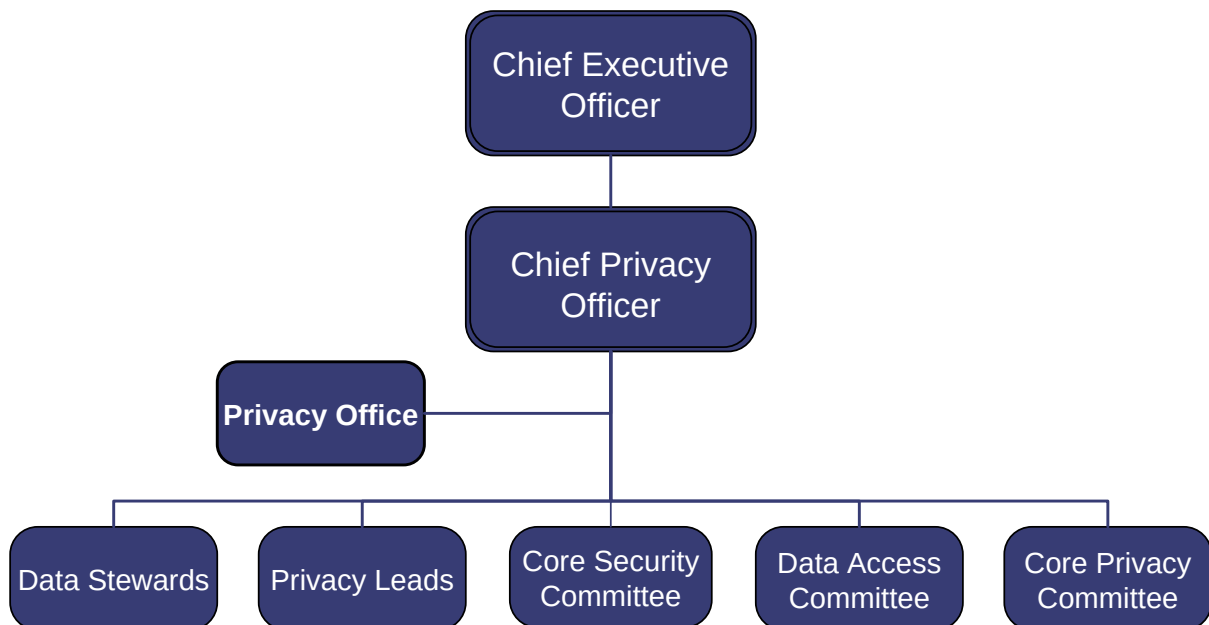
The CCO Privacy Program is comprised of 3 main components: People, Process and Technology. By focusing on these three business components, the CCO Privacy Program can proactively embed privacy controls into the areas which may present the highest level of privacy related risk to the organization.

I. People

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of PHI that it maintains. CCO meets these commitments through its Privacy Program. The CCO Privacy Program is designed to build a culture of privacy which strives to educate personnel and representatives of the organization on their individual responsibilities for safeguarding PHI.

Privacy Governance at CCO

The CCO Privacy Program is overseen by the Chief Privacy Officer (CPO), who reports directly to CCO's President and Chief Executive Officer. The Privacy Office supports the CPO in carrying out her responsibilities, as does a network of individuals and committees with specific privacy and security related responsibilities.



CCO Privacy Office

The Privacy Office is comprised of the Director, Privacy, three Senior Privacy Specialists and a Privacy Analyst. The Director, Privacy is responsible for the day-to-day operation of privacy processes within CCO and compliance with CCO privacy policies.

The Senior Privacy Specialists are responsible for providing advice and support to program areas by ensuring that CCO's privacy policies, procedures and practices are incorporated into the design of CCO programs and systems. This is achieved by conducting privacy assessments, delivering privacy training and developing communication materials related to the Privacy Program.

A Privacy Analyst also supports the privacy objectives of the Privacy Office and is responsible for tracking the status of privacy risk mitigation activities and the analysis of privacy metrics used to assess the effectiveness of the Privacy Program.

Privacy Support Network

Data Stewards are assigned to each data holding and are responsible for managing both internal and external requests for access to CCO data. Data Stewards are well versed in the purpose(s) of the data holding that they are responsible for and are able to communicate these to the Information Management Coordinator and other stakeholders.

Program Area Privacy Leads are responsible for ensuring that the CCO Privacy Program is implemented in their respective programs. Privacy Leads are well versed in *PHIPA*, CCO's Privacy Policy and all policies and practices that give effect to this policy, as they relate to their role.

The Privacy Office also relies on committees to assist with the management of the Privacy Program. The Core Security Committee is comprised of IT managers, Systems Security Specialists and the Director, Privacy. This Committee supports CCO's mission by evaluating information security vulnerabilities and implementing systems security standards, procedures and guidelines to ensure that CCO Systems are appropriately secured. The Core Security Committee's main objective is to continuously improve CCO's Information Security posture.

The Core Privacy Committee is comprised of the CPO, Privacy Office staff, IT Security and key members of CCO's information management team which provides advice and consultation to the CPO on specific privacy topics. The Core Privacy Committee's key responsibilities include consultation and advice related to preparation for the IPC triennial review of CCO's information management practices, the implementation of recommendations arising from the reviews and enterprise wide privacy initiatives.

The Data Access Committee is co-chaired by the CPO and the Director, Cancer Informatics, and is ultimately responsible for reviewing and approving requests for access to CCO data. The Data Access Committee reviews all data requests, including research-related requests, related to the disclosure of PHI and ensuring that the requests are consistent with *PHIPA* and CCO's Data Use & Disclosure Policy.

II. Process

CCO's *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario* (CCO Privacy Policy) is based on the 10 privacy principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*. It guides CCO on the collection, use, disclosure and protection of PHI in its custody and control.

