Privacy & Access Office

Ontario

2011 Prescribed Person Triennial Review Report

October 2011
Version 3

CCO Privacy & Access Office
620 University Avenue, 15th floor
Toronto, ON M5G 2L7
Phone: 416.217.1816
Fax: 416.971.6888
Email: privacyandaccessoffice@cancercare.on.ca

Ontario
Cancer Care Ontario
Action Cancer Ontario

Table of Contents

ACRONYMS

ATC…… Access To Care
CAB…… Change Advisory Board
CCC……ColonCancerCheck
CCO…… Cancer Care Ontario
CCSR……Colorectal Cancer Screening Registry
CEO……Chief Executive Officer
CIO…….. Chief Information Officer
CPO……Chief Privacy Officer
CSP…….. Cancer Screening Program
CTO……Chief Technology Officer
DAC……..Data Access Committee
DSA…….. Data Sharing Agreement
EISO……Enterprise Information Security Office
HIC……Health Information Custodian
IPC…… Information and Privacy Commissioner / Ontario
ITIL……Information Technology Infrastructure Library
MOHLTC…… Ontario Ministry of Health and Long-Term Care
MOU…… Memorandum of Understanding between CCO and the MOHLTC dated December 2, 2009
OCSR……..Ontario Cancer Screening Registry
ODDAR…… Online Direct Data Access Request
O.Reg. 329/04……Ontario Regulation 329/04 to PHIPA
ORN…… Ontario Renal Network
PET…….. Positron Emission Tomography
PHI…… Personal Health Information
PHIPA……..*Personal Health Information Protection Act, 2004* (Ontario)
PIA…… Privacy Impact Assessment
REB…….. Research Ethics Board
WTIS…… Wait Times Information Strategy

INTRODUCTION

Cancer Care Ontario **(CCO)** is the provincial agency responsible for continually improving cancer services. Formally launched in 1997 and funded by the Ontario government, CCO is governed by the *Cancer Act* (Ontario). Further, as an Operational Service Agency of the Ontario Government, CCO's mandate is determined pursuant to a Memorandum of Understanding **(MOU)** between CCO and the Ministry of Health and Long-Term Care **(MOHLTC)** dated December 2, 2009.

As the provincial agency responsible for continually improving cancer services, and the Ontario Government's cancer advisor, CCO:

- Directs and oversees close to $750 million public health care 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 health care 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.

In addition to cancer, CCO has other core lines of business including supporting and hosting the provincial Access to Care **(ATC)** program, which is a part of the Government of Ontario's Wait Times Information Strategy **(WTIS)**. CCO has also worked with renal leadership in Ontario to launch the newly formed Ontario Renal Network **(ORN)**, as well as special access programs such as Positron Emission Topography **(PET)** Scans Ontario. These activities are governed by separate accountability agreements between CCO and the 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)**.

Subsection 39(1)(c) of PHIPA permits health information custodians (**HICs**) to disclose PHI without consent to certain prescribed persons who compile or maintain a registry of PHI for the purposes of facilitating or improving the provision of health care ("prescribed registry" purposes). Currently CCO is designated as a "prescribed person" for the purposes of subsection 39(1)(c) of the PHIPPA, under subsection 13(1) of the Ontario Regulation (**O. Reg**.) 329/04, with respect to CCO's role in compiling and maintaining the Colorectal Cancer Screening Registry (**CCSR**) as part of the ColonCancerCheck (**CCC**) program. It is expected that in May 2011, O. Reg 329/04 will be amended to designate CCO as a "prescribed person" with respect to the Ontario

Cancer Screening Registry (**OCSR**) (a "prescribed registry") as part of the Cancer Screening Program **(CSP)**. The CSP is an expansion of the service delivery model used by the CCC program, which invites, recalls and reminds a target population of Ontarians to proactively be screened for colorectal cancer. The CSP is comprised of three screening modules, i) breast screening ii) cervical screening and iii) colorectal cancer screening. The framework and infrastructure which has successfully been used for the CCC program will now be expanded to support screening for breast and cervical cancer. As a prescribed registry, CCO has the authority to collect, use and disclose PHI for the purpose of facilitating or improving this provision of breast, cervical and colorectal cancer screening services and care for Ontarians.

The CSP will leverage the key components of the service delivery model which is currently employed for the CCC Program. This will include:

- Identification of the target screening population for each type of cancer (breast, cervical and colorectal);
- Inviting the identified population to engage with their primary care provider to discuss screening;
- Notifying participants who are screened of their test results; and
- Communicating with program participants when it is time to be re-screened.

As noted above, the following three screening modules comprise the CSP, colorectal, cervical and breast screening. The operational status of each module is as follows:

1. Colorectal Screening (known as CCC): The CCC program is fully operational and has robust privacy controls embedded within the administrative, processing and technical infrastructure. This program was reviewed in 2008 by the IPC and received its first 3 year approval of its privacy practices.
2. Cervical Screening: The cervical screening module will be integrated into the existing screening infrastructure on September 2011. A privacy gap analysis for the integration of the cervical service delivery component has been conducted and updates to the current policy and its supporting procedures have been made to address the program expansion.
3. Breast Screening: The breast screening component of the CSP will be integrated into the existing screening infrastructure on April 2012. This breast screening component will also follow a similar service delivery methodology as the one in place for colorectal and cervical screening. As with the cervical module, a preliminary gap assessment has been conducted on the conceptual model for breast screening. Initial updates to the current policy and its supporting procedures have been made to address the program expansion. A Privacy Specialist is fully engaged in the project planning activities for the CSP and as more details are identified for the 2012 launch, the appropriate privacy controls will be built into the program.

A conceptual Privacy Impact Assessment (**PIA**) is currently being conducted on CSP. Any privacy risks identified by the PIA will be addressed before the September 2011 expansion to include the cervical module. Additionally, as changes are made to the program, updates will be made to the PIA in accordance with the CCO Privacy Impact Assessment Standard.

Furthermore, in order to begin operations of the expanded CSP, subsection 13(2) of O. Reg. 329/04 requires each prescribed person to have in place practices and procedures to protect the privacy of the individuals whose PHI it receives and to maintain the confidentiality of that

information. Subsection 13(2) further requires each prescribed person to ensure that these practices and procedures are approved by the Information and Privacy Commissioner/Ontario **(IPC)** on a triennial basis in order for HICs, and other persons authorized under PHIPA, to disclose PHI to the prescribed person without an individual's consent.

As noted above, the initial approval of CCO's practices and procedures in respect of the CCSR (prescribed registry) was received from the IPC on May 1, 2008. CCO had its status renewed on October 31, 2008, for an additional three year term. This report constitutes CCO's submission to the IPC for the 2011 approval process in respect of its prescribed registry role as the OCSR. The OCSR, as stated above, is a prescribed registry which supports CSP's expansion of services to other types of cancer. Therefore, the PHIPA Regulation change will rename the "Colorectal Cancer Screening Registry" as the "Ontario Cancer Screening Registry". The policies and procedures for CCSR will be amended to reflect the expansion of services to include the colorectal, breast and cervical screening modules.

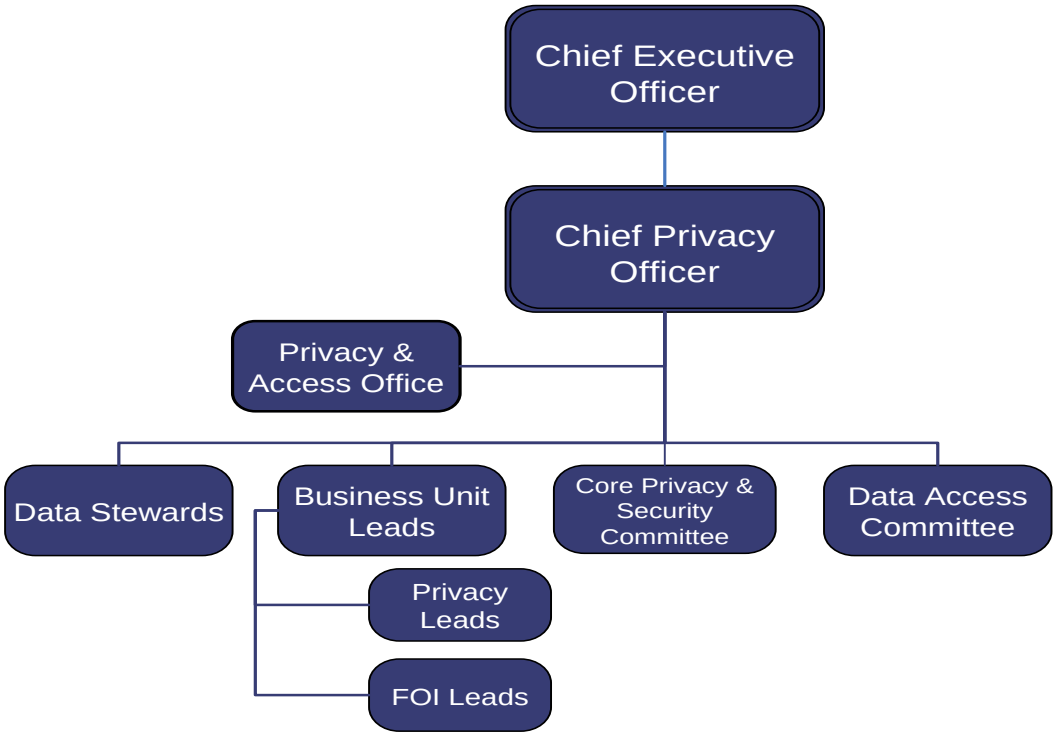
CCO also operates as a prescribed entity under Subsection 45(1). A separate report has been submitted to IPC in respect of its prescribed entity role.

CCO'S PRIVACY PROGRAM

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of PHI within its custody or control. CCO meets this commitment through its Privacy Program. This Program is overseen by the Chief Privacy Officer **(CPO)** who reports directly to CCO's President & Chief Executive Officer **(CEO)**. The CPO is supported in carrying out her responsibilities by a network of individuals and committees with specific privacy and security related responsibilities, including:

- A Director, Privacy & Access who is responsible for the day-to-day operation of privacy processes within CCO and the development and implementation of, and the compliance with, CCO privacy policies.
- A Senior Privacy Specialist who reports to the Director, Privacy & Access and supports the CSP Privacy Program.
- A Chief Data Steward who assigns a Data Steward to each CSP data-holding who is responsible for authorizing both internal and external requests for access to CSP data in accordance with CCO's Data Use and Disclosure Policy.
- A Facilities Manager who is responsible for ensuring the physical integrity of CCO's premises.
- Systems Security Specialists who report to the Chief Technology Officer **(CTO)** and oversee IT security safeguards for CCO data.
- The Core Privacy and Security Committee, composed of the CPO, members of the Privacy & Access Office, members of the Enterprise Information Security Office **(EISO)**, and key members of CCO's information management team - which provides advice and consultation to the CPO on specific privacy topics.
- A Data Access Committee (**DAC)**, supported by an Information Management Coordinator, which is responsible for reviewing and approving requests for access to CCO data.

PRIVACY ORGANIZATIONAL CHART



The key components of CSP's Privacy Program include:

- CSP's Privacy Policy and associated procedures;
- a privacy network comprised of individuals and committees, as described above;
- an employee privacy training, communication and awareness program;
- a privacy audit and compliance program; and
- privacy impact assessments and addendums on the CSP's existing and evolving processes and data holdings .

STATUS OF THE CCO 2008 PRESCRIBED REGISTRY TRIENNIAL REVIEW RECOMMENDATIONS

The IPC's 2008 triennial review of CCO, in respect of its prescribed registry practices and procedures, resulted in 11 recommendations to be addressed prior to the next triennial review.. The following charts provide:

- a detailed description of the recommendations;
- the manner in which the recommendations have been addressed or will be addressed; and
- the status of each recommendation.

2008 IPC Prescribed Registry Recommendations – Privacy

2008 IPC Compliance Recommendation	CCO Enhancement	Status		Expected Date of Completion
		Complete	In Progress	
1. Execute agreement between MOHLTC and CCO, in respect of the Colorectal Cancer Screening Registry.	A Data Privacy Agreement for a Prescribed Registry between CCO and MOHLTC has been executed.	✓		
2. Execute an agreement between CCO as a prescribed person and CCO as a prescribed entity.	A Data Sharing Agreement between CCO as a prescribed entity and CCO as prescribed registry has been executed.	✓		
3. Execute agreement with the third party mail service provider.	An agreement between CCO and the third party mail service provider was executed. Following a procurement process which took place in 2010-11,CCO entered into a new agreement with this provider who was the successful bidder in this	✓		

	process.			
4. The templates for invitation letters, screening results notification letters and screening reminders letters should be finalized.	The following templates have been developed. Result notification, Invitation letters, and Reminder communications.	✓		
5. A summary of the privacy impact assessment on the Colorectal Cancer Screening Registry be developed and made available on the CCC website.	A summary of the privacy impact assessment has been posted on the CCO website.	✓		
6. The FOBT Kit Privacy Insert to be revised to specify that the individual will be able to obtain results even if they opt out of being contacted by the Program. as described in this report.	FOBT Kit Privacy Insert was updated as per IPC recommendation.	✓		
7. Policies and procedure for reviewing and approving data requests from external parties for data maintained within the Colorectal Cancer Screening Registry be developed.	All requirements have been met through: - The development of the CCC Data Request Procedure - Updating the CCO Business Process for Data Requests.	✓		
8. A protocol for de-identifying the personal health information maintained in the registry prior to its use for secondary purposes, including analysis and research, to be developed.	All requirements have been met through the development of CCO De-identification Guidelines.	✓		

2008 IPC Recommendations – Security

2008 IPC Compliance Recommendation	CCO Enhancement	Status		Expected Date of Completion
		Complete	In Progress	
1. Security policies and procedures to be updated to reflect recent security enhancements including: a) Port-level security b) PGP whole disk encryption c) RSA SecurID	All requirements have been met through: - Port-level Security CCO's Personal Computer Security Policy - Policy on access to CCO Systems by Consultants - CCO's Password Policy	✓		
2. A comprehensive threat and risk assessment (TRA) in respect of the Colorectal Cancer Screening Registry to be conducted.	All requirements have been met, through: - The completion of security assessments of the CCC technology infrastructure including a TRA of the application and data store	✓		
3. A strategy for addressing the risks identified in the threat and risk assessment conducted in July 2008, be developed and implemented, prior to the next IPC Prescribed Person Review.	All requirements have been met. Note: The System on which the TRA was conducted is no longer in production.	✓		

As the above noted recommendations are specific to the CCC program, CCO has and will continue to consider all previous IPC findings during the development of the program solutions.

Policies, procedures, correspondence templates and the development of PIA's/TRA's for the CSP will all be assessed against the 2008 recommendations.

CCO 2011 PRESCRIBED PERSON TRIENNIAL REPORT - OVERVIEW AND METHODOLOGY

The *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (the **Manual**) was developed by the IPC to outline the new processes to be followed when reviewing the practices and procedures used by Prescribed Persons, such as CCO, to protect the privacy of individuals and to maintain the confidentiality of the PHI received by the Prescribed Person.