Each principle as outlined in the CCO Privacy Policy is operationalized through specific procedures and guidelines that inform program areas of their responsibilities and obligations when working with PHI.

Privacy Policy Framework

As a part of its annual due diligence in 2009, the Privacy Office reviewed its policies and procedures and minor amendments were made to the following documents to reflect new processes:

- CCC Breach Management Procedure;
- CCC Access Control Procedure; and
- CCO Privacy Training and Awareness Procedure.

Additionally, an assessment of the existing policy structure was conducted with the aim of aligning its governing documents to a CCO enterprise wide policy framework. The new proposed policy framework will follow a tiered approach with enterprise Policies at the top, followed by mandatory conformance Standards and then unique program area Procedures. Each subordinate policy governance tier draws its authority from the higher tiers, by providing more deployment details but not establishing conceptually new principles, requirements or responsibilities. An investigation into this new policy platform will be a part of the 2010 privacy program goals. The Privacy Office will need to ensure that the new policy framework does not negatively impact the existing program.

Privacy Assessments

In 2009, the Privacy Office used the following three tools to conduct privacy assessments where CCO programs were informed of possible privacy risks and mitigating strategies as required.

1. Preliminary Privacy Assessment Form

The Privacy Office has introduced a Preliminary Privacy Assessment Form (PPAF) that all project and program managers are required to complete when requesting a privacy assessment. The completed PPAF assists the Privacy Office in determining whether the proposed initiative involves the collection, use and/or disclosure of PHI, in addition to determining if a PIA is required.

2. **Privacy Impact Assessments (PIAs)**

A PIA is a process that allows CCO to assess a program or information system's privacy risks, in addition to ensuring compliance with PHIPA and CCO's Privacy Policy. In accordance with CCO's PIA Policy, a PIA will be conducted when material changes are made to an existing program or when a new program or system, that will collect PHI, is developed. Where required, a PIA also details mitigating strategies and an action plan. A critical step in the PIA process is the implementation of the recommendations detailed in the assessment.

3. **PIA Addendum**

An addendum to a PIA is conducted to assess changes to existing projects or programs for which a PIA has already been conducted, but where the proposed changes are found to be minor.

In 2009, CCO conducted the following privacy assessments:

Assessments	Date Completed
Computerized Physician Order Entry Oncology Patient Information System – Addendum to 2007 PIA	April 2009
Surgical Efficiency Targets Program (SETP) - Addendum to 2007 SETP PIA	May 2009
Colonoscopy Interim Reporting Tool (CIRT) - Addendum to 2007 CIRT PIA	June 2009
ColonCancerCheck - Addendum to 2008 ColonCancerCheck PIA	June 2009
Ontario Wait Time Information System (WTIS) – Alternative Level of Care (ALC) – Interim Tool PPAF	July 2009
Client Profile Database PPAF	September 2009
Ontario Wait Time Information System (WTIS) – Alternative Level of Care (ALC) – Addendum to 2008 WTIS PIA	November 2009
Emergency Room National Ambulatory Reporting System Initiative (ERNI)	November 2009
Interactive Symptom Assessment and Collection (ISAAC) - Addendum to the 2007 Provincial Palliative Care Integration Project (PPCIP) PIA	November 2009
Aboriginal Data Indicators Pilot – PPAF	November 2009
Enterprise Data Warehouse (EDW) - Addendum to January 2008 EDW PIA	November 2009

Assessments	Date Completed
Cancer Stage Project • Cancer Stage Automation – PPAF • Cancer Stage ePath – PPAF	November 2009 December 2009

Training and Awareness

In 2009, 234 new employees received CCO privacy training, 67 of these employees received CCC specific privacy training and 71 received WTIS specific privacy training.

Additionally, as part of a collaborative effort, the CCO Privacy Office and the CCO Enterprise Information Security Office developed the first Privacy and Security web-based training program under CCO's new eLearning initiative, which launched in November 2009. The Privacy and Security eLearning curriculum is a key component of an overall strategy to effectively manage the delivery of training at CCO.

This new Privacy and Security training curriculum fulfills the annual privacy and security refresher requirement which is mandatory for all staff to complete. 650 employees and representatives fulfilled their 2009 annual privacy and security refresher requirement through the use of the new eLearning program.

The eLearning program will also serve to fulfill the new employee's privacy and security orientation training requirement which was offered at the monthly New Employee Human Resources Orientation sessions. This training is mandatory for all new employees, service providers and other representatives such as consultants, students, volunteers and researchers who work at CCO. The following courses are included in the Privacy and Security eLearning curriculum:

- Privacy;
- Information Security;
- A Privacy and Security Acknowledgement; and
- Privacy FAQs.

The privacy and security training course at CCO outlines:

- CCO's status under PHIPA and the responsibilities and privileges this entails;
- The importance of privacy to CCO's operations;
- The accountability of all staff to practice privacy-sensitive work habits;
- The information security best practices for protecting CCO systems and data to which staff have access;
- CCO's Information Security and Privacy policies, standards and procedures; and
- The roles of both the CCO Privacy Office and the Enterprise Information Security Office.

Users are required to read and digitally accept a Privacy and Security Acknowledgement Form upon completion of their training.

Additionally, for those persons who work in the ColonCancerCheck (CCC) program, a separate CCC privacy training curriculum is also available. The following courses are included in the CCC Privacy eLearning curriculum:

- ColonCancerCheck Privacy; and
- ColonCancerCheck Privacy Acknowledgement.

In 2010, a new WTIS module will be added to the eLearning Privacy Curriculum for those employees who support the provincial Wait Times initiative.

Communications

The Privacy Office is committed to effective communications with both internal and external stakeholders as part of building a culture of privacy. In 2009, CCO's internal privacy communications focused on building an extensive communication plan to deliver key privacy messages to all CCO staff through a variety of mediums.