The Manual states that CCO must ensure its practices and procedures include the policies, procedures, agreements and documentation set out in *Appendix "A" - List of Required Documentation* of the Manual, and contain the minimum content set out in *Appendix "B" - Minimum Content of Required Documentation*. In order to verify if CCO has developed and implemented all requirements set out in the Manual, a written report and sworn affidavit will be submitted to the Commissioner.

CCO's Privacy & Access Office undertook the review of CSP's procedures and practices along with other supporting departments. The Privacy & Access Office created a comprehensive reference checklist based on the full requirements outlined in the Manual for the purposes of creating a tracking sheet for each requirement. There were multiple stages of the review process; the main stages of the review process can be broken down as follows:

i. *Engaging departments* – The Privacy & Access Office engaged departments across CCO and provided them with a full briefing on the scope of the review, including the IPC requirements in terms of documentation/logs concerning their program area and timelines.

ii. *Document collection and checklist reconciliation* – All relevant documentation was gathered, reviewed and compared against the requirements set out in the Checklist and Manual.

iii. *Policy drafting* – Where the documentation did not fully meet a requirement, minor amendments were made or new documents were developed.

iv. *Report drafting* – *T*he final CCO 2011 Prescribed Person Triennial Review Report was drafted and finalized, after all of the requirements were reviewed and responded to.

The structure of the CCO 2011 Prescribed Person Triennial Review Report follows the List of Required Documentation provided in Appendix "A" of the Manual. The Report is presented in a table format, wherein each required document listed in Appendix "A" is organized in a separate table. It is recommended that this report be reviewed along with the Manual, as requirements have not been duplicated verbatim in this report.

As noted in the Manual, each requirement includes a minimum set of criteria or content, as provided in Appendix “B” of the Manual. If CCO complies fully with a requirement, all documents which meet the criteria of that requirement are listed. If compliance with a requirement has not been fully met by CCO, the table will identify the gaps along with the measures to be implemented in order to fully meet the IPC requirements. The table also shows the status of the identified measures for full compliance. A quick matrix grid has been included to highlight CCO’s compliance with the IPC requirements by mapping each requirement to the appropriate CCO documentation or tool.

The Privacy, Security, Human Resources and Organizational Indicators, as outlined in Appendix “C” of the Manual, are reported within a separate table. An explanation is provided where certain indicators are not reported on and, where appropriate, the measures to be implemented to permit future reporting of such indicators are also provided.

Lastly, a list and summary of all CCO documents and tools that were reviewed as part of this exercise has been included in the appendices of this report.

CCO'S PRIVACY PROGRAM FRAMEWORK

The ability of CCO's Privacy & Access Office to fulfill its commitment to respecting personal privacy, safeguarding confidential information, and ensuring the security of PHI within its custody or control, is supported by CCO's Enterprise Information Security Office (**EISO**) and the Human Resources, Facilities, Legal and Procurement departments within CCO. These business units have embedded privacy practices within their own programs. This Privacy Program Framework (**Figure 1**) demonstrates this interconnectivity and the permeability between these groups, as illustrated through the policies, standards, procedures, and guidelines that support Privacy's initiatives. Moreover, it shows the depth and collaboration within CCO as the Privacy & Access Office works towards fulfilling its commitment.

The Privacy Program Framework follows a tiered approach with enterprise policies at the top. Each subordinate tier draws its authority from a higher tier, whereby the subordinate tiers support the higher tiers, by providing additional detail but not establishing conceptually new principles, requirements or responsibilities. Each document level requires a different approval process (policies are approved at the highest level of the organization). Policies are formal, brief, and high-level statements or plans that embrace an organization's general beliefs, goals, and objectives. Standards are mandatory actions or rules designed to support and conform to a policy. Procedures are a series of steps taken to accomplish an end goal. Guidelines are not mandatory, but they provide additional detail or context with the aim to streamline a particular process.

Please see Appendix A – Supporting Documentation, where all supporting documentation referenced in the Report has been summarized.

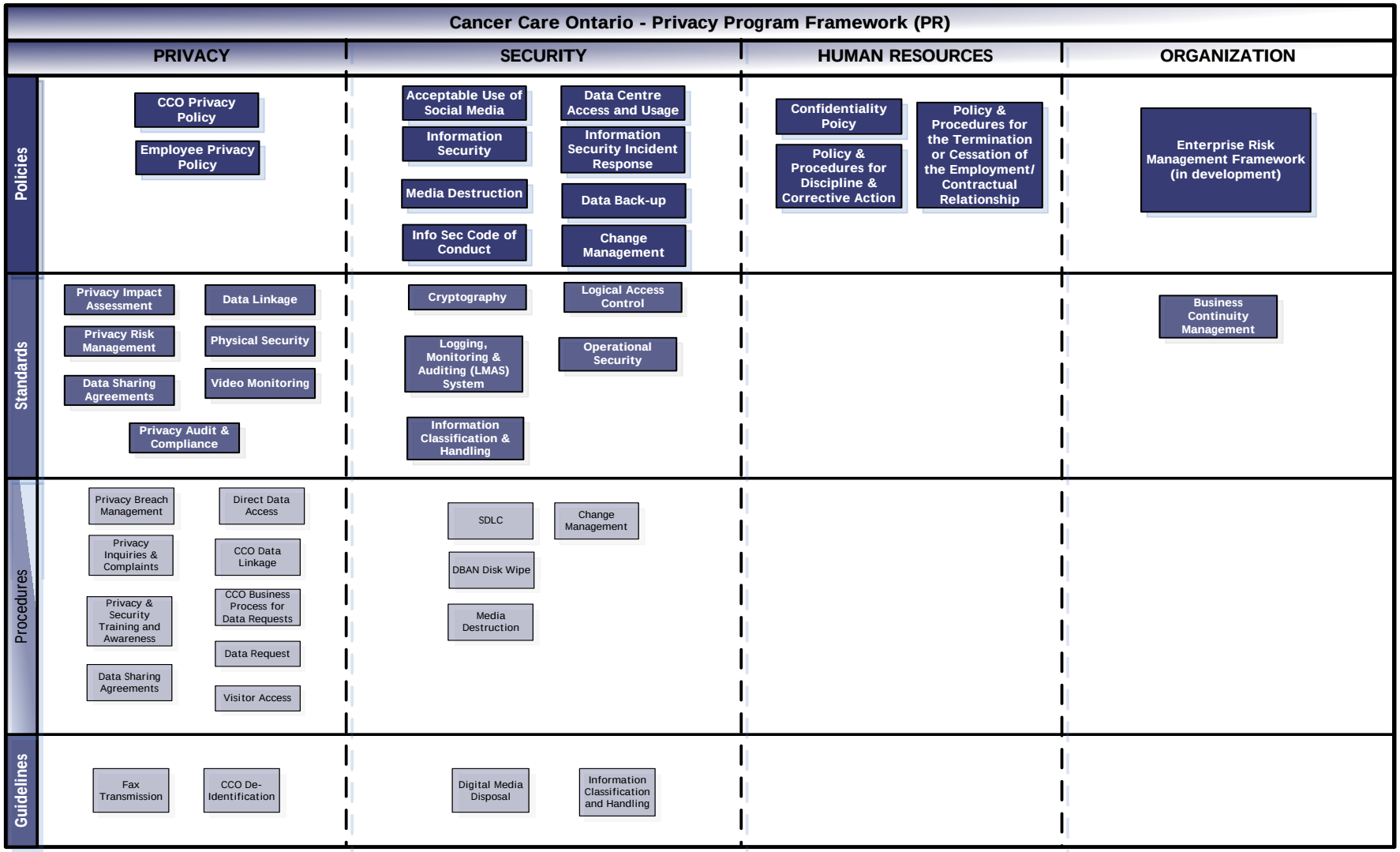


Figure 1: Privacy Program Framework with respect to the CSP

PART 1: PRIVACY DOCUMENTATION

Privacy Documentation Matrix

CCC Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10 (N/A)	Requirement 11 (N/A)	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
CCC's Access Control Procedure								x											x														
CCO's Application for Disclosure for Information from CCO for Research Purposes													x	x																			
CCO's Business Process for Data Requests												x	x											x									
CCO Privacy Audit and Compliance Standard		x		x		x						x	x			x			x			x		x	x		x	x	x		x		x
CCO's Contract Management System																					x													
CCO's Data Access Committee Terms of Reference													x																					
CCO's Data Linkage																						x												

CCC Privacy Matrix *Procedure*	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10 (N/A)	Requirement 11 (N/A)	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
CCO's Data Linkage Standard																						**x**											
CCC's Data Request Procedure	**x**											**x**	**x**											**x**									
CCO's Data Sharing Agreement Initiation Form				**x**								**x**					**x**															
CCO's Data Sharing Agreement Procedure				**x**								**x**				**x**	**x**	**x**															
CCO's Data Sharing Agreement Standard				**x**								**x**				**x**	**x**																
CCO's Data Sharing Agreement Summary Chart																		**x**															
CCO's Data Sharing Agreement Template				**x**								**x**					**x**																
CCO's Data Steward Terms of Reference	**x**			**x**				**x**																									

CCC Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10 (N/A)	Requirement 11 (N/A)	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
CCO's Decision Criteria for Data Requests												**x**	**x**											**x**									
CCO's De-Identification Guidelines	**x**											**x**	**x**											**x**									
CCO's Direct Data Access Audit Procedure								**x**																									
CCO's Employee Exit Process								**x**																									
CCO's Information Classification and Handling Guideline																			**x**														
CCO's Information Management Coordinator Terms of Reference													**x**																				
CCO's List of Data Linkages																							**x**										
CCO's Logging, Monitoring, and Auditing Standard		**x**																									**x**						

CCC Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10 (N/A)	Requirement 11 (N/A)	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
CCO's Media Destruction Policy								**x**				**x**																					
CCO's Microsoft Access Data Access Management Tool															**x**																		
CCO's Non-disclosure/Confidentiality Agreement													**x**	**x**																			
CCO's Online Direct Data Access Request (ODDAR) Form and Tool								**x**	**x**																								
CCO's Privacy & Access Office Remediation Program																					x				**x**	**x**		**x**		**x**		**x**	
CCO's Privacy & Access Office Operational Manual		**x**																	x								**x**						
CCO's Privacy & Security Acknowledgement Form																								**x**									

CCC Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10 (N/A)	Requirement 11 (N/A)	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
CCC's Privacy Breach Management Procedure				**x**		**x**							**x**						**x**			**x**		**x**	**x**				**x**	**x**	**x**		**x**
CCO's Privacy Breach Report Form																													**x**				
CCO's Privacy Impact Assessment Standard																									**x**								
CCO's Preliminary Assessment Form				**x**																													
CCC's Privacy Inquiries and Complaints Procedure																															**x**	**x**	**x**
CCC's Privacy FAQs			**x**																														
Principle & Policies for the Protection of Personal Health Information at CCO	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**								**x**	**x**	**x**	**x**					**x**	**x**		**x**		**x**	**x**	**x**	**x**	**x**
Online Direct Data Access Request Tool									**x**																								

CCC Privacy Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10 (N/A)	Requirement 11 (N/A)	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19	Requirement 20	Requirement 21	Requirement 22	Requirement 23	Requirement 24	Requirement 25	Requirement 26	Requirement 27	Requirement 28	Requirement 29	Requirement 30	Requirement 31	Requirement 32	Requirement 33
CCO's IM/IT Stage - GatingPolicy				x																												
CCO's Procurement Documentation and Records Management Procedure																			x													
CCO's Procurement of Goods and Services Policy																			x													
CCO's Statement of Information Practices			x																													
CCO's Template Schedule for Third Party Agreements																			x	x												
CCO's Digital Media Disposal Guideline	x																															

IPC Requirements

Privacy: IPC Requirement 1: Privacy policy in respect of CCO's status as a Prescribed Person.

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of PHI within its custody, including information contained in the OCSR. A main component of the CSP's Privacy Program (which manages the OCSR) is the Privacy Policy. The CSP is governed by CCO's Privacy policy and is supported by CSP specific policies and procedures that provide additional information on the Privacy Principle in the CSP context and how it is operationalized.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CSP's Data Request Procedure*, Privacy & Access Office
3. *CCO's De-identification Guidelines,* Privacy & Access Office and Chief Information Officer (**CIO**)
4. *CCO's Data Steward, Terms of Reference*, Privacy & Access Office
5. *CCO's Digital Media Disposal Guidelines,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 2: Policy and procedures for ongoing review of privacy policies, procedures and practices.

The current practice of the CCC program is to review its policies and associated procedures annually to ensure their operational effectiveness and ensure that they reflect both current legislative requirements and privacy best practices. This practice shall continue once the program is expanded to the CSP.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office
3. *CCO's Logging, Monitoring and Auditing Standard,* EISO
4. *Privacy & Access Office Operational Manual,* Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 3: Policy on the transparency of privacy policies, procedures and practices.

CCO provides information on CCC's Privacy Program and its privacy policies, procedures and practices, to the organization, the public and other stakeholders, through a variety of means including, the CCC web pages on CCO's internal and public websites, CCO's Statement of Information Practices, as well as newsletters, updates and other privacy awareness initiatives. Preparations are in place for the rebranding of the CCC web pages and other communications tools related to the CSP for September 2011. These communications vehicles will be used to post the updated privacy policy, procedures and practices.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Privacy FAQs*, Privacy & Access Office – Name change to CSP's Privacy FAQs with expanded program launch.
3. *CCO's Statement of Information Practices*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 4: Policy and procedures for the collection of PHI

CSP policies and procedures articulate its commitment to limit the collection of PHI to only that which is permitted by PHIPA and to only that which is necessary. The policies and procedures identified below meet this commitment by setting out criteria for identifying the purposes for the collection of PHI, the review and approval processes for the collection of PHI and the conditions or restrictions that must be satisfied prior to the collection of PHI.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office –Name change to CSP's Privacy Breach Management Procedure with expanded program launch.
3. *CCO's Privacy Audit and Compliance Standard, Privacy & Access Office*
4. *CCO's Data Steward, Terms of Reference*, Privacy & Access Office
5. *CCO's Data Sharing Agreement Standard*, Privacy & Access Office
6. *CCO's Data Sharing Agreement Procedure*, Privacy & Access Office
7. *CCO's Data Sharing Agreement Template,* Privacy & Access Office
8. *CCO's Data Sharing Agreement Initiation Form,* Privacy & Access Office
9. *CCO's Preliminary Privacy Assessment Form,* Privacy & Access Office
10. *CCO's IM/IT Stage-Gating Policy, CIO*

The following measures are currently being implemented by CSP to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 5: List of data holdings containing PHI.

CSP has in place an up-to-date list and brief description of the data holdings of PHI which it maintains. This list is appended to the *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition and is publically available for review at http://cancercare.on.ca/common/pages/UserFile.aspx?fileId=13632.The following document outlines CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 6: Policy and procedures for statements of purpose for data holdings containing PHI.

The CSP has in place policies and procedures which require that statements of purpose for all data holdings containing PHI be created, reviewed, amended and/or approved on an ongoing basis.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office

3. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office –Name change to CSP's Privacy Breach Management Procedure with expanded program launch.

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 7: Statements of Purpose for Data Holdings Containing PHI.

The CSP maintains a statement of purpose for each data holding containing PHI, identifying the purpose of the data holding, the PHI contained in the data holding, the source(s) of the PHI and the need for the PHI in relation to the identified purpose.