1. The Privacy Office used posters to raise visibility and awareness on the compliance services it provides to CCO employees and programs. These posters were also used to promote the launch of the eLearning Privacy and Security training initiative for the annual refresher.
2. A quarterly newsletter providing updates from the Privacy Office was distributed to Data Stewards and Privacy Leads and posted on the Privacy page of CCO's intranet, where all CCO staff may review it. The 2009 newsletters included information on staffing changes, new programs, corporate initiatives and policy & procedure updates.
3. Additionally, programs such as the CCC enhanced its WebEx site, where internal CCC staff and external stakeholders, such as health care providers, receive updates on the screening program. This site is also used as a forum for communications between the various parties. The WebEx site includes a privacy section which provides privacy related information to stakeholders in a Frequently Asked Questions (FAQs) format, such as the statutory authority for CCC to collect PHI, the collection of information from Health Information Custodians without an individual's consent, and the privacy safeguards implemented in the program.
4. In November of 2009, CCO participated in the Annual PHIPA Summit by speaking on the following topics, the "Steps to Becoming a Prescribed Health Registry" and "Achieving Reasonable Security through a Security Health Check". This opportunity allowed CCO to share our own experiences with PHIPA and health information management with other leaders in the health sector.

Breach Management

Breach management at CCO begins with training all employees and representatives to be aware and knowledgeable on what constitutes a privacy breach and each employee's individual responsibility for reporting the breach to the Privacy Office. CCO classifies a privacy breach as the misuse or unauthorized collection, use and disclosure of PHI

which is in the custody and control of CCO. Privacy breaches include uses and/or disclosures of PHI that contravene PHIPA and/or CCO's Privacy and Security Policies.

The steps taken by the Privacy Office in addressing the breach are:

- Containment;
- Investigation;
- Resolution; and
- Reporting.

In 2009, 28 privacy breaches were investigated at CCO. The following chart summarizes the breaches and the outcome of the investigations. All of the recommendations stemming from the investigations were resolved and implemented. Several incidents involved the e-mailing of PHI. In order to address this issue, the Privacy Office will be revising its training material to include more education on the secure use of e-mail.

CCO Program	Number of Incidents	Description of Incidents	Outcome of Investigation
ColonCancerCheck	19	Participants' mailing address out of date	Breach <i>Root Cause: Incorrect Mailing Address</i>
	1	E-mailing PHI	Breach <i>Root Cause: Policy infraction</i>
Ontario Health Study	1	E-mailing PHI	Breach <i>Root Cause: Policy infraction</i>
	1	E-mailing PHI	Breach <i>Root Cause: Policy infraction</i>
New Drug Funding Program	1	E-mailing PHI	Breach <i>Root Cause: Policy infraction</i>
Wait Times Information System	1	Sharing of User name and password	Breach <i>Root Cause: Policy Infraction</i>
	1	Emailing of PHI (Internal) to authorized users	Breach <i>Root Cause: Policy Infraction</i>

	1	Emailing of PHI (Internal) to unauthorized users	Breach <i>Root Cause:</i> <i>Policy infraction</i>
Access to Care Informatics - Surgical Efficiency Targets Program (SETP)	2	Unencrypted Medical Record Numbers (MRN) sent to authorized users	Breach <i>Root Cause:</i> <i>Program Procedure infraction</i>

Additionally, in order to improve the tracking, management and reporting of breaches in a timely manner, the Privacy Office is currently developing an electronic breach escalation solution. This application will allow the analysis of metrics to identify trends which can address the underlying issues that lead to a breach. The Privacy Office has also created a database to record and manage breach report recommendations and monitor the timeliness of corrective actions.

Data Requests

CCO receives requests for data from external parties such as researchers and other prescribed entities. CCO also receives requests from Integrated Cancer Programs (ICPs), laboratories and hospitals for a subset of the data they have already provided CCO. CCO follows its Data Use and Disclosure Policy to examine, process and log these external requests.

Most requests for data come from researchers for the purpose of Research Ethics Board approved studies. CCO seeks to support cancer research by processing data requests as efficiently as possible. CCO also strictly adheres to its requirements under PHIPA to ensure that PHI is only disclosed to researchers for studies approved by Research Ethics Boards.

CCO received a total of 247 data access requests in 2009, 46 of which were research requests. Figure 1 illustrates the types of research requests received and Figure 2 illustrates the status of the data requests received in 2009.