The following document outlines CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 8: Policy and procedures for limiting agent access to and use of PHI.

CCO ensures that access to PHI maintained by the CSP in the OCSR, is strictly limited in accordance with the "need to know" principle, where employees access and use only the minimum amount of identifiable information necessary for carrying out their job responsibilities.

CCO's comprehensive access request and approval process must be followed before an individual is permitted access to data.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Access Control Procedure*, Privacy & Access Office – Name change to CSP's Access Control Procedure with expanded program launch..
3. *CCO's Online Direct Data Access Request Form*, CIO
4. *CCO's Media Destruction Policy*, EISO
5. *CCO Employee Exit Process*, Human Resources
6. *CCO's Direct Data Access Audit Procedure*, Privacy & Access Office and CIO
7. *CCO's Chief Data Steward, Terms of Reference*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 9: Log of agents granted approval to access and use PHI.

The CSP relies on CCO for log management. CCO maintains a log of users who are granted approval to access and use PHI to prevent against unauthorized access, use and disclosure of PHI. The Online Direct Data Access Request (**ODDAR**) tool logs internal uses and access to PHI (non-research).
The following document outlines CCO's compliance with this requirement:

1. *Online Direct Data Access Request Form,* CIO
2. *Online Direct Data Access Request Tool,* CIO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

***Privacy: IPC Requirement 10*:** Policy and procedures for the use of PHI for research.

All research undertaken at CCO, per section 44 of PHIPA, is considered a disclosure of PHI to the researcher regardless of whether the researcher is a CCO employee or an external party (non-CCO employee) and is not considered by CCO to be a use of PHI for research purposes.

All research requests for PHI must be accompanied by a Research Ethics Board (**REB**) approval; a research plan; and an Application for Disclosure for Information from CCO for Research Purposes, which sets out the terms and conditions that a researcher must abide by when using the PHI disclosed by CCO for research purposes. This application, along with the CCO Non-disclosure/Confidentiality Agreement forms the agreement between CCO and a researcher.

As such, this requirement is not applicable to CCO. Please see Requirement 13 - *Policies and Procedures for Disclosures of Personal Health Information for Research Purposes and the Execution of Research Agreements.*

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
N/A					

***Privacy: IPC Requirement 11*:** Log of approved uses of PHI for research.

CCO does not log all approved uses of PHI for research, as all research undertaken at CCO, per section 44 of PHIPA, is considered a disclosure of PHI to the researcher regardless of the researcher being a CCO employee or an external party (non-CCO employee) and is not considered by CCO to be a use of PHI for research purposes.

However, CCO does log all approved disclosures of PHI for research purposes. Please see Requirement 15 – *Log of Research Agreements*.

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
N/A					

***Privacy: IPC Requirement 12*:** Policy/procedure for disclosure of PHI for purposes other than research

CCO is committed to ensuring the data access processes and procedures related to disclosures of PHI from the OCSR, for purposes other than research, is in accordance with PHIPA, its Regulation and CSP's Privacy Policy. CCO has a comprehensive data request process in place to be utilized by all individuals requesting access to PHI for purposes other than research. The documents listed below identify the process, including the documentation that must be completed, submitted, reviewed or executed by all responsible parties and committees.

The following documents outline CCO's compliance with this requirement:

1. *CCC's Data Request Procedure*, Privacy & Access Office – Name change to CSP's Data Request Procedure with expanded program launch.
2. *CCO's Privacy Audit and Compliance Standard,* Privacy & Access Office
3. *CCO's Business Process for Data Requests*, CIO
4. *CCO's De-Identification* Guidelines, Privacy & Access Office and CIO
5. *CCO's Data Sharing Agreement Template*, Privacy & Access Office
6. *CCO's Data Sharing Agreement Standard*, Privacy & Access Office
7. *CCO's Data Sharing Agreement Procedure* Privacy & Access Office
8. *CCO's Data Sharing Agreement Initiation Form,* Privacy & Access Office
9. *CCO's Decision Criteria for Data Requests*, CIO
10. *CCO's Media Destruction Policy & Procedure,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 13: Policy/procedure for disclosures of PHI for research purposes and the execution of research agreements.

At CCO, all research requests for PHI must be accompanied by REB approval; a research plan; and an Application for Disclosure for Information from CCO for Research Purposes, which sets out the terms and conditions that a researcher must abide by when using the PHI disclosed by CCO for research purposes. This application, along with CCO's Non-disclosure/Confidentiality Agreement, forms the agreement between CCO and a researcher.

The following documents outline CCO's compliance with this requirement:

1. *CCC's Data Request Procedure*, Privacy & Access Office – Name change to CSP's Data Request Procedure with expanded program launch.
2. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office – Name change to CSP's Privacy Breach Management Procedure with expanded program launch..
3. *CCO's Privacy Audit and Compliance Standard,* Privacy & Access Office
4. *CCO's Business Process for Data Requests,* CIO
5. *CCO's Application for Disclosure of Information from CCO for Research Purposes,* CIO
6. *CCO's Non-Disclosure/Confidentiality Agreement,* CIO
7. *CCO's Decision Criteria for Data Requests,* CIO
8. *CCO's Information Management Coordinator, Terms of Reference,* CIO
9. *CCO's Data Access Committee, Terms of Reference,* CIO
10. *CCO's De-Identification Guidelines,* Privacy & Access Office and CIO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 14: Template Research agreements.

CCO has a comprehensive data request process in place to be utilized by all researchers requesting access to PHI, de-identified or aggregate information, contained in the Colorectal Cancer Screening Registry, for research purposes. The research agreement sets out the responsibilities of the researcher and CCO when PHI is disclosed by CCO. This agreement demonstrates CCO's commitment towards preventing unauthorized disclosure of PHI.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Application for Disclosure of Information from CCO for Research Purposes,* CIO
2. *CCO's Non-Disclosure/Confidentiality Agreement,* CIO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 15: Log of research agreements

The *Microsoft Access Data Access Management Tool* maintains a log of executed Research Agreements between CCO and all researchers.

The following document outlines CCO's compliance with this requirement:

1. *Microsoft Access Log,* CIO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 16: Policy and Procedures for the execution of data sharing agreements.

Through its data sharing agreement processes, CCO demonstrates its commitment to ensuring that all data exchanges involving data from the CCSR (to be renamed CSP) between CCO and a third party are done so in accordance with PHIPA and privacy best practices.
The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy Audit and Compliance Standard,* Privacy & Access Office
3. *CCO's Data Sharing Agreement Standard*, Privacy & Access Office
4. *CCO's Data Sharing Agreement Procedure*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 17: Template data sharing agreements.

CCO's template data sharing agreements specify the terms and conditions to be included in each data sharing agreement executed by CCO when collecting or disclosing PHI for purposes

other than research. These agreements demonstrate CCO's commitment towards preventing unauthorized collection, use or disclosure of PHI.

The following policies outline compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Data Sharing Agreement Template*, Privacy & Access Office
3. *CCO's Data Sharing Agreement Standard*, Privacy & Access Office
4. *CCO's Data Sharing Agreement Procedure*, Privacy & Access Office
5. *CCO's Data Sharing Agreement Initiation Form*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 18: Log of data sharing agreements

CCO maintains a log of all DSAs in place with external parties, including DSAs that pertain to the collection or disclosure of PHI in the Ontario Cancer Screening Registry.

The following document outlines CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Data Sharing Agreement Procedure*, Privacy & Access Office
3. *CCO's Data Sharing Agreement Summary Chart,* Legal Department

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance	CCO	Status	Comments

Requirement	Enhancement	Scheduled	In Progress	N/A	
All requirements have been met.					

***Privacy: IPC Requirement 19*:** Policy and procedures for executing agreements with third party service providers in respect of PHI.

CCO requires that written agreements, with the appropriate privacy provisions, be entered into with third parties prior to permitting access to and use of PHI. These documents ensure that third parties access and use data in accordance with CCO privacy and security policies and that retention and disposal requirements are being met within the required time frame.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Procurement of Goods and Services Policy*, Procurement Office
3. *CCC's Access Control Procedure,* Privacy & Access Office – Name change to CSP's Access Control Procedure with expanded program launch.
4. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office
5. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office – Name change to CSP's Privacy Breach Management Procedure with expanded program launch..
6. *CCO's Procurement Documentation and Records Management Procedure*, Procurement Office
7. *Privacy & Access Operational Manual*, Privacy & Access Office
8. *CCO's Template Schedule for Third Party Agreements,* Legal Department
9. *CCO's Information Classification and Handling Guideline* (Draft), EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 20: Template agreement for all third party service providers.

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of PHI within its custody and within the custody of third parties retained by CCO. It meets this commitment through the inclusion of the appropriate privacy provisions in its template agreement for all third party service providers, in addition to incorporating privacy and security related provisions and responsibilities as required on an ongoing basis.

The following document outlines CCO's compliance with this requirement:

1. *CCO's Template Schedule for Third Party Agreements,* Legal Department

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 21: Log of agreements with third party service providers.

CCO maintains a log of all agreements with third party service providers through its Contract Management System.

The following document outlines CCO's compliance with this requirement:

1. *Contract Management System*, Procurement Office
2. *CCO's Privacy & Access Office Remediation Program – Log of Third Party Service Providers with Access to PHI*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 22: Policy and procedures for the linkage of records of PHI

At CCO, all linkages of records of PHI are performed in accordance with PHIPA, CCO and CSP privacy policies and the terms and conditions of agreements in place with data providers.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Data Linkage Standard,* CIO

2. *CCO's Data Linkage Procedure,* CIO

3. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office – Name change to CSP's Privacy Breach Management Procedure with expanded program launch.

4. *CCO's Privacy Audit and Compliance Standard,* Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 23: Log of approved linkages of records of PHI

CCO maintains a List of Data Linkages which tracks the number of approved data linkages. The List includes the category of requestor, the date the linkage was approved and the nature of the records of PHI linked.

The following document outlines CCO's compliance with this requirement:

1. *List of Data Linkages,* CIO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 24: Policy/procedures with respect to de-identification and aggregation

CCO is committed to providing de-identified and / or aggregate information, rather than PHI, to requesting parties if the de-identified and / or aggregate information serves the identified purpose. CCO meets this commitment by conducting a thorough review of all data requests and the purpose for which the data is to serve, in addition to reviewing the data that is to be disclosed to determine if it is reasonably foreseeable that the information could be utilized, either alone or with other information, to identify an individual.

The following documents comply with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Data Request Procedure*, Privacy & Access Office – Name change to CSP's Data Request Procedure with expanded program launch.
3. *CCO's De-Identification Guidelines*, Privacy & Access Office and CIO
4. *CCO's Business Process for Data Requests*, CIO
5. *CCO's Privacy & Security Acknowledgment form*, Privacy & Access Office
6. *CCO's Decision Criteria for Data Requests*, CIO
7. *CCO's Privacy Audit and Compliance Standard,* Privacy & Access Office

8. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office – Name change to CSP's Privacy Breach Management Procedure with expanded program launch.

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

***Privacy: IPC Requirement 25*:** PIA policy and procedures.

CCO has policies in place to identify the circumstances in which Privacy Impact Assessments (**PIA**s) are required. These policies provide clear direction on the scope of PIAs at CCO, the responsibility for conducting PIAs and the process for implementing recommendations arising from completed PIAs. All new initiatives and changes to existing projects are reviewed to determine if a PIA is required to identify the privacy risks and appropriate mitigating strategy.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy Impact Assessment Standard*, Privacy & Access Office
3. *CCO's Privacy & Access Office Remediation Program – Log of Privacy Impact Assessments*, Privacy & Access Office
4. *CCO's Privacy Audit and Compliance Standard,* Privacy & Access Office
5. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office –Name change to CSP's Privacy Breach Management Procedure with expanded program launch.

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 26: Log of PIAs

CCO maintains a log of all PIAs which have been undertaken to ensure that identified privacy risks are tracked and mitigated in a timely manner.
The following documents outline compliance with this requirement:

1. *CCO's Privacy & Access Office Remediation Program – Log of Privacy Impact Assessments*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 27: Policy and procedures in respect of privacy audits

Privacy audits are a key component of CCO's and the CSP's overall Privacy Program. In order for CCO to protect the privacy and confidentiality of the PHI it receives, privacy audits are conducted to ensure there is no unauthorized access, use or disclosure of PHI.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office
3. *Privacy & Access Office Operational Manual,* Privacy & Access Office

4. *CCO's Logging, Monitoring and Auditing Standard,* EISO

The Privacy Audit and Compliance program will be reviewed and updated as required to align with the objectives of the new enterprise risk management framework to be developed and implemented in 2011.

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 28: Log of privacy audits

CCO maintains an up-to-date and accurate log of all privacy audits conducted at the program and business unit and enterprise level.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office
2. *Privacy & Access Office Remediation Program*, Privacy & Access Office

The Privacy Audit and Compliance program will be reviewed and updated as required to align with the objectives of the new enterprise risk management framework to be developed and implemented in 2011.

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 29: Policy and procedures for privacy breach management

CSP policies stipulate that it is mandatory to report all privacy breaches or suspected privacy breaches. CSP's Privacy Breach Management Procedure clearly defines the identification, reporting, containment, notification, investigation and remediation processes to be followed when a privacy breach or suspected privacy breach has occurred.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office –Name change to CSP's Privacy Breach Management Procedure with expanded program launch.
3. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office
4. *CCO's Privacy Breach Report Form*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 30: Log of privacy breaches

CSP maintains a comprehensive log of all privacy breaches, including suspected privacy breaches that occur.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office – Name changed to CSP's Privacy Breach Management Procedure as of September 2011
3. *CCO's Privacy & Access Office Remediation Program – CSP's Privacy Breach Log*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Privacy: IPC Requirement 31: Policy and procedures for privacy complaints

CSP reviews and responds to all complaints from the public, on its information practices and/or its compliance with PHIPA. Through the use of its privacy complaints processes, the public is encouraged to contact CCO and have the appropriate measures taken when responding to the complaint.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Privacy Inquiries and Complaints Procedure*, Privacy & Access Office – Name change to CSP's Privacy Inquiries and Complaints Procedure with expanded program launch.
3. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office – Name change to CSP's Privacy Breach Management Procedure with expanded program launch.
4. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 32: Log of privacy complaints

CSP maintains a log of all privacy complaints.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Privacy Inquiries and Complaints Procedure*, Privacy & Access Office – Name change to CSP's Privacy Inquiries and Complaints Procedure with expanded program launch.
3. *Privacy & Access Office Remediation Program - CCC's Log of Privacy Complaints and Inquiries*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Privacy: IPC Requirement 33: Policy and procedures for privacy inquiries

CSP reviews and responds to all inquiries from the public, on the information practices of the CSP and/or its compliance with PHIPA. Through the use of its privacy inquiries processes, the public is encouraged to contact CCO and have the appropriate measures taken when responding to the inquiry.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Privacy Inquiries and Complaints Procedure*, Privacy & Access Office – Name change to CSP's Privacy Inquiries and Complaints Procedure with expanded program launch.
3. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office –Name change to CSP's Privacy Breach Management Procedure with expanded program launch.

4. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

PART 2: SECURITY DOCUMENTATION

Security Documentation Matrix

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Acceptable Use of Social Media Policy	x													x				
Access Card Procedure																x		
Acquisition Development and Application Security Standard	x																	
Cryptography Standard						x	x											
EasyLobby Visitor Grid log				x														
KeyScan System Log				x														
Information Security Code of Conduct	x	x	x		x	x			x	x	x			x				
Data Sharing Agreement Procedure					x													
Data Sharing Agreements Standard					x													
Data Sharing Agreement Template					x													
Digital Media Disposal Guidelines								x										
Information Security Policy	x	x	x		x	x	x	x	x	x	x	x	x	x	x		x	
Information Security Framework	x														x	x		
Information Security Program Plan 2010-2011	x																	
Logging, Monitoring, and Auditing Standard	x	x					x		x	x				x	x			

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Log of Security Audits															x	x		
Logical Access Control Standard	x		x			x	x		x									
Operational Security Procedure: Patching											x							
Operational Security Standard								x			x				x	x		
Visitor Access Procedure			x															
Video Monitoring Standard			x															
Change Management Policy												x						
Change Management Process												x						
Data Backup Policy	x				x								x					
IM/IT Stage-Gating Process and Project Management Lifecycle Methodology	x																	
New Employee Facilities & Information Technology Services Form			x	x														
Photo ID Request Form			x															
Employee Exit Process			x															
Employee Exit Checklist			x															
HP Data Protectors Session Logs					x								x					
Information Management Coordinator Terms of Reference					x													
Incident management Framework	x	x								x							x	
Authorization to Access Data Centre Employee Form			x															
Authorization to Access Data Centre Contractor Form			x															
Open Media Logs					x								x					

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Personal Action Form			x															
Provision of Paging and Mobile Phone with Email Devices						x												
Data Backup Process and Standard						x							x					
Data Center Access and Usage Policy			x															
Principle & Policies for the Protection of Personal Health Information at CCO															x			
Privacy & Access Office Operational Manual													x					
Privacy & Access Office Remediation Program					x													
Privacy Audit and Compliance Procedures					x													
CCC's Privacy Breach Management Procedure					x													
Threat Risk Assessment Template															x			
CCO's Template Schedule for Third Party Agreements					x			x					x					
Direct Data Access Procedure			x															
Application for Disclosure of Information From form CCO for Research Purposes					x													
Security Risk Management Standard															x	x		
Senior Team Lad Job Description															x			
Security Incident Tracking Spreadsheet																		x
Non-Disclosure Confidentiality Agreement					x													
Information Classification and Handling Standard					x	x	x						x					

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Information Classification and Handling Guideline					**x**	**x**	**x**						**x**					

IPC Requirements

Security: IPC Requirement 1: Information Security Policy.

CCO has implemented a broad overarching information security policy. This policy provides for a comprehensive information security program supporting administrative, technical, and physical controls consistent with established industry standards and practices.
The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Code of Conduct ,* EISO
3. *Acceptable Use of Social Media Policy* , EISO
4. *Logical Access Control Standard ,* EISO
5. *Logging, Monitoring and Auditing Standard ,* EISO
6. *Information Security Program Plan 2010-2011,* EISO
7. *IM/IT Stage-Gating Process and Project Lifecycle Management,* Project Management Office
8. *Data Backup Policy,* Technology Services
9. *Information Security Framework,* EISO
10. *Incident Management Framework,* EISO
11. *Acquisition Development and Application Security Standard,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 2: Policy and procedures for ongoing review of security policies, procedures and practices.

The entire body of the security policy framework is assessed over the span of a three year cycle. However, the reviews occur on an annual basis. These updates are done according to CCO corporate practices. The implementation of the program itself is an incremental and iterative process. Ongoing development allows CCO to maintain an acceptable level of organizational risk that evolves with changes in technology, industry practices or standards, business environments, and information security threats. Monitoring, measurement and metrics help guide the program improvements towards maturity.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Code of Conduct ,* EISO
3. *Logging, Monitoring and Auditing Standard,* EISO*,*
4. *Incident Management Framework,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 3: Policy and procedures for Ensuring Physical Security of Personal Health Information.

CCO's Facilities, Human Resources and Information Technology Services have put in place policies and procedures to ensure PHI is not stolen, lost, or used or accessed by unauthorized individuals. In addition, these departments have ensured there are controlled and varying levels of access to CCO premises which house PHI. CCO is committed to protecting the physical security of all information within CCO, especially highly confidential information including PHI.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Code of Conduct ,* EISO
3. *Logical Access Control ,* EISO
4. *Direct Data Access Procedure,* Privacy & Access Office and CIO

5. *New Employee Facilities & Information Technology Services Form,* Facilities Department
6. *Photo ID Request Form,* Human Resources
7. *Authorization to Access Data Centre Employee Form*, Technology Services
8. *Authorization to Access Data Centre Contractor Form*, Technology Services
9. *Data Center Access and Usage Policy,* Technology Services
10. *Employee Exit Checklist,* Human Resources
11. *Employee Exit Process ,* Human Resources
12. *Personal Action Form (PAF) ,* Human Resources
13. *Visitor Access Procedure*, Facilities Department
14. *Video Monitoring Standard,* Facilities Department
15. *Privacy Audit and Compliance Standard*, Privacy & Access Office
16. *Access Card Procedure,* Facilities Department

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Security: IPC Requirement 4: Log of agents with access to the premises of CCO.

CCO maintains a comprehensive log of all accesses to its premises by visitors and CCO employees.

The following documents outline CCO's compliance with this requirement:

1. *New Employee Facilities & Information Technology Services Form*, Facilities Department and Technology Services.
2. *EasyLobby Visitor Grid Log,* Facilities Department
3. *KeyScan System Log,* Facilities Department

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 5: Policy and Procedures for Secure Retention of Records of PHI.

The secure retention of PHI in either paper or electronic format is managed internally through the Information Security Policy, the Information Security Code of Conduct, and appropriate agreements. Third party retention of PHI is limited to the off-site retention of backup tapes where the applicable security requirements are enforced through CCO's Data Backup Policy, Data Backup Process and Standard, Template Schedule for Third Party Agreements and the agreement with the third party service provider.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Code of Conduct,* EISO
3. *Information Management Coordinator Terms of Reference,* CIO
4. *Non-Disclosure/Confidentiality Agreement,* CIO
5. *Application for Disclosure of Information from CCO for Research Purposes,* CIO
6. *Data Sharing Agreement Template,* Privacy & Access Office
7. *Data Sharing Agreement Procedure,* Privacy & Access Office

8. *Data Sharing Agreement Standard,* Privacy & Access Office
9. *CCO's Template Schedule for Third Party Agreements,* Legal Department
10. *Privacy Audit and Compliance Standard,* Privacy & Access Office
11. *CCC's Privacy Breach Management Procedure, Privacy & Access Office – Name change to CSP's Privacy Breach Management Procedure* with expanded program launch.
12. *Data Back-up Policy,* Technology Services
13. *Data Back-up Process and Standard,* Technology Services
14. *Open Media Logs,* Technology Services
15. *HP Data Protectors Session Logs,* Technology Services
16. *Privacy & Access Office Remediation Program – Log of Third Party Service Providers with Access to PHI.*
17. *Information Classification and Handling Standard* (Draft), *EISO*
18. *Information Classification and Handling Guideline* (Draft), EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 6: Policy and Procedures for Secure Retention of Records of PHI on Mobile Devices.

EISO is in the process of undertaking an extensive review to update its mobile and remote access standards to ensure full compliance with this requirement. EISO will complete this review and develop the appropriate documentation by the end of September 2011. In the interim, CCO has in place policies and standards which identify why records containing PHI must be safeguarded on mobile devices. CCO's Information Security Code of Conduct and Information Classification and Handling Standard and Guideline provide guidance to its employees on the secure handling of PHI on mobile media.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Code of Conduct ,* EISO
3. *Logical Access Control Standard ,* EISO
4. *Cryptography Standard,* EISO
5. *Provision of Paging and Mobile Phone with Email Devices ,* Technology Services
6. *Information Classification and Handling Standard* (Draft), EISO
7. *Information Classification and Handling Guideline* (Draft), EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
Secure retention of PHI on mobile devices (and all sub requirements as outlined in the manual).	CCO is undertaking a review of its mobile and remote access standards to address regulatory requirements. This update will facilitate compliance with this section. Development of *Remote Access Standard*		√		Completion Date: 2012

Security: IPC Requirement 7*:* Policy and Procedures for Secure Transfer of Records of PHI.

The security requirements for the secure transfer of PHI, specifically with external parties, are managed through Data Sharing Agreements and other third party service provider agreements. For internal control, CCO has documented standards for the use of cryptographic technologies and logical access controls. Collectively, these standards and agreements provide for a technical and administrative framework that supports the secure transfer of confidential information, including PHI.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Cryptography Standard ,* EISO
3. *Logical Access Control Standard ,* EISO
4. *Logging, Monitoring and Auditing Standard ,* EISO
5. *Information Classification and Handling Standard* (Draft), EISO
6. *Information Classification and Handling Guideline* (Draft), EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
Outline the procedures that must be followed in transferring records of PHI through each of the approved methods. This includes: – A discussion of the conditions pursuant to which records of PHI will be transferred – The agent(s) responsible for ensuring the secure transfer – Any documentation that is required to be completed, provided and/or executed in relation to the secure transfer – The agent(s) responsible for completing, providing and/or executing the documentation – And the required content of the documentation.	Development of corresponding guidelines and procedures in order to facilitate implementation of the related standards. Development of procedures and technical capability for the logging and monitoring of transfers.		√		Completion Date: 2012

– Whether the agent transferring records of PHI is required to document the date, time and mode of transfer – The recipient of the records of PHI – And the nature of the records of PHI transferred – Address whether confirmation of receipt of the records of PHI is required from the recipient – The manner of obtaining and recording acknowledgement of receipt of the records of PHI and the agent(s) responsible for doing so					

Security: IPC Requirement 8: Policy and Procedures for Secure Disposal of Records of PHI.

CCO currently has in place practices that address the secure disposal of PHI on its premises. Additionally, CCO employees receive training on the correct method for destruction and disposal of PHI in either paper or electronic formats. These practices are now being formalized in a procedural document to reflect new vendor arrangements, technologies, and regulatory guidelines. This enhancement of existing practices will be finalized by the end of September 2011.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Operational Security Standard ,* EISO
3. *Digital Media Disposal Guideline,* EISO
4. *CCO's Template Schedule for Third Party Agreements,* Legal Department

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance	CCO Enhancement	Status	Comments

Requirement		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 9: Policy and Procedures Relating to Passwords.

CCO has implemented policies and procedures with respect to supporting passwords for authentication to information systems, equipment, resources, applications and programs. These policies and procedures represent a foundation from which technical controls are implemented, including controls to identify, authenticate, and authorize users and systems accessing CCO information resources.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Logical Access Control Standard ,* EISO
3. *Information Security Code of Conduct ,* EISO
4. *Logging, Monitoring and Auditing Standard ,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 10: Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs.

CCO has implemented a system for the creation, maintenance and ongoing review of system control and audit logs that are consistent with evolving industry standards and that are commensurate with the amount and sensitivity of the personal health information maintained,

with the number and nature of agents with access to personal health information and with the threats and risks associated with the personal health information.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Code of Conduct ,* EISO
3. *Logging, Monitoring and Auditing Standard ,* EISO
4. *Incident Management Process Framework,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 11: Policy and Procedure for Patch Management.

CCO has standard operating practices for patch management. These practices provide baseline patching of operating systems and applications. The EISO will continue to implement support tools for managing software on desktops and servers. Technology and process enhancements to patching are implemented on a regular basis, with enhancements to meet regulatory requirements planned for implementation by the end of September 2011.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Code of Conduct,* EISO
3. *Operational Security Standard,* EISO
4. *Operational Security Procedure: Patching,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Security: IPC Requirement 12: Policy and Procedures Related to Change Management.

CCO has implemented change management practices based on alignment to the Information Technology Infrastructure Library **(ITIL)** standards for service management. CCO's previously reviewed practices include a well-established Change Advisory Board **(CAB)**, which oversees the introduction of changes into CCO's technical environment. The CAB membership includes Technology Services, Information Security, Privacy and business unit representation. .

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Change Management Policy*, Technology Services
3. *Change Management Process*, Technology Services

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 13: Policy and Procedures for Back-Up and Recovery of Records of PHI.

CCO has implemented operational policies and procedures for the back-up and recovery of records of PHI. These documents in conjunction with the third party service provider

agreements address administrative processes, technical practices for backups and data recovery, and the controls relevant to the off-site storage of backup media.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Data Backup Policy,* Technology Services
3. *CCO's Template Schedule for Third Party Agreements,* Legal Department
4. *HP Data Protector Session Logs,* Technology Services
5. *Data Backup Process Standard,* Technology Services
6. *Open Media Logs*, Technology Services and Third Party Service Provider
7. *Privacy & Access Office Operational Manual,* Privacy & Access Office
8. *Information Classification and Handling Standard* (Draft), EISO
9. *Information Classification and Handling Guideline* (Draft), EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Security: IPC Requirement 14: Policy and Procedures on the Acceptable Use of Technology.

CCO has implemented policies and practices outlining the acceptable use of information systems, technologies, equipment, resources, applications and programs. These policies are complemented by both online and in person training sessions to ensure CCO employees understand the appropriate use of technology.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Code of Conduct ,* EISO

3. *Acceptable Use of Social Media Policy* , EISO
4. *Logging, Monitoring and Auditing Standard ,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 15: Policy and Procedures In Respect of Security Audits.

CCO has put in place standards and practices that outline the types of security audits that are required to be conducted. These practices include review of compliance with the security policies, procedures and practices; threat and risk assessments; security reviews or assessments; and technical vulnerability assessments; penetration testing and ethical hacks (when appropriate) and reviews of system control and audit logs. The EISO plans to augment the existing process documents and templates to fully meet the specifics of IPC review manual requirements for the end of September 2011.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Information Security Framework,* EISO
3. *Logging, Monitoring, and Auditing Standard ,* EISO
4. *Security Risk Management Standard,* EISO
5. *Operational Security Standard,* EISO
6. *Principles & Policies for the Protection of Personal Health Information at Cancer Care Ontario, 4th edition,* Privacy & Access Office
7. *Threat Risk Assessment Template,* EISO
8. *Log of Security Audits,* EISO
9. *Senior Team Lead Job Description,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 16: Log of Security Audits.

CCO is in the process of updating its risk management processes, including tools for risk tracking and remediation tracking (risk register). The EISO will continue security operational process development to implement operational assurance activities. As well, there are planned enhancements for the existing process documents and templates to meet regulatory requirements. It is anticipated that the initial work to establish a system for tracking risk findings will be in place for September 2011.

The following documents outline CCO's compliance with this requirement:

1. *Security Risk Management Standard, EISO*
2. *Operational Security Standard*, EISO
3. *Information Security Framework*, EISO
4. *Log of Security Audits,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 17: Policy and Procedures for Information Security Breach Management.

EISO has implemented practices for the identification, reporting, containment, notification, investigation and remediation of information security incidents. These existing and reviewed practices will be bolstered this year by improvements to the administrative policies and incident tracking methods. This work has synergy with the security and privacy auditing and logging technologies that are currently being implemented. Planned enhancements to the information security incident management policy are scheduled to be completed by the end of September 2011.

The following documents outline CCO's compliance with this requirement:

1. *Information Security Policy* , EISO
2. *Incident Management Framework,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Security: IPC Requirement 18: Log of Information Security Breaches.

CCO has implemented practices for the identification, reporting, containment, notification, investigation and remediation of information security incidents. An enhancement of EISO's logging practices is scheduled to be completed by the end of September 2011.

The following documents outline CCO's compliance with this requirement:

1. *Security Incident Tracking Spreadsheet*, EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Part 3: HUMAN RESOURCES DOCUMENTATION

Human Resources Documentation Matrix

CCO Human Resources Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11
CCO's Code of Conduct											x
CCO's Privacy Audit & Compliance Standard	x		x								
CCO's Confidentiality Policy					x						
CCO's Contract Management System							x				
CCO's Employee Exit Process										x	
CCO's Employee Exit Checklist										x	
CCO's Information Security Code of Conduct			x	x							
CCO's Information Security Policy			x	x							
CCO's Intranet-Human Resources Workflow: How Do I Hire a new Employee?					x						
CCO's Personnel Action Form					x					x	
CCO's Privacy & Access Office Operational Manual	x										

CCO Human Resources Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11
CCO's Privacy & Access Office Remediation Program	**x**	**x**		**x**							
CCO's Privacy and Security Training and Awareness Procedure	**x**	**x**	**x**								
CCO's Privacy & Security eLearning Module						**x**	**x**				
CCC's Privacy Breach Management Procedure	**x**										**x**
Principles and Policies for the Protection of Personal Health Information at CCO	**x**	**x**	**x**								
CCC's Privacy Training Curriculum	**x**										
CCO's Privacy Training Curriculum	**x**										
CCO's Procurement of Goods and Services Policy					**x**						
CCO's "Progressive Discipline" Policy											**x**
CCO's Secondment Policy					**x**						
CCO's Security Training Curriculum			**x**								
CCO's Statement of Confidentiality						**x**					
CCO's Template Schedule for Third Party Agreements						**x**					
CCO's Termination Monthly Reports										**x**	
CCO's Unpaid Student Intern Policy					**x**						

CCO Human Resources Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11
CCO's VIP Payroll System							**x**				
Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program								**x**			
Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program									**x**		

IPC Requirements

Human Resources Requirement 1 : Policy and procedures for privacy training and awareness

CCO has a comprehensive privacy training and awareness program in place to ensure that all employees are aware of CCO privacy policies, procedures and best practices. Through the new employee privacy and security training program and the annual privacy and security refresher training program, all CCO employees, consultants, contractors, students, researchers and volunteers are informed of their privacy and security responsibilities, in addition to CCO's legislative compliance obligations. Additionally, the CSP provides an supplementary training module to all of its employees, to highlight the privacy procedures specific to the screening program. This ensures that all users of CCO systems, including systems containing PHI, have received the requisite privacy and security training. CCO's extensive training and awareness program plays a key role in fostering a culture of privacy and security in the organization.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy & Security Training and Awareness Procedure*, Privacy & Access Office
3. *CCO's Privacy Training Curriculum*, Privacy & Access Office
4. *CCC's Privacy Training Curriculum,* Privacy & Access Office – Name change to CSP's Privacy Training Curriculum with expanded program launch.
5. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office –Name change to CSP's Privacy Breach Management Procedure with expanded program launch.
6. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office
7. *Privacy & Access Office Operational Manual,* Privacy & Access Office
8. *Privacy & Access Office Remediation Program – Log of Privacy and Security Training Completion*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Human Resources Requirement 2: Log of attendance at initial privacy orientation and ongoing privacy training

CCO tracks completion of its privacy training program through the electronic acceptance of a Privacy and Security Acknowledgement form.

The following document outlines CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy & Security Training and Awareness Procedure*, Privacy & Access Office
3. *CCO's Privacy & Access Office Remediation Program – Log of Privacy and Security Training Completion*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Human Resources: IPC Requirement 3: Policy and procedures for security training and awareness.

CCO has a comprehensive security training and awareness program in place to ensure that all employees are aware of CCO security policies, procedures and best practices. Through the new employee privacy and security training program and the annual privacy and security refresher training program, all CCO employees, consultants, contractors, students, researchers and volunteers, are informed of their security responsibilities and obligations. This ensures that all users of CCO systems, including systems containing PHI, have received the requisite security

training. CCO's extensive training and awareness program plays a key role in fostering a culture of privacy and security in the organization.
The following documents outline compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy and Security Training and Awareness Procedure*, Privacy & Access Office
3. *CCO's Information Security Policy,* EISO
4. *CCO's Information Security Code of Conduct,* EISO
5. *CCO's Security Training Curriculum*, EISO
6. *CCO's Privacy Audit and Compliance Standard*, Privacy & Access Office
7. *Privacy & Access Office Remediation Program – Log of Privacy and Security Training Completion*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Human Resources: IPC Requirement 4: Log of attendance at initial security orientation and ongoing security training.

CCO tracks completion of its security training program through the electronic acceptance of a Privacy and Security Acknowledgement form.

The following documents outline compliance with this requirement:

1. *CCO's Information Security Policy,* EISO
2. *CCO's Information Security Code of Conduct,* EISO
3. *CCO's Privacy & Access Office Remediation Program – Log of Privacy and Security Training Completion,* Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met					

Human Resources: IPC Requirement 5: Policy and Procedure for the Execution of Confidentiality Agreement with Agents.

CCO ensures that the Confidentiality obligations for each individual representing it are clearly articulated at the outset of engagement with the organization. Agreements are in place for all individuals working for or under contract with CCO, which clearly outline the importance of preserving the confidentiality of all information of a private or sensitive nature, including all PHI.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Confidentiality Policy*, Privacy & Access Office and Human Resources
2. *CCO's Personnel Action Form*, Human Resources
3. CCO's Intranet - Human Resources Workflow: *How do I hire a new employee*?[1], Human Resources
4. *CCO's Procurement of Goods and Services Policy*, Procurement Office
5. *Secondment Policy,* Human Resources
6. *Unpaid Student Intern Policy,* Human Resources

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

[1] Available on CCO's Intranet Site – Human Resources page: https://ecco.cancercare.on.ca/Divisions/HRFinance/HR/PoliciesAndProcedures/hdi_hire_new_employee.aspx

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Human Resources: IPC Requirement 6: Template Confidentiality Agreement with Agents.

CCO's has put in place administrative safeguards to ensure that CCO employees, representatives and third parties under contract with CCO, will meet their obligations to protect confidential information, including PHI, to which they may have access in the course of performing their job duties.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Statement of Confidentiality*, Human Resources
2. *CCO's Template Schedule for Third Party Agreements,* Legal Department
3. *Privacy & Security eLearning Module,* Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Human Resources: IPC Requirement 7: Log of Executed Confidentiality Agreements with Agents.

CCO's Human Resources Department maintains a log of confidentiality agreements executed by employees of CCO. Agreements executed by third parties retained by CCO, with access to PHI, include a template schedule outlining the third party's confidentiality obligations in respect of the PHI. A log of agreements is maintained by CCO's Procurement Office.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Contract Management System*, Procurement Office
2. *CCO's VIP Payroll System*, Human Resources
3. *Privacy & Security eLearning Module,* Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Human Resources: IPC Requirement 8: Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program

CCO has in place an effective governance structure including delegated roles to carry out the Privacy Program at CCO.

The following documents outline compliance with this requirement:

1. *Director, Privacy & Access Job Description (Management)*, Privacy & Access Office
2. *Privacy Team Lead Job Description*, Privacy & Access Office
3. *Privacy Specialist Job Description*, Privacy & Access Office
4. *Senior Privacy Specialist Job Description*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Human Resources: IPC Requirement 9: Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program

CCO has in place an effective governance structure including delegated roles to carry out the Security Program at CCO.

The following documents outline CCO's compliance with this requirement:

1. *Senior Team Lead Job Description,* EISO
2. *Intermediate Information Security Specialist Job Description*, EISO
3. *Senior Information Security Specialist/Security Architect Job Description,* EISO
4. *Associate Information Security Specialist Job Description*, EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Human Resources: IPC Requirement 10: Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship.

The process that is followed at CCO upon termination or cessation of the employment, contractual or other relationship is outlined in several documents. The policies and procedures listed below ensure that when an employee, volunteer or third party relationship with CCO ends, all access privileges to CCO's systems and premises are terminated, and all property including records of PHI, access cards and keys are returned in a timely fashion. CCO is enhancing its existing system and processes to embed the appropriate controls which will ensure all requirements are met upon termination of an employment or contractual relationship with CCO.

The following documents outline compliance with this requirement:

1. *CCO's Employee Exit Process*, Human Resources
2. *CCO's Employee Exit Checklist*, Human Resources
3. *CCO's Personnel Action Form*, Human Resources
4. *CCO's Termination of Employment Policy,* Human Resources

5. *CCO's Termination Monthly Reports,* Human Resources

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Human Resources: IPC Requirement 11: Policy and Procedures for Discipline and Corrective Action

CCO ensures that access to and use of PHI by its employees and third parties complies with its privacy and security policies and procedures, enforcement of which are supported by Human Resources and the Privacy & Access Office and through legal agreements with third parties under contract with CCO.

The following documents outline compliance with this requirement:

1. *CCO's Code of Conduct*, Human Resources
2. *CCO's Progressive Discipline Policy*, Human Resources
3. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office –Name change to CSP's Privacy Breach Management Procedure with expanded program launch.

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

PART 4: ORGANIZATIONAL AND OTHER DOCUMENTATION

Organizational and Other Documentation Matrix

CCO Organizational and Other Documentation Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8
CCO's Architecture Review Board Terms of Reference			x					
Business Continuity and Disaster Recovery Plan								x
Business Continuity and Discovery Recovery Test Strategy for 2011/2012								x
Business Continuity Service Framework								x
CCO Board of Directors Orientation Handbook		x						
CCO Privacy Audit & Compliance Standard						x		
CCO's Core Privacy Committee Terms of Reference			x					
CCC's Privacy Breach Management Procedure						x		
CCO's Information Security Policy		x	x					
CCO's Information Security Program Plan		x	x					
CCO's Privacy & Access Office Remediation Program					x	x	x	
CCO's Privacy & Access Office Operation Manual						x		
Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario, 4th edition	x		x					

CCO Organizational and Other Documentation Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8
CCO's Statement of Information Practices	**x**							
Summary of Annual Privacy Report to the Board of Directors	**x**							
Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program		**x**						
CCO's Information Security Framework		**x**						

IPC Requirements

Organizational and Other: IPC Requirement 1*:* Privacy governance and accountability framework.

CCO's privacy governance and accountability framework identifies the Chief Executive Officer as ultimately accountable for CCO's compliance with PHIPA and its Regulation as well as with all privacy policies, procedures and practices at CCO. The Chief Privacy Officer has been delegated day-to-day authority to manage the Privacy Program and is supported by the Privacy & Access Office in carrying out her duties. Significant Privacy Program initiatives, changes and updates to the Privacy Program are presented to the CCO Board of Directors. The Audit & Finance Committee of CCO's Board of Directors oversees the CCO Privacy Program. As of September 2011, this function will be transferred to the Strategic Planning, Performance & Risk Management Committee of the Board.

The following documents outline compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Statement of Information Practices*, Privacy & Access Office
3. *Summary of Annual Privacy Report to the Board of Directors,* Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Organizational and Other: IPC Requirement 2*:* Security Governance and Accountability Framework.

CCO's security policy outlines the CEO's accountability for ensuring the security of PHI as well as the appropriate delegation of day-to-day authority to manage the security program. The CCO Board of Directors Orientation Handbook includes briefing elements of both the Privacy and Security program. CCO's Executive Team and Board are apprised of the security program updates through the Chief Privacy Officer and Chief Information Officer briefing updates. The Audit & Finance Committee of CCO's Board of Directors oversees the CCO security program.

As of September 2011, this function will be transferred to the Strategic Planning, Performance & Risk Management Committee of the Board.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Information Security Policy*, EISO
2. *CCO's Information Security Program Plan 2010-2011,* EISO
3. *CCO Board of Directors Orientation Handbook,* Legal Department
4. *CCO's Information Security Framework,* EISO
5. *Senior Team Lead Job Description,* EISO

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Organizational and Other: IPC Requirement 3: Terms of Reference for committees with roles with respect to the Privacy Program and/or security program.

CCO has terms of reference for every committee that has a role in the Privacy Program. CCO's Core Privacy Committee, comprised of the Chief Privacy Officer, Privacy Office employees, EISO, and key members of CCO's information management team, supports the Privacy & Access Office in addressing significant privacy issues.

The following documents outline compliance with this requirement:

1. *CCO's Information Security Policy*, EISO
2. *CCO's Information Security Program Plan 2010-2011*, EISO
3. *CCO's Architecture Review Board Terms of Reference,* Technology Services
4. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office

5. *CCO's Core Privacy Committee Terms of Reference*, Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Organizational and Other: IPC Requirement 4: Corporate Risk Management Framework.

CCO has completed an enterprise wide risk identification activity which has been reported to the MOHLTC in December 2010. Areas of privacy risk include:

- Managing the conflicts between the *Freedom of Information and Protection of Privacy Act (***FIPPA**) and PHIPA for CCO in its various roles;
- The challenges of operating under multiple PHIPA authorities in order to effectively support the cancer system in Ontario; and
- Rolling out the new CCO Stage-Gating process (which includes various Privacy checkpoints) to all enterprise projects.

This risk identification activity demonstrates that CCO is currently aptly managing its Privacy related risks, with appropriate controls in place for the safeguarding of PHI.

The Privacy & Access Office has a Remediation Program in place, where privacy risks and remediation activities are logged. This program will be updated to align with the new enterprise risk management framework to be developed and implemented in 2011.

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
A corporate risk management framework (and all sub requirements as outlined in the manual)	Implementing a Privacy Risk Management Standard		√		Completion Date: 2012

Organizational and Other: IPC Requirement 5: Corporate Risk Register.

CCO has executed an enterprise wide risk identification activity which has been reported to the MOHLTC in December 2010. Areas of privacy risk include:

- Managing the conflicts between FIPPA and PHIPA for CCO in its various roles;
- The challenges of operating under multiple PHIPA authorities in order to effectively support the cancer system in Ontario; and
- Rolling out the new CCO Stage-Gating process (which includes various Privacy checkpoints) to all enterprise projects.

This risk identification activity demonstrates that CCO is currently aptly managing its Privacy related risks, with appropriate controls in place for the safeguarding of PHI.

The Privacy & Access Office has a Remediation Program in place, where privacy risks and remediation activities are logged. This program will be updated to align with the new enterprise risk management framework to be developed and implemented in 2011.

The following documents outline CCO's compliance with this requirement:

1. *CCO's Privacy & Access Office Remediation Program logs*

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Organizational and Other: IPC Requirement 6: Policy and procedures for maintaining a consolidated log of recommendations.

The Privacy & Access Office's Remediation Program includes the maintenance of a number of logs which track the operations of the Privacy Program at CCO, which have been implemented to effectively address any privacy risks or recommendations identified in PIAs, breach reports and IPC reviews. The remediation program contributes to the Privacy & Access Office's overarching strategy for risk management at CCO.