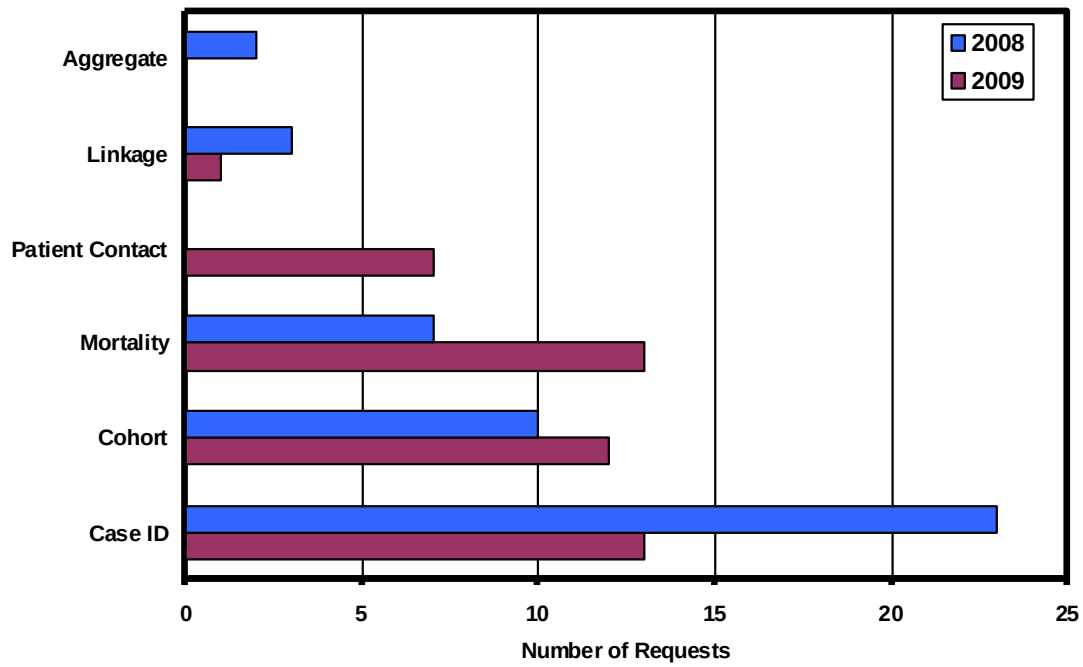


Figure 1: Types of Data Request for Research

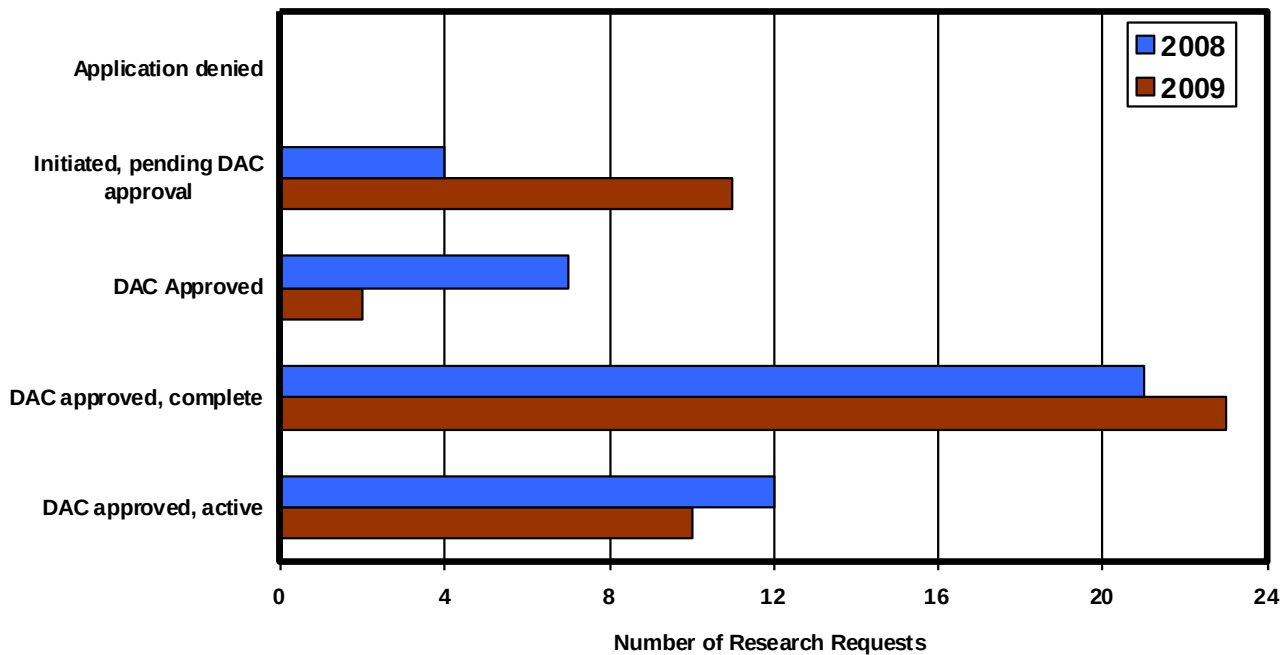


Figure 2: Status of Data Requests for Research

Patient Recruitment for Cancer Research

In 2009, a new process was implemented for patient recruitment for cancer research studies. Under Section 44 of PHIPA, CCO is required to obtain a patient's consent to be contacted for the purpose of participating in research. As such, CCO must obtain consent *prior* to contact by a researcher whose study otherwise meets the requirements outlined in PHIPA and in CCO's privacy policies.

In February 2009, CCO advised the IPC of the new patient recruitment procedure that balances the public benefit of vital cancer research with the privacy prerogatives contained in PHIPA. The IPC was briefed on the initiative and supporting documentation was created for public consumption.

To ensure that cancer research initiatives are not foreclosed, CCO has initiated a pilot patient contact process. Once CCO has approved a researcher's data request through its Data Access Committee, CCO works with the researcher to identify prospective participants. CCO contacts the prospective participants to introduce the research study and to provide an opportunity for individuals to "opt-out" of future contact. Participants may opt-out of the study by calling a number or returning a self addressed and stamped envelope. At the conclusion of this process and once CCO has provided formal approval for the research study, the contact information of the individuals who have not opted out of the study, along with written authorization to contact these individuals, will be provided to the researcher. The terms of this engagement will be specified in a confidentiality / non-disclosure agreement. The effectiveness of the pilot and the resource implications of the process will be evaluated to ensure that patient contact studies are adequately supported.

Seven research requests involving patient contact were received in 2009 since the new process went into effect. The Data Access Committee worked with researchers to identify the correct research cohort, prepared communications and begun mailing participant notification for the pilot.

III. Technology

The following section describes the technical safeguards implemented in the protection of PHI at CCO.