The following documents outline compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCC's Privacy Breach Management Procedure*, Privacy & Access Office –Name change to CSP's Privacy Breach Management Procedure as of September 2011
3. *CCO's Privacy Audit & Compliance Standard*, Privacy & Access Office
4. *CCO's Privacy & Access Office Operations Manual,* Privacy & Access Office
5. *CCO's Privacy & Access Office Remediation Program logs,* Privacy & Access Office

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Organizational and Other: IPC Requirement 7: Consolidated log of recommendations.

CCO maintains logs to track all recommendations made by the Privacy & Access Office to address identified privacy risks, and the status of implementation of each recommendation, as part of its Remediation Program.

The following documents outline CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
2. *CCO's Privacy & Access Office Remediation Program*, Privacy & Access Office
    a. CCC's *Log of Privacy Assessments*
    b. *CCC's Log of Privacy Breaches*
    c. *CCC's Log of Privacy Complaints & Inquiry*
    d. *CCC's Log of IPC Recommendations*

Note: The names of all the logs will be changed to CSP as of September 2011.

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

Organizational and Other: IPC Requirement 8: Business Continuity and Disaster Recovery Plan.

CCO's Technology Services Business Continuity and Disaster Recovery Plan was previously reviewed by the IPC in the 2008 triennial review. CCO has undertaken a multi-year project to enhance its Business Continuity and Disaster Recovery Plan ("the Plan"). The first "test" was the fan out test within Technology Services and was completed in March 2011. The test plans will start small and work up to a larger test scenario over the next two years. The revised Plan documents and implements the appropriate processes which manage every phase of a disaster from response through to restoration.

1. *CCO's Business Continuity and Disaster Recovery Plan*, Technology Services

2. *CCO's Business Continuity Service Framework*, Technology Services
3. *CCO's Business Continuity and Discovery Recovery Test Strategy for 2011/2012*, Technology Services

The following measures are currently being implemented by CCO to fully meet the IPC requirements or they are not applicable to our organization:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Scheduled	In Progress	N/A	
All requirements have been met.					

PRIVACY, SECURITY AND OTHER INDICATORS

Part 1- Privacy Indicators

As per the IPC's request, all Indicators are for the period of October 31, 2008 - June 30, 2011.

General Privacy Policies, Procedures and Practices

	IPC Key Indicator Required	CCO's Response
1	Record of dates for review of policies and procedures since the prior review of the IPC.	There have been three reviews of CCC's Privacy Policy and Procedures from October 2008 to March 31, 2011. The following CCC Policy & Procedures were reviewed in October 2009 & 2010 o CCC's Privacy Policy CCC's Access Control Procedure o CCC's Data Request Procedure o CCC's Compliance Procedure o CCC's Privacy Breach Management Procedure o CCC's privacy inquiries and complaints Procedure o CCC's Privacy Training & Awareness Procedure – The following CCC Policies and Procedures were reviewed in March 2011. The review was conducted to ensure applicability of the CCC policies to the Ontario Cancer Screening Program. These revised Policies and Procedures will be implemented once the Ontario Cancer Screening Registry is operational. o CCC's Privacy Policy – merged with CCO Privacy Policy o CCC's Access Control Procedure – Name change to CSP Access Control Procedure o CCC's Data Request Procedure - Name change to CSP Data Request Procedure. o CCC's Privacy Breach Management Procedure - Name change to CSP Breach Management Procedure. o CCC's privacy inquiries and complaints Procedure – Name change to privacy inquiries and complaints Procedure

		o CCC's Privacy Training & Awareness Procedure – merged with CCO Privacy Training & Awareness Procedure o CCC's Compliance procedure – Replaced with CCO's Privacy Audit & Compliance Standard
2	Log of amendments, date of amendment and description of amendment, as a result of the prior review of the IPC.	There was no amendment to any CCC related policy and procedures as a result of the IPC review of CCO in October 2008.
3	Record of new policies and procedures developed as a result of the prior review of the IPC.	One procedure for CCO in respect of the prescribed registry was developed as a result of the last review by the IPC in October 2008. The IPC review recommended that CCO should develop a procedure for reviewing and approving requests from external parties for access to the data maintained within the Colorectal Cancer Screening Registry. As a result of this recommendation, the following procedure was created in November 2008. • CSP Data Request Procedure
4	Record of dates and nature of communication regarding amendments.	The privacy procedure was communicated in November 2008. It has been communicated through CCO's intranet and/or public-facing website, per CCO's dissemination procedure.
5	Record of changes to public communication materials, as a result of the prior review of the IPC.	As a result of the IPC's review of the CCO prescribed registry in 2008, the following public communication materials were changed / finalized. • FOBT Kit Privacy Insert • FOBT Result Notification Letter • FOBT Invitation Letter • FOBT Reminder Letter • Summary of PIA on Colorectal Cancer Screening Registry (CCSR) was posted on CCO website.

Collection

IPC Key Indicator Required		CCO's Response
1	The number of data holdings containing personal health information.	CCO has 14 data holdings which are operating under the PHIPA authority of a prescribed registry.
2	The number of statements of	14 statements of purpose have been developed for these

	purpose developed for data holdings containing personal health information.	data holdings.
3	The number and list of the statements of purpose for data holdings containing PHI that were reviewed since the prior review of the IPC.	14 statements of purpose for CCO's data holdings operating under the PHIPA authority of a prescribed registry were reviewed since the prior review of the IPC in order to meet the IPC's 2011 requirements. Statements of purpose are reviewed on an annual basis by CCO's Privacy & Access Office, with support from the assigned Data Steward for each data holding. Please refer to Appendix 1 to Indicators – List of Statements of Purpose, for a complete list of statements of purpose for CCO's programs operating under the PHIPA authority of a prescribed registry.
4	Log of amendments, date of amendment and description of amendment made to statements of purpose as a result of the prior review of the IPC.	No amendments to CCO's Statements of Purpose, in respect of the prescribed registry, were required as a result of the IPC's last review of CCO in October 2008.

Use

IPC Key Indicator Required		CCO's Response
1	The number of agents granted approval to access and use personal health information for purposes other than research.	From October 31, 2008 to June 30, 2011, CCO's Online Direct Data Access Request **(ODDAR)** system has recorded 628 requests for access to data holding within the prescribed registry to use PHI for purposes other than research as related to data holdings associated with CCO's role as a prescribed registry. **Note:** Per the CSP Access Control Procedure, internal users must request and receive approval for direct access to each individual CSP data holding through the ODDAR system prior to receiving access privileges. It is common for internal users to require access to multiple data holdings in order to perform their job duties, thus requiring the users to submit multiple access requests through the ODDAR system. Further, each internal user must renew their access

		privileges on an annual basis by submitting a request, indicating that they have completed the Annual Privacy and Security Training Refresher and receiving approval for direct access to each individual CSP data holding through the ODDAR system.
2	The number of requests received for the use of personal health information for research, since the prior review of the IPC.	N/A **Note:** CCO in respect of the prescribed registry does not have internal requests for PHI for research purposes.
3	The number of requests for the use of personal health information for research purposes that were granted and that were denied, since the prior review of the IPC.	N/A **Note:** CCO in respect of the prescribed registry does not have internal requests for PHI for research purposes.

Disclosure

IPC Key Indicator Required		CCO's Response
1	The number of requests received for the disclosure of personal health information for purposes other than research, since the prior review of the IPC.	From October 2008 to June 30, 2011, CCO in respect of the prescribed registry received zero requests for PHI for purposes other than research.
2	The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied, since the prior review of the IPC.	There have been zero requests for the disclosure of PHI for purposes other than research hence none were granted or denied.
3	The number of requests received for the disclosure of personal health information for research purposes, since the prior review of the IPC.	From October 2008 to June 30, 2011, there were five external research requests received by CCO in respect of the prescribed registry, for PHI.
4	The number of requests for the disclosure of personal health information for research purposes that were granted	Request Granted = 5

	and that were denied, since the prior review of the IPC.	Request Denied = 0
5	The number of Research Agreements executed with researchers to whom personal health information was disclosed, since the prior review of the IPC.	Two research agreements were executed with researchers to whom personal health information was disclosed. Three research agreements are in the process of being executed.
6	The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes, since the prior review of the IPC.	From October 2008 to June 30, 2011, there were zero requests received for de-identified and/or aggregate information for both research and other purposes.
7	The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes, since the prior review of the IPC.	No acknowledgements or agreements were executed by persons to whom de-identified and/or aggregate information was disclosed since the prior review of the IPC.

Data Sharing Agreements

IPC Key Indicator Required		CCO's Response
1	The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity, since the prior review of the IPC.	As of June 30, 2011, there has been one Data Sharing Agreement amended for the collection of PHI by CCO, under the PHIPA authority of a prescribed registry
2	The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity, since the prior review of the IPC.	From October 31 2008 to June 30, 2011 CCO (as a prescribed person) has not executed a data sharing agreement for the disclosure of personal health information.

Agreements with Third Party Service Providers

IPC Key Indicator Required		CCO's Response
1	The number of agreements executed with third party service providers with access to personal health information, since the prior review of the IPC.	From October 31 2008 to June 30, 2011, there have been eight agreements executed with third party service providers with access to personal health information in the prescribed registry.

Data Linkage

IPC Key Indicator Required		CCO's Response
1	The number and a list of data linkages approved, since the prior review of the IPC.	From October 31 2008 to June 30, 2011, there has been one data linkage approved for CCO in respect of the prescribed registry.

Privacy Impact Assessments

IPC Key Indicator Required		CCO's Response
1	The number and a list of privacy impact assessments completed since the prior review by the IPC and for each privacy impact assessment:	From October 31 2008 to June 30, 2011, CCO has completed two PIAs. The PIAs completed are as follows: 1. CCC – Addendum to 2008 PIA, June 2009 2. CIRT – Addendum to 2008 PIA, June 2009

	• The data holding, information system, technology or program, • The date of completion of the privacy impact assessment, • A brief description of each recommendation, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	Please refer to Appendix 3 -Indicators – Summary from the Log of PIAs, for a list of Privacy Impact Assessments completed by CCO since October 2008.
2	The number and a list of privacy impact assessments undertaken but not completed, since the prior review of the IPC.	As of June 30, 2011, there is no outstanding PIA yet to be completed.
3	The number and list of privacy impact assessments that were not undertaken but will be completed and the proposed date of completion.	There is no outstanding PIA since the last review of the IPC.
4	The number of determinations made, since the prior review of the IPC, that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.	CCO uses a Preliminary Privacy Assessment Form (PPAF), completed in the initiating phase of a project, to determine whether a PIA or Addendum to a PIA is required for a project based on the collection, use or disclosure of PI/PHI which is in scope for that project. 1. Since the IPC's last review of CCO in October 2008, the following PPAFs have been completed: ISC – Preliminary Privacy Assessment Form, June 2011 2. Physician Linked Invitation - Preliminary Privacy Assessment Form, June 2011
5	The number, list and a brief description of privacy impact assessments reviewed, since the prior review of the IPC.	There were no reviews of PIAs since the last review of the IPC. As noted above the original CCC PIA was amended two times to reflect changes in the operation of the program.

		A PIA on CSP program is currently in progress. The PIA is analyzing the service delivery model for CSP as well as conducting an authority analysis on the CSP.

Privacy Audit Program

	IPC Key Indicator Required	CCO's Response
1	The dates of audits of agents granted approval to access and use personal health information, since the prior review of the IPC, and for each audit conducted: • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	The auditing of access to PHI for the prescribed registry specific data holdings will be part of the recently implemented logging, monitoring and auditing project. The project is being implemented for each CCO program in a staged process. The first CCO data holding was integrated with the logging, monitoring and auditing system in July 2010. Data holdings associated with CCO's role as a prescribed registry are scheduled to be added to logging, monitoring and auditing system in 2011 Additionally, the Privacy Audit and Compliance program is currently being reviewed and updated as required to align with the objectives of the new enterprise risk management framework to be developed and implemented in 2011. The new enterprise risk management framework will define the nature of privacy audits to be conducted at CCO moving forward. CCO does not currently maintain a brief description of each recommendation resulting from audits conducted per the *Direct Data Access Audit Procedure*. However, a security risk tracking utility will be implemented by July 2011. The tool will be able to report on a brief description of each recommendation, the date each recommendation was or is proposed to be addressed and the manner in which each recommendation was addressed or is proposed to be addressed.
2	The number and a list of all other privacy audits completed, since the prior review of the IPC, and for each audit: • A description of the nature and type of audit conducted,	Per CCO's Privacy Audit and Compliance Standard, the following types of privacy audits were completed since the IPC's last review of CCO in October 2008: 1. **Annual policy reviews** -2008 – 1 review completed 2010 – 1 review completed

	• The date of completion of the audit, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	2. **Operational reviews** -2008 – 2 'clean desk' audits completed -2009 – 4 'clean desk' audits completed Due to the sensitive nature of CCO's security practices, CCO has excluded some of details of these practices from the public version of this report, however these have been provided to the IPC. For all other audits completed since the prior review of the IPC, CCO does not currently maintain a brief description of each recommendation made, the date each recommendation was or is proposed to be addressed or the manner in which each recommendation was addressed or is proposed to be addressed. *Moving forward, CCO will maintain a record of each of these items or other audits undertaken.*

Privacy Breaches

IPC Key Indicator Required		CCO's Response
1	The number of notifications of privacy breaches or suspected privacy breaches received, since the prior review of the IPC.	From October 31 2008 to June 30, 2011, there have been 99 privacy breaches reported for the program operating under the PHIPA authority of a prescribed registry.
2	With respect to each privacy breach or suspected privacy breach: • The date that the notification was received, • The extent of the privacy breach or suspected privacy breach, • Whether it was internal or external, • The nature and extent	CCC maintains a comprehensive log of all reported privacy breaches and incidents. The root cause of privacy breaches are noted as follows: 1. **97 breaches:** Mailing of results to a wrong address 2. **1 breach:** Lost screening activity reports (currently under investigation, potentially 10,000 patient records). 3. **1 breach:** Policy infraction Please refer to Appendix 4 to Indicators- Summary from the Log of Privacy Breaches for a list of privacy breaches.

	of personal health information at issue, • The date that senior management was notified, • The containment measures implemented, • The date(s) that the containment measures were implemented, • The date(s) that notification was provided to the health information custodians or any other organizations, • The date that the investigation was commenced, • The date that the investigation was completed, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	

Privacy Complaints

	IPC Key Indicator Required	CCO's Response
1	The number of privacy complaints received, since the	From October 31 2008 to June 30, 2011, there have been 20 privacy complaints reported for the program operating

	prior review of the IPC.	under the PHIPA authority of a prescribed registry.
2	Of the privacy complaints received, the number of privacy complaints investigated, since the prior review of the IPC, and with respect to each privacy complaint investigated: • The date that the privacy complaint was received, • The nature of the privacy complaint, • The date that the investigation was commenced, • The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation, • The date that the investigation was completed, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, • The manner in which each recommendation was addressed or is proposed to be addressed, and • The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.	CCC maintains a comprehensive log of all reported privacy complaints. Please refer to Appendix 5 to Indicators – Summary of Log of Privacy Complaints for a list of privacy complaints.
3	Of the privacy complaints received, the number of	As of June 30, 2011, all complaints received have been investigated.

	privacy complaints not investigated, since the prior review of the IPC, and with respect to each privacy complaint not investigated: • The date that the privacy complaint was received, • The nature of the privacy complaint, and • The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.	