Enterprise Information Security Office

(1) Information Security Program

In order to protect PHI, the CCO Privacy Office works in close partnership with the Enterprise Information Security Office (EISO) which is responsible for the operation and development of CCO's information security program. The information security program at CCO is comprised of a broad range of activities, across the portfolio of work at CCO, and is delivered under the authority of the Chief Information Officer (CIO). This includes information security support of CCO's daily business operations, as well as consultations concerning project activities resulting in new information systems.

This section of the Annual Privacy Report discusses the information security milestones completed which support the Privacy Office objectives for protecting PHI retained by CCO.

(2) IT Security Resources and Roles

In 2008, CCO transitioned the information security program to the Chief Technology Office (CTO), to ensure a separation of duties for security assessment and oversight activities from those related to operational security. In 2009, building upon the previous transition, two key organizational changes occurred from a security perspective:

- The *Enterprise Information Security Office (EISO)* was officially established within the CTO, consisting of a manager and three full time staff. The EISO is structured to provide security services to all CCO projects and initiatives thus enabling the application of leading security principles and practices in a consistent manner. An important objective of this new service based approach is to ensure that internal information security resources are available for all CCO initiatives to leverage throughout their project lifecycle. A core function of the EISO is to provide CCO management with security risk management facilities by conducting security assessments that identify security risks and facilitating appropriate management of any identified risks.

The Privacy Program makes extensive use of the EISO's services to ensure that PHI is appropriately safeguarded and security risks are being managed.

(3) Information Security Risk Assessments

During 2009, a number of information security risk assessments were conducted in support of new and existing initiatives as part of the security risk management program. CCO regularly conducts both formalized and informal security assessments including Threat and Risk assessments (TRA) and Technical Vulnerability Assessments. The following initiatives had a TRA conducted in 2009:

- ColonCancerCheck(CCC)
- Wait Time Information System – Alternate Level of Care
- Collaborative Cancer Staging Project
- Interactive Symptom Assessment and Collection (ISAAC) application

As well, internal security review exercises were performed for projects like the Ontario Health Study pilot assessment centres and various core information technology initiatives within CCO.

(4) Information Security Program Enhancements

- **Enterprise Security Health Check** - As an element of continuous improvement, CCO undertook a major internal and third-party assessment of its information security program. This assessment project was called the

Enterprise Security Health Check and was conducted based on industry leading standards of practice for information security (e.g. ISO 27001 and ISO 27002). The results of this assessment were very positive, indicating that CCO is well positioned to be a leader in information security management in Ontario's health care sector. This assessment also provided recommendations for enhancing CCO's Information Security program over the coming years. The EISO has begun to address the findings of the assessment which will ensure that the proper foundation for safeguarding PHI exists and continues to improve within CCO.

- **Governance, Architecture, and Policy Framework** - An enhanced policy framework has been developed in collaboration with the Privacy Office, reviewed by various CCO stakeholders, and approved by the CIO for use. The existing information security policies are now being aligned to this new framework, which includes mappings to relevant standards and legislation, such as ISO 27001, ISO 27002 and PHIPA.
- As well, an information security governance structure has been established where it aims to facilitate coordination with the Privacy Office when responding to security risks.

(5) Information Security Infrastructure Improvements

In 2009, CCO introduced additional technical safeguards and improved existing safeguards to enhance protections for PHI. New safeguards initiatives included:

- Improving the media destruction capabilities and processes.
- Developing the audit processes to conduct more detailed access audits.
- Enhancing secure and managed file transfer capability for moving information securely between organizations.
- Review and enhancement of the existing anti-malware capabilities.

(6) Physical Security and Laptop Audits

According to CCO's Work Station Security Policy, all CCO laptops must be secured with the cable lock affixed to each workstation. Laptops must be secured during the workday and taken home or locked securely when offsite. At CCO, laptops and cable locks are provided concurrently

Laptop Audits were conducted on a quarterly basis by representatives from the Privacy Office and the Enterprise Information Security Office, where all workstations at CCO were examined to ensure compliance with the policy. The Privacy and Security specialists performing the audits confiscated unlocked laptops and advised individuals contravening the Work Station Security Policy of the correct procedure for securing their laptops.

PHI Access Monitoring and Auditing Project

In the 2008 triennial review of CCO, in its role as a prescribed entity, the Office of the Information and Privacy Commissioner/Ontario (IPC) recommended that CCO "develop and implement a comprehensive policy and associated procedures for the frequent review of system audit trails."

The IPC noted that the audit program should “detect unauthorized access to data holdings containing PHI and to detect information security incidents in a timely manner”. It should also be:

- Appropriate to the amount and sensitivity of the PHI collected;
- Commensurate with the number and nature of individuals with access to PHI;
- Consistent with industry standards; and
- Commensurate with the threats and risks associated with PHI.

In collaboration with the EISO, the Privacy Office launched the multi-year PHI Access Monitoring and Auditing project in 2009 in response to the IPC’s recommendation. This project entails a comprehensive analysis of threats and risks associated with access to PHI within CCO, in order to determine the appropriate controls necessary to detect unauthorized access to PHI in a timely manner.

To ensure alignment with other healthcare organizations that use PHI as a part of their day-to-day operations, CCO has undertaken an engagement that will validate its new logging, monitoring and auditing standard against peers, industry standards and best practices.

Year in Review - Privacy Updates for CCO Programs

2009 was an exciting year for CCO in that many new programs were added to CCO's portfolio. The following summarizes the programs that the Privacy Office has provided support and guidance to:

1. Ontario Health Study (OHS)

The OHS is a long-term, population-based, cohort study that will enable comprehensive studies of the risk factors which contribute to cancer, cardiovascular and other chronic diseases. The first phase of the study, the Integrated Pilot Study, took place between March and September 2009 – where men and women, between the ages of 35 – 69 years, from three Ontario communities, Mississauga, Owen Sound and Sudbury were recruited. The data collected from the participants with their informed express consent, included medical history, place of residence, occupational history, diet and exercise, along with the collection of biospecimens for use in future research based studies.

CCO has taken on the role of day-to-day operations and management for the study, in addition to its role as co-funder. In managing the study, CCO is leveraging its privacy network, where it has appointed an OHS Privacy Lead as the primary point of contact on all privacy matters and for ongoing privacy operations. A Manual of Privacy Best Practices has been developed to advise the OHS on their privacy responsibilities. Furthermore, a Privacy Report Card outlining the collection, use and disclosure practices, in addition to the information safeguards used in the study pilot has been developed.

2. Ontario Renal Network (ORN)

The MOHLTC in association with CCO established the Ontario Renal Network to improve patient care through the coordination and integration of renal services across the province. CCO will measure, monitor, assess and report on the performance of Chronic Kidney Disease (CKD) services and advise the MOHLTC, LHINs and other relevant stakeholders on all matters relating to CKD prevention and management.

CCO will lead the development of an integrated information management program that supports the infrastructure necessary to measure, monitor, assess and compare the quality of the CKD program, develop evidence based CKD standards, develop data requirements and establish reporting and review cycles. These activities will be managed as a part of our PHIPA section 45 function, as a prescribed entity.

The Privacy Office has provided on-going support and guidance in the development of its business model and outlining of operational activities. Furthermore, it will develop a PIA on the program's interim solution for data collection and performance reporting, once the programs long term IM/IT strategy has been established.

3. Interactive Symptom Assessment and Collection (ISAAC)

As a health information network provider (HINP), CCO manages the ISAAC Application and Database on behalf of health care providers. The ISAAC Application captures information on patients' symptom intensity using the Edmonton Symptom Assessment System (ESAS) and tracks functional status using the Palliative Performance Scale (PPS). ESAS may be entered directly by the patient into an ISAAC kiosk at their local cancer centre, through a secure website or it may be recorded on paper and subsequently entered into ISAAC by health care providers.

In 2009, the ISAAC application introduced an alternate patient access option, where cancer patients can now enter their ESAS symptom scores by telephone through Tele-ISAAC, an interactive voice recognition (IVR) system. Tele-ISAAC increases the range of options for patients to access ISAAC and contribute to timely symptom management, subsequently improving patient care.

The Privacy Office developed an Addendum to the 2007 Provincial Palliative Care Integration Project (PPCIP) PIA to provide a summary of the progress made on the recommendations presented in the 2007 PPCIP PIA, in addition to considering the privacy risks associated with Tele-ISAAC.

4. Ontario Breast Screening Program (OBSP)

The OBSP is a provincial screening program operated through CCO and funded by MOHLTC. The OBSP's mission is to reduce deaths from breast cancer by delivering high quality breast screening to women aged 50 and over at affiliated hospitals and independent health facilities.

As part of the annual review of OBSP policies, the Privacy Office conducted a review of the OBSP Guide to Information Management Practices. As well, the process for collecting information from participants and disclosing it to Primary Care Physicians was reviewed to ensure that the information collection practices are in compliance with the legislation and privacy best practices.

5. RN Performed Flexible Sigmoidoscopy (FSIG) Pilot Project

The goals for the FSIG Pilot Project are to evaluate the feasibility and acceptability of the RN led FSIG clinics and determine whether a new nursing role within the interdisciplinary team would enhance the capacity of human resources within the system. The data captured by the program is collected by CCO to support its prescribed entity duties for planning, evaluating and managing the provision of health care.

The Privacy Office developed FAQs to provide privacy tips to the program and also reviewed the program's amended Memorandum of Understanding with the hospitals reflecting the expanded scope of the pilot project.

6. ColonCancerCheck (CCC)

CCC is a province wide colorectal cancer screening program designated as a prescribed registry under PHIPA. It is a population-based colorectal cancer screening initiative targeted to Ontarians aged 50 to 74. CCC has reduced mortality from colorectal cancer through an organized screening program and to improve the capacity of physicians to provide comprehensive cancer screening. CCC is working toward the goal of reducing colorectal cancer mortality in Ontario by 15 percent within ten years.

In 2009, the CCC program focused on deployment of its information technology solution, InScreen, and the launch of a Primary Care Invitation Pilot. The goal of the Pilot is to engage Ontario's primary care providers in the process of recruiting and inviting eligible Ontarians for screening. The Pilot will allow CCC to share information with primary care providers about their screening activities, thereby proactively engaging providers in promoting screening activities for their patients between 50 and 74.

In order to provide support to the Pilot and InScreen initiative, the Privacy Office developed an Addendum to both the CCC PIA and the Colonoscopy Interim Reporting Tool (CIRT) PIA. All recommendations from these PIA's were addressed prior to the launch of the new initiatives.

In September 2009, the CCC Privacy Specialist also completed an annual privacy audit of the fulfillment house which provides lettershop services to the program. The audit involved the review of the lettershop facilities and evaluation of their administrative, physical and technical safeguards. Privacy training was also provided to the fulfillment house staff that process the CCC letter. The privacy training focused on key CCC privacy practices, such as storage and retention of PHI, technical safeguards, privacy breach management and confidentiality.

7. Aboriginal Data Indicators Pilot

The MOHLTC and CCO have partnered on a project to enhance cancer data collection on the Aboriginal population in Ontario. The premise of the pilot is that better data can assist in improving the health status of Aboriginal people and the quality of care they receive.

The Privacy Office has conducted an authority review as well as completed a Preliminary Privacy Assessment of the program to ensure that the pilot complies with the provisions of PHIPA and the CCO Privacy Policy. Lastly, the Privacy Office also reviewed the Memorandum of Understanding between CCO and the Aboriginal health access centres.

8. Cancer Stage (CS) Project

The primary goal of the CS Project is to develop and implement an electronic data collection process to determine cancer stages for all Ontarians newly diagnosed with cancer.