Part 2 - Security Indicators
As per the IPC's request, all Indicators are for the period of October 31, 2008 - June 30, 2011.

General Security Policies and Procedures

	IPC Key Indicator Required	CCO's Response
1	The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.	There have been three reviews of security policies and procedures since the IPC's last review of CCO in October 2008: 1. March 2009 2. September-December 2010 3. January – July 2011 **Note:** the 2010 review consisted of a full revision of CCO's suite of security policies and procedures.
2	Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	The 2010 review of CCO's suite of security policies and procedures resulted in amendments to all existing policies, standards or procedures or developments of new security policies, standards and procedures.
3	Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	Eight new security policies and/or procedures were developed as a result of the IPC's last review of CCO in October 2008. These new security policies and procedures are as follows: • Information Security Policy; • Acceptable Use of Social Media Policy; • Information Security Code of Conduct; • Information Classification and Handling Guideline (Draft); • Information Classification and Handling Standard (Draft); • Logical Access Control Standard; • Cryptography Standard; and • Logging, Monitoring and Auditing Standard.
4	The dates that each amended and newly developed security policy	All of the new security policies, standards, procedures which were developed and approved have been communicated through CCO's intranet. The following

	and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.	documents/ were published in July 2010: • Information Security Code of Conduct; and • Acceptable Use of Social Media Policy. The following documents were published in July 2011: • Information Security Policy • Logical Access Control Standard • Cryptography Standard • Logging, Monitoring, and Auditing Standard
5	Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	No externally available information security communication materials were amended as a result of the IPC's last review of CCO in October 2008.

Physical Security

IPC Key Indicator Required		CCO's Response
1	The dates of audits of agents granted approval to access the premises and locations within the premises where records of personal health information are retained since the prior review by the Information and Privacy Commissioner and for each audit: A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	CCO practice is to conducts audits when an incident or suspected physical security incident has occurred. There have been no physical security breaches since the previous IPC review in 2008. If a physical security breach was investigated, a full review of CCO's EasyLobby Visitor Grid Log and KeyScan System Log would be required. CCO's Privacy Audit and Compliance program will be reviewed and updated to align with the objectives of the new enterprise risk management framework (to be developed and implemented in 2011) The program will include scheduled audits of agents granted access to the premises where PHI is retained.

Security Audit Program

	IPC Key Indicator Required	CCO's Response
1	The dates of the review of system control and audit logs since the prior review by the Information and Privacy Commissioner of Ontario and a general description of the findings, if any, arising from the review of system control and audit logs.	System control and audit logs are reviewed systematically as part of CCO's operational processes. These audits occur on a network, server, and application level using a variety of software tools to review and alert based on predefined criteria. Additionally, as a component of a recommendation, from the IPC's last review of CCO in October 2008, to improve CCO's logging, monitoring, and auditing; a centralized security information event management capability has been implemented to support CCO's audit activities moving forward.
2	The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit: – A description of the nature and type of audit conducted, – The date of completion of the audit, – A brief description of each recommendation made, – The date that each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is expected to be addressed.	3 security audits have been completed since the IPC's last review of CCO in October 2008, as noted in CCO's log of security assessments. CCO's security audits include: • Threat risk assessments; and • Vulnerability assessments. Please refer to Appendix 5 to Indicators – Summary from the Log of Security Audits, for a list of security audits completed since the IPC's last review of CCO.

Information Security Breaches

	IPC Key Indicator Required	CCO's Response
1	The number of notifications of information security breaches or suspected information security breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	There have been 11 security incidents and breaches at CCO since the IPC's last review of CCO in October 2008. The current incident/breach log does not distinguish between PE and PR incidents hence the number below includes incidents and breaches for both PE and PR. : • 11 were determined to be security incidents • 2 were determined to be security breaches It must be clarified that the 177 incidents and breaches that were previously reported were mostly virus detections, nearly all of which were automatically quarantined and removed prior to spread. Based on CCO's definitions, there were in fact 11 security incidents and 2 security breaches. **Note:** CCO's EISO defines security incidents and security breaches as follows: • *Incident* – An event of significance that is being investigated as a potential breach to policy or attempt to circumvent established controls. Near-miss breaches or immaterial breaches should be classified as an incident. If automated tools are available incidents should generate an Alert for investigation. • *Breach* – Violation of regulatory requirements, material violation of corporate policy, or compromise of a sensitive asset.
2	With respect to each information security breach or suspected information security breach: – A description of the nature and type of audit conducted, – The date that the notification was received, – The extent of the information security breach or suspected information security breach, – The nature and extent of	CCO's EISO has determined that policy violations are the root cause of both security breaches which have occurred at CCO since the IPC's last review of CCO in October 2008. Descriptions of the 11 suspected information security breaches (including the 2 breaches) are captured in Appendix 7 to the indicators.

	personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the health information custodians or any other organizations, – The date that the investigation was commenced, – The date that the investigation was completed, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	

Part 3 – Human Resources Indicators
As per the IPC's request, all Indicators are for the period of October 31, 2008 - June 30, 2011.

Privacy Training and Awareness

	IPC Key Indicator Required	CCO's Response
1	The number of agents who have received and who have not received initial privacy orientation, since the prior review of the IPC.	As of June 30, 2011, all CCO employees (includes both PE and PR) have received initial privacy orientation since the IPC's last review of CCO in October 2008. The staff working for CCO in its capacity as a prescribed person also completes a separate privacy training module dedicated to CCO's role as a prescribed person. • **2009:** 282 employees received initial privacy orientation at the start of their employment • **2010:** 204 employees received initial privacy orientation at the start of their employment • **2011:** 113 employees received initial privacy orientation at the start of their employment **Note:** CCO electronically tracks completion of initial privacy orientation through its eLearning tool. The tool is unable to track the employees who have completed the privacy training module specific to CCO's role as a prescribed registry. CCO will be making changes to the eLearning tool to ensure that staff completing separate training module on CCO's role as a prescribed person are properly logged and documented. The completion of initial privacy orientation is mandatory for all employees within 30 days of their start date, per the Privacy and Security Training and Awareness Procedure and as a condition of employment with CCO.
2	The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation.	CCO electronically tracks completion of initial privacy orientation through its eLearning tool. The completion of initial privacy orientation is mandatory for all employees within 30 days of their start date, per the Privacy and Security, Training and Awareness Procedure and as a condition of employment with CCO. CCO will be enhancing its eLearning tool to track and enforce compliance with this onboarding requirement. CCO system access for

		employees who do not complete their initial privacy orientation within 30 days of their start date will be disabled.
3	Record of agents who have attended and who have not attended ongoing privacy training each year, since the prior review of the IPC.	As of June 30, 2011, the number of CCO employees (includes both PE and PR) who completed ongoing privacy training each year since the IPC's last review of CCO in October 2008 are as follows: • **2009:** 650 completed the Annual Privacy Refresher Training • **2010:** 686 completed the Annual Privacy Refresher Training • **2011:** The Annual Privacy Refresher is scheduled for October 2011. Per the Privacy and Security Training and Awareness Procedure, all CCO employees are required to complete privacy training on an annual basis. Since the implementation of CCO's eLearning tool in 2009, there have been fewer than 10 employees each year who have not completed the Annual Privacy Refresher Training curriculum, for reasons such as long-term leave. **Note:** CCO electronically tracks completion of the Annual Privacy Refresher Training curriculum through its eLearning tool. This record is contained in CCO's Log of Privacy and Security Training Completion.
4	Record of dates and number of communications to agents by CCO in relation to privacy and a brief description of each communication, since the prior review of the IPC.	There have been a number of communications to CCO employees since October 2008, as described in CCO's Privacy & Access Office Communication Plan. These are as follows: **2008:** • Revised and published Statement of Information Practices (internal and external) • Revised and published Privacy FAQs (internal and external) • Developed and published Privacy Brochure (external) • Launched CCC's Website **2009:** • Developed and published privacy posters to raise visibility and awareness on compliance services provided by CCO's Privacy & Access Office (internal) • Developed and published two privacy newsletters (internal) • Revised and published Privacy Statement (internal). • CCC program launched WebEx (communication tool for internal staff as well as external health care providers associated with the program). A Privacy FAQ section was published on the WebEx. **2010:**

		• Developed and published two privacy newsletters (internal) • Created privacy messaging on breaches which was delivered in a calendar format • Developed and launched privacy screensavers on all CCO computers (internal) **2011:** • Developed and published two privacy newsletters (internal)

Security Training and Awareness

IPC Key Indicator Required		Number
1	The number of agents who have received and who have not received initial security orientation, since the prior review of the IPC.	As of June 30, 2011, all CCO employees (includes both PE and PR) have received initial security orientation since the IPC's last review of CCO in October 2008. • **2009:** 282 employees received initial security orientation at the start of their employment • **2010:** 204 employees received initial security orientation at the start of their employment • **2011:** 113 employees received initial security orientation at the start of their employment **Note:** CCO electronically tracks completion of initial security orientation through its eLearning tool. The completion of initial security orientation is mandatory for all employees within 30 days of their start date, per the Privacy and Security Training and Awareness Procedure and as a condition of employment with CCO.
2	The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation.	CCO electronically tracks completion of initial security orientation through its eLearning tool. The completion of initial security orientation is mandatory for all employees within 30 days of their start date, per the Privacy and Security Training and Awareness Procedure and as a condition of employment with CCO. CCO will be enhancing its eLearning tool to track and enforce compliance with this requirement where CCO system access for employees who do not complete the initial privacy orientation within 30 days

		of their start date will be disabled.
3	Record of agents who have attended and who have not attended ongoing security training each year, since the prior review of the IPC.	As of June 30, 2011, the number of CCO employees who completed ongoing security training each year since the IPC's last review of CCO in October 2008 are as follows: • **2009:** 650 completed the Annual Security Refresher Training • **2010:** 686 completed the Annual Security Refresher Training • **2011:** The Annual Security Refresher Training is scheduled for October 2011. Per the Privacy and Security Training and Awareness Procedure, all CCO employees are required to complete security training on an annual basis. Since the implementation of CCO's eLearning tool in 2009, there have been fewer than 10 employees each year who have not completed the Annual Security Refresher Training curriculum, for reasons such as long-term leave. **Note:** CCO electronically tracks completion of the Annual Security Refresher Training curriculum through its eLearning tool. This record is contained in CCO's Log of Privacy and Security Training Completion.
4	Record of dates and number of communications to agents by CCO in relation to information security and a brief description of each communication, since the prior review of the IPC.	There have been a number of security communications to CCO employees since October 2008. These are as follows: **2008:** • CTO division and security program update (internal) • Lunch and Learn session on Information security program and policy update (internal) • Safe computing use at CCO – protecting against viruses (internal) **2009:** • Protecting CCO information from computer viruses and other malware - Cyber Security Awareness Month (internal) • Security services overview at the CIO Quarterly meeting (internal) • Security Health Check Presentation (external) Protecting CCO information from computer viruses (internal) • Description of security services on eCCO (internal) **2010:** • Encryption of All Health Information on Mobile Devices (internal) • Security Lunch & Learns - Crypto 101 (internal) • Security Lunch & Learn – Social Media (internal)

		• Social Media Presentation – Joint CCO/eHealth Information Security Seminar (external) **2011:** • Technology Services Tech Update (Jan 2011) – LiveMeeting & Crypto 101 (internal) • Technology Services Tech Update (April 2011) – breaches in the news and the security blog (internal) • Technology Services Bulletin (April 11, 2011) – Provision of Paging and Mobile Phone with Email Devices (internal) • Technology Services Bulletin (April 14, 2011) – CCO Security Policy & Standards For Review (internal) • Anti-virus upgrade to Forefront Endpoint Protection 2010 (internal) • Technology Services Bulletin (May 4, 2011) – Mobile Device Security Measures (internal) • Work@Home Pilot Group Security Awareness Training (June-July 2011) • Security Notice – Forefront Antivirus False Positive (internal)

Confidentiality Agreements

	IPC Key Indicator Required	CCO's Response
1	The number of agents who have executed Confidentiality Agreements each year since the prior review by the Information and Privacy Commissioner of Ontario.	As of June 30, 2011, the number of Confidentiality Agreements executed are as follows: • Nov 1, 2008 to Dec 31 2008 – 24 Confidentiality Agreements executed • Jan 1, 2009 to Dec 31, 2009 - 282 Confidentiality Agreements executed • Jan 1, 2010 to Dec 31, 2010 – 306 Confidentiality Agreements executed • Jan 1, 2011 to Jun 30, 2011 – 117 Confidentiality Agreements executed **Note:** The numbers noted above include CCO employees associated with both the roles of CCO i.e. as a prescribed entity and as a prescribed registry. These numbers do not include the number of third party service providers who

		have accepted confidentiality terms. All agreements with third party service providers contain confidentiality terms. CCO's Contract Management System (CMS) is currently being enhanced to track and log confidentiality terms accepted by third party service providers.
2	The date of commencement of the employment, contractual or other relationship for agents that have yet to executed the Confidentiality agreements and the date by which the Confidentiality Agreement must be executed.	All CCO employees and contractors are required to sign a Confidentiality Agreement with CCO. As of June 30, 2011, there are no outstanding Confidentiality Agreements that have not been executed.

Termination or Cessation

IPC Key Indicator Required		CCO's Response
1	The number of notifications received from agents since the prior review by the Information and Privacy Commissioner of Ontario related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.	As of June 30, 2011, 482 notifications were received in relation to termination of employment, contractual or other relationship with CCO, since the IPC's last review of CCO in October 2008. **Note:** The numbers noted above include CCO employees associated with both the roles of CCO i.e. as a prescribed entity and as a prescribed registry.

Part 4 – Organizational Indicators
As per the IPC's request, all Indicators are for the period of October 31, 2008 - June 30, 2011.

Risk Management

	IPC Key Indicator Required	CCO's Response
1	The dates that the corporate risk register was reviewed by the prescribed person or prescribed.	One review of CCO's corporate risk register was conducted in December 2010. **Note:** The Privacy & Access Office's Remediation Program will be updated to align with the new enterprise risk management framework to be developed and implemented in 2011.
2	Whether amendments were made to the corporate risk register as a result of the last IPC review, and if so, a brief description of the amendments made.	No recommendations for amendments to CCO's corporate risk register were made by the IPC since its last review of CCO in October 2008. **Note:** The Privacy & Access Office's Remediation Program will be updated to align with the new enterprise risk management framework to be developed and implemented in 2011.

Business Continuity and Disaster Recovery

	IPC Key Indicator Required	CCO's Response
1	The dates that the business continuity and disaster recovery plan was tested since the prior review by the Information and Privacy Commissioner of Ontario.	CCO is in the process of finalizing and implementing its revised Business Continuity and Disaster Recovery Plan, including the Test Strategy for 2011/2012. The IT Infrastructure Disaster Recovery Plan most recent test was conducted in June 2011.
2	Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief	CCO's Business Continuity Service Framework will be revised based on findings from tests performed on a regular basis, in accordance with the Business Continuity and Disaster Recovery Test Strategy for 2011/2012. The first test of the Plan was been completed in March 2011.

	description of the amendments made.	There are currently no modifications planned as a result of the initial testing of the IT Infrastructure.