The Privacy Office was actively involved in the development of privacy requirements for the different streams of the project as well as participated in the Request for Proposal process, requesting vendor services for the automation of pathology reports.

9. Access to Care (ATC)

The ATC Portfolio is comprised of information technology and information management (IM/IT) initiatives with a single strategic focus on improving access, quality and efficiency of patient care and tracking patients as they move across the continuum of care. The mandate of the ATC Portfolio is the development and implementation of information strategies and information systems to support improved access to care, ongoing operation of information systems, data analysis and reporting.

The ATC Portfolio currently includes the following initiatives:

(i) **Emergency Room / Alternate Level of Care (ER/ALC)**

CCO's ATC Office was tasked with developing an Emergency Room / Alternate Level of Care (ER/ALC) Information Strategy. The province's commitment to reduce ER wait times is supported by the ER/ALC Wait Time Strategy which sets out a results focused agenda to reduce demand on ERs, to increase ER capacity/patient flow and to move patients waiting in acute care hospitals to a more appropriate level of care out of the hospital. The following initiatives under the ER/ALC Information Strategy have been reviewed by the Privacy Office:

- a. **ALC Resource Matching & Referral (RM&R) Provincial Reference Model (PRM)** - The ALC RM&R PRM defines a standard approach for the implementation of resource matching and referral solutions in LHINs and LHIN clusters across the province of Ontario.

The Privacy Office conducted a preliminary privacy assessment of the ALC RM&R solution's conceptual architecture and concluded that the PHIPA statutory authority for the operation of the ALC RM&R solution is that of a HINP. The result of the assessment led to a series of privacy requirements that are included in the PRM. However, another assessment will need to be conducted in order to ensure the ALC RM&R final solution is operating in compliance with PHIPA.

The Privacy Office developed the privacy standards to be included in the PRM. The standards are based on PHIPA principles and privacy best practices.

- b. **ER National Ambulatory Care Reporting System (NACRS) Initiative** – The ER NACRS Initiative has been developed to report on ER data. As a key recommendation in the delivery of the ER/ALC Information Strategy, the public reporting turn-around time of ER data must be accelerated to a one month period and linkages with other data sets must also be made. CCO and CIHI will work collaboratively to use NACRS Level 1 Data instead of EDRS data for provincial performance management in Ontario.

The Privacy Office completed a privacy assessment of the transfer of PHI from CIHI to CCO. An outcome of the assessment recommended the appointment of a data steward, confirmed controlled access to the data holding to authorized users and an update to the CCO-CIHI data sharing agreement to reflect the program changes.

- c. **ER/Community Care Access Centre (CCAC) Notification System** - The ER/CCAC Notification System is being developed to implement one of the recommendations from the ER/ALC Information Strategy. The objective of the project is to develop a Business Process Tool to address the following goals:

- Avoid hospital admissions through the ER by identifying patients that could be treated at home instead of being admitted;
- Identify existing CCAC clients that could benefit from improved community support (avoiding future ER visits);

- Identify high risk patients, such as seniors, that could benefit from a CCAC assessment and community support (avoiding future ER visits); and
- Capture data for performance management and reporting to support decision-making.

The Privacy Office conducted a preliminary privacy assessment of the ER/CCAC Notification System's conceptual architecture and concluded that the PHIPA statutory authority for the operation of the solution is that of a HINP. A comprehensive PIA will be conducted upon completion of a detailed system architecture.

- d. **Client Profile Database (CPRO)** - The ER/ALC Information Strategy identifies the need to collect information specific to patients awaiting Long-Term Care in the community (i.e., retirement homes and supportive housing). The CPRO database collects information on a monthly basis directly from CCAC systems specific to patients who are waiting for long-term care placement.

The Privacy Office completed a preliminary privacy assessment for the collection of PHI by CCO from the MOHLTC. The assessment concluded that the data set collected by CCO is PHI and that the PHIPA statutory authority for the collection is that of a prescribed entity.

(ii) Surgical Efficiency Targets Program (SETP)

SETP was established to support Ontario's strategy of reducing wait times through improved surgical processes. SETP uses data concerning operating room (OR) performance to analyze processes and identify areas where OR performance challenges exist. The implementation and operational support for SETP was transferred from University Health Network to CCO on June 30, 2009.

The Privacy Office developed an Addendum to the 2007 SETP PIA, which was originally developed for the MOHLTC, for the purposes of identifying potential privacy risks concerning the program, in addition to providing CCO recommendations to mitigate those risks. Privacy continues to be a part of the changes which are planned for this program and will provide additional support and analysis as the program develops.

(iii) Enterprise Data Warehouse (EDW)

CCO's EDW supports the acquisitions and delivery of information to CCO and external information consumers through a robust analytic web portal for the population of cancer indicators and in support of critical cancer planning, research and decision making. The primary objectives for the EDW roadmap include:

- Support and implement the analytic and reporting initiatives outlined in the CCO Information Strategy 2008 – 2011, to assist CCO in fulfilling its mandate
- Establish a "single version of the truth" by continuing to standardize and enrich the information within the EDW and increasing the quality and management of information available
- Conform to existing CCO privacy and security policies and procedures

The Privacy Office completed an Addendum to the January 2008 EDW PIA. The Addendum includes a privacy assessment of the current EDW architecture. EDW operates under CCO's prescribed entity authority. The recommendations stemming from this privacy assessment are expected to be implemented by the end of 2010.

(iv) Wait Time Information Program (WTIP)

The Ontario Wait Time Strategy, launched by MOHLTC in 2005, aims to provide Ontario patients with greater access to health care services by enabling the monitoring, management, and reduction of wait times for adult and pediatric surgical procedures and treatments (e.g. cancer surgery, cataract surgery, and MRI and CT scans). To enable the monitoring of these benchmarks, the Ontario Wait Time Strategy implemented a web-based information system, the Wait Times Information System (WTIS), to facilitate wait times management and provide the public with wait times information.

In 2008, the WTIS was identified as the platform of choice for capturing ALC Wait Times. As a result, the WTIP is enhancing the WTIS to enable the collection of ALC data in near real time. The expanded system is expected to be completed in 2011 and implemented in existing WTIS acute care facilities and in post-acute care facilities.

The Privacy Office completed a privacy assessment of the changes to the WTIS and concluded that the changes will have no significant impact on the current privacy posture of WTIP. The Office recommended that WTIP make minor amendments to the Licence Agreements that it currently has with its partners.

In 2009, WTIP conducted an Operational Effectiveness Review, whereby staff were required to complete a privacy survey specifically responding to questions concerning privacy policies and procedures as they relate to their day to day operations. In 2009, staff performance was rated as above average as most respondents answered 100% of the questions correctly.

CONCLUSION

The continuous engagement of the Privacy Office in all of CCO's various development activities, attests to the value of privacy as a business enabler. The service delivery model for the Privacy Office has changed in order to ensure the presence of privacy throughout the life cycle of all program initiatives. The enhancements have strengthened the privacy infrastructure to permit streamlined access to privacy resources through a standardized work intake procedure, dedicated specialists assigned to each program and preliminary assessments to identify privacy risks from the outset of a project. The Privacy Office will monitor the effectiveness of the new service delivery model to ensure that CCO's Privacy Program continues to fulfill its obligations to the organization.

New Legislative Requirements

Freedom of Information and Protection of Privacy Act

As of January 1st, 2010 CCO has been designated as an “institution” within the meaning of the *Freedom of Information and Protection of Privacy Act* (FIPPA). As a result, all persons may have a legal right of access to information in the custody and/or control of CCO, with the exception of personal health information and subject to a limited set of exemptions. The objective of FIPPA is to make government more open and therefore more accountable to the people of Ontario, while protecting individual privacy. The Board Chair of CCO has been named the head of the institution for the purposes of decision-making under FIPPA and he has delegated his decision-making responsibilities to the Chief Privacy Officer.

Both FIPPA and PHIPA outline the conditions under which the public may access information, while balancing the need for individual privacy. FIPPA applies to many records created and/or used by CCO. As such, FIPPA applies not only to records created by CCO but also to any records that it receives. As a general rule, PHIPA will continue to govern the protection of all personal health information within CCO’s custody and control.

As both FIPPA and PHIPA require the measured review and control of CCO information assets, they will be managed by the newly expanded Privacy & Access Office. To ensure compliance with the legislation, CCO has hired a Freedom of Information (FOI) Coordinator and a FOI Analyst to gather and process all access requests. Additionally, a FOI Lead has been identified for each CCO business unit. These individuals are responsible for assisting the Privacy & Access Office in searching for responsive records and helping to identify records to which access exemptions may apply.

Upon receiving notice in October of 2009 that CCO would be designated as an institution under FIPPA, in preparation for its expanded mandate and for CCO’s new role under FIPPA, the Privacy Office:

- Recruited a FOI Coordinator and Analyst to gather and process all access requests;
- Reviewed the Governance structure at CCO and implemented the required changes to ensure compliance with FIPPA;;
- Outlined the business requirements and procured the required case management tools; and
- Updated the CCO external and internal website to include FIPPA web pages.

Furthermore, the Privacy Office developed the following tools to ensure compliance with the Act:

- FOI Policy Framework, including standards and procedures;
- FAQs for employees;
- Terms of Reference for FOI Leads;
- Directory of Records/Personal Information Banks;
- FOI Manual;
- Training materials for staff; and

- Communication plan for new compliance requirements.

The Privacy & Access Office is working closely with Public Affairs to ensure effective issues management to provide consistent messaging to the public, media and the MOHLTC.

Goals for 2010

CCO Privacy Office continues to grow in order to match the growth of the organization and the evolving nature of its programs and projects. To this end, the Privacy Office will focus on the following goals in 2010:

- 1) A proposed enhanced policy framework has been developed for the organization. The Privacy Office will conduct a comprehensive review of its existing policies, procedures and standards to ensure alignment with the proposed framework.
- 2) As discussed in the Technology section, CCO plans to operationalize its new audit initiative in 2010. The initiative will utilize both automated and manual processes to monitor access to PHI in CCO systems.
- 3) Introduce a standard for information management. Each program that processes PHI will be asked to maintain a bank of information management practices that will include a description of the program, data holdings, the status of PIA recommendations and other key elements, as defined.
- 4) The Privacy Office will work closely with CCO's Human Resources Division to develop an Employee Privacy Policy to ensure the protection of employee personal information.
- 5) As CCO will be required to comply with the *Freedom of Information and Protection of Privacy Act* (FIPPA) commencing January 1, 2010, the new Privacy and Access Office will launch policies and procedures to ensure compliance with the Act and refine the Access program as required.
- 6) The Privacy Office will identify and review all vendor and partner agreements used by CCO to develop standard privacy provisions to be included in the template agreements.
- 7) The Privacy Office will implement its Communications Plan for 2010 where it will disseminate information on privacy best practices and tips in a dynamic manner, such as through screensavers on all CCO desktops and laptops.
- 8) The Privacy Office will review and refine the current privacy gating process to ensure that it is effectively operationalized into CCO's project management life cycle.
- 9) The Privacy Office will continue reviewing its information management practices in light of the 2008 triennial IPC Prescribed Entity and Prescribed Registry Reports.
- 10) The Privacy Office will seek Prescribed Registry designation under PHIPA for the Integrated Cancer Screening Program.