APPENDIX 1 to Indicators – List of Statements of Purpose

Note: The list of data holdings are the data holdings currently supporting the CCC Program. The new data holdings as developed for the CSP program will be added to this list.

Data Holding	Data	Source	Statement of Purpose
CCC Interim Solution	This dataset contains: • Clinical data • Demographic and address data • Call centre operational activities data	• MOHLTC • Laboratories • Fulfillment House • Call Centre direct data entry.	System no longer used, required for Data migration, Archive and Audit only 1. The purpose of the data holding is to securely store data (including PHI) to support CCC Operations. PHI is collected for CCC client management and operations including, clinical results, direct client interactions and correspondence.
CCC LMS	This dataset contains: • Clinical data • Client Demographic data • Provider Demographic and Address data	• CCC – Siebel	1. The purpose is to support Colon Cancer Check Screening Operations. 2. PHI is collected for data exchange to and from Health Service Providers via secure web portal (OMD) as well as for validation of patient lists and electronic distribution of Provider Reports.
CCC - Siebel	This dataset contains: • Clinical data • Demographic and address data	• MOHLTC (RPDB, HNS, CHDB, CPDB, CAPE) • Laboratory (LIRT) • Hospital (CIRT)	1. The purpose of this data holding is to support CCC Operations, Planning and Performance. 2. Integrated Screening Siebel CRM system (CCC). It is a front end system for InScreen client management and operations including, Clinical

Data Holding	Data	Source	Statement of Purpose
	• Call centre operational activities data	• Fulfillment House • Statistics Canada (PC to LHIN) • Call Center direct data entry	Results, direct client interaction and Correspondence.
Screening Hub Integration	This dataset contains: • Clinical data • Demographic and address data • Call centre operational activities data	• MOHLTC (RPDB, HNS, CHDB, CPDB, CAPE) • Laboratory (LIRT) • Hospital (CIRT) • Fulfillment House (Correspondence) • Statstistics Canada (PC to LHIN) • Siebel Call Center	1. The purpose of this data holding is to support CCC Operations, Planning and Performance. 2. InScreen Integration Hub (Customer Data Integration) to support downstream InScreen information and data requirements. E.g. Siebel InScreen and Datamart reporting. Various sources from MOHLTC, Siebel InScreen, StatsCan and CCO are standardized, cleansed and integrated for downstream operations.
Screening Hub Stage – CAPE	This dataset contains: • Administrative Physician Data • HIN	• MOHLTC	1. The CAPE data set will be used to identify physicians in Ontario who have rostered patients. 2. This information will be used to compile a list of eligible rostered patients who will be invited to participate in the ColonCancerCheck program.
Screening Hub Stage – CHDB	This dataset contains: • Administrative Care • Clinical Data • PHI	• MOHLTC	1. The claims data received will be used to determine volumes of non-program FOBT kits processed and validating performance of facilities and physicians who have conducted Colonoscopies. 2. It will also be used as criteria for identifying the candidate population for the invitation pilot.

Data Holding	Data	Source	Statement of Purpose
Screening Hub Stage – CIRT	This dataset contains: • Administrative Care • Clinical Data • PHI	• Hospitals	1. The purpose of this data holding is to understand colonoscopy activity conducted within participating facilities. 2. The data collected through CIRT will be used to understand colonoscopy activity conducted within participating facilities from volume, wait time and quality perspectives. It is also used to determine funding and volume allocations across participating facilities.
Screening Hub Stage – LIRT	This dataset contains: • Administrative Care • Clinical Data • PHI	• Laboratories	1. The purpose of this data holding is to gather information from laboratories on FOBT results. 2. The data collected through the LIRT are FOBT results that is used for (a) generate participant communications; and (b) monitoring and reporting on FOBT volumes, geographic differences, test quality, variations between participating laboratories and highlighting the need for further awareness or education programs.
Screening Hub Stage - OPDB (Pharmacy Claims)	This dataset contains • Administrative Pharma Data • PHI	• MOHLTC	1. The purpose of this data holding is to gather information of FOBT dispensed by pharmacies. 2. This data will be used to evaluate the level of dispensing of FOBT kits at the pharmacies.
Screening Hub Stage - OCR	This dataset contains: • Administrative Care • Clinical Data	• CCO as PE	1. The OCR is a computerized database of information on all Ontario residents who have been diagnosed with cancer ("incidence") and/or who have died of cancer ("mortality"). All new cases of cancer are registered, except non-melanoma skin cancer.

Data Holding	Data	Source	Statement of Purpose
	• PHI		2. This information is used to support CCSR by identifying individuals who are ineligible for colorectal screening.
Screening Hub Stage - RPDB	The dataset contains: • Administrative Care • Clinical Data • PHI	• MOHLTC	1. This data holding contains information from Registered Person Database. This data is used in operationalization of colorectal screening. 2. This data will be used to identify Ontarians who are eligible and could be invited to participate in the CCC program. It will also be used for identity validation and data linking for client cancer journey assessment.
Screening Hub Stage - Siebel	The dataset contains: • Client demographics and address information • PHI	• Integration Hub • Call Centre direct entry	1. The purpose of this data holding is to integrate information for InScreen. 2. Recent Client, Address and Screening related activity within Siebel InScreen, required in the Screening Hub for integration purposes.
Primary Care Provider Reporting	This dataset contains: • Clinical data • PHI	• Integration Hub • Siebel	1. This data holding contains information on primary care providers. 2. This is used to store primary care provider screening activity reports. The report summarizes client level information for providers.

Note: The data holdings above reflect the current CCC program. As the cervical and breast screening modules are operationalized, this list will be updated to reflect the new data holding for the CSP.

APPENDIX 2 to Indicators – List of Data Linkages

Acronyms:

OCR…….. Ontario Cancer Registry
ALR…….. Activity Level Reporting
PIMS…….. Pathology Information Management System
OBSP…….. Ontario Breast Screening Program
NDFP…….. New Drug Funding Program
CIRT…….. Colonoscopy Interim Reporting System
LRT…….. Laboratory Reporting System

1. Research Linkages (in support of Section 44 activities):

Project Name	Data Holdings Linked	Year Approved by DAC
FOBT study	CIRT/LRT	2010

APPENDIX 3 to Indicators – Summary from the Log of PIAs

PIA	Date	Status	Recommendation	Completed	Pending	Deferred	In Process	To be Started	Date Recommendation Completed	Manner In which Recommendation Addressed
CCC PIA Addendum	June 2009	Complete	1. Without the appropriate third party relationship to and guidance from the CCC Program a disclosure of PHI may occur that is not in compliance with PHIPA.	Yes	N/A	N/A	N/A	N/A	August 2009	Audited all third party vendors accessing PHI and ensured that all of them have a contract in place with CCO.
			2. The data elements of PHI provided to PCPs on their patients for the purpose of verifying eligibility for CCC invitation may exceed the purpose of disclosure (verification of CCC eligibility).	Yes	N/A	N/A	N/A	N/A	August 2009	The purpose for collection, use and disclosure for each data element for the invitation pilot was documented.

PIA	Date	Status	Recommendation	Completed	Pending	Deferred	In Process	To be Started	Date Recommendation Completed	Manner In which Recommendation Addressed
CIRT PIA Addendum	June 2009	Complete	1. There is no indication that CCC makes the purposes of its collection of CIRT PHI known to HICs that supply the PHI.	Yes	N/A	N/A	N/A	N/A	October 2009	CIRT Manual updated.
			2. There is need to confirm that only the data required for those purposes is collected through the CIRT to comply with CCC's Privacy Policy.	Yes	N/A	N/A	N/A	N/A	October 2009	The purpose of collection of data elements was confirmed and it is documented.
			3. The CCC Privacy Policy does not address internal data linking for CCC business	Yes	N/A	N/A	N/A	N/A	October 2009	CCC Privacy Policy reviewed.

PIA	Date	Status	Recommendation	Completed	Pending	Deferred	In Process	To be Started	Date Recommendation Completed	Manner In which Recommendation Addressed
			purposes or for CCC internal data linkages							

APPENDIX 4 to Indicators – Summary from the Log of Privacy Breaches

The table below lists the breaches from November 1, 2008 – June 30, 2011

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
12	12/17/2008	12/17/2008 – 12/23/2008	External	FOBT Test result to wrong address – participant moved	Result letter returned	12/17/2008	12/17/2008	12/29/2008	Yes	12/29/2008 – 01/04/2009	None	N/A
13	12/29/2008	12/29/2008 – 01/04/2009	External	FOBT Test result to wrong address – incorrect address on requisition	Result letter returned	12/29/2008	12/29/2008	01/20/2009	Yes	01/20/2009 – 01/25/2009	None	N/A
14	01/27/2009	01/27/2009 - 01/30/2009	External	FOBT Test result to	Result letter returned	01/27/2009	01/27/2009	01/30/2009	Yes	01/30/2009 – 02/5/2009	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				wrong address - incorrect address on requisition								
15	02/13/2009	02/13/2009 - 02/18/2009	External	FOBT Test result to wrong address - incorrect address on requisition	Result letter returned	02/13/2009	02/13/2009	02/20/2009	Yes	02/20/2009 - 02/25/2009	None	N/A
16	02/25/2009	02/25/2009 - 03/02/2009	External	FOBT Test result to wrong address - incorrect address on	Result letter returned	02/25/2009	02/25/2009	03/5/2009	Yes	03/5/2009 - 03/10/2009	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				requisition								
17	03/04/2009	03/04/2009 - 03/09/2009	External	Laboratory left PHI on participant's voicemail.	N/A	N/A	03/04/2009	04/5/2009	Yes	03/4/2009 - 03/10/2009	Raise issues as detailed by IPC with stakeholders and to recommend to strengthened privacy provision in the contract between stakeh	September 2009 - Addressed were raised in the Joint steering committee of the stakeholders. August-October 2009 - Developed frequently asked questions for HICs, Included privacy as a standing item on the stakeholder meetings, engaged OAML and Privacy

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
											olders. Increase privacy awareness among health information custodians	Office of the participating laboratories to discuss relevant privacy issues.
18	03/23/2009	03/23/2009 - 03/28/2009	External	FOBT Test result to wrong address - incorrect address on requisiti	Result letter returned	03/23/2009	03/23/2009	04/2/2009	Yes	04/2/2009 - 04/7/2009	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				on								
19	04/21/2009	04/21/2009 - 04/24/2009	External	FOBT Test result to wrong address - lab data entry error	Result letter returned	04/21/2009	04/21/2009	04/24/2009	Yes	04/24/2009 - 04/29/2009	None	N/A
20	04/24/2009	04/24/2009 - 04/28/2009	External	FOBT Test result to wrong address - incorrect address on requisition	Result letter returned	04/24/2009	04/24/2009	04/28/2009	Yes	04/28/2009 - 05/03/2009	None	N/A
21	July 2008 Breach- not noted here											
22	04/28/2009	04/28/2009 -	External	FOBT Test result to	Letter was provided	04/28/2009	04/28/2009	04/29/2009	Yes	04/29/2009 - 05/04/2009	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
		04/29/2009		wrong address - incorrect address on requisition	by recipient to the participant							
23	05/28/2009	05/28/2009 - 06/02/2009	External	FOBT Test result to wrong address – participant moved	Result letter returned	05/28/2009	05/28/2009	06/2/2009	No		None	N/A
24	06/4/2009	06/4/2009 - 06/9/2009	External	FOBT Test result to wrong address - incorrect address on requisition	Result letter returned	06/4/2009	06/4/2009	06/12/2009	Yes	06/12/2009 - 06/17/2009	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
25	06/5/2009	06/5/2009 - 06/9/2009	External	FOBT Test result to wrong address - incorrect address on requisition	Result letter returned	06/5/2009	06/5/2009	06/12/2009	Yes	06/12/2009 - 06/17/2009	None	N/A
26	06/19/2009	06/19/2009 - 06/24/2009	External	FOBT Test result to wrong address - incorrect address on requisition	Result letter returned	06/19/2009	06/19/2009	06/25/2009	Yes	06/25/2009 - 06/30/2009	None	N/A
27	06/29/2009	06/29/2009 - 07/4/2009	External	FOBT Test result to wrong address - 2	Result letter returned	06/29/2009	06/29/2009	07/29/2009	Yes	06/29/2009 - 07/04/2009	Vendor to review process for checki	July 29, 2009 – Process was implemented to ensure 5 prior and 5 after envelope

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				results in one envelope							ng content of envelope when inserter machine stoppage occurs. Vendor to increase privacy awareness	are manually checked by two individuals whenever an inserter stoppage occurs. July 29, 2011 Vendor provided further training to the staff assigned to CCC project.

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
											of the staff.	
28	08/4/2009	08/4/2009 - 08/9/2009	External	FOBT Test result to wrong address - lab data entry error	Result letter returned	08/4/2009	08/4/2009	08/10/2009	Yes	08/10/2009 - 08/15/2009	None	N/A
29	08/7/2009	08/7/2009 - 08/12/2009	External	FOBT Test result to wrong address - lab data entry error	Result letter returned	08/7/2009	08/7/2009	08/19/2009	Yes	08/19/2009 - 08/24/2009	None	N/A
30	08/14/2009	08/14/2009 - 08/19/2009	External	FOBT Test result to wrong address - ineligible address	Letter shredded	08/14/2009	08/14/2009	08/27/2009	Yes	08/27/2009 - 09/02/2009	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				on requisition								
31	08/27/2009	08/27/2009 - 08/28/2009	External	FOBT Test result to wrong address - NCOA	Recipient to provide letter to the participant	08/27/2009	08/27/2009	08/28/2009	Yes	08/28/2009 - 09/03/2009	None	N/A
32	10/16/2009	10/16/2009 - 10/21/2009	External	Email containing PHI was sent to CCO Service Desk	Emails containing PHI were destroyed.	10/26/2009	10/26/2009	10/26/2009	No	N/A	Prohibit use of email in transmission of PHI. Raise awareness	October 26th, 2009 – Stakeholder was advised not to use email for transmission of PHI. November 3rd, 2009 - Privacy Specialist presented to Program monthly meeting on privacy best practices for transfer of PHI

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
											on Privacy to all Program stakeholders. CCO's Service Desk to create a procedure for dealing with PHI receiv	and reiterated the process to be followed for transfer of PHI to CCO. November 10th, 2009 – A Procedure was created for Service Desk staff for dealing with PHI received via an email.

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
											ed via an email	
33	10/16/2009	10/16/2009	External	FOBT Test Result to the wrong address.	Result letter returned	10/16/2009	10/16/2009	10/16/2009	Yes	10/16/2009 - 10/21/2009	None	N/A
34	11/16/2009	11/16/2009	External	FOBT Test Result to the wrong address.	Result letter returned	11/16/2009	11/16/2009	11/16/2009	Yes	11/16/2009 - 11/21/2009	None	N/A
35	11/16/2009	11/16/2009 - 11/17/2009	External	FOBT Test Result to the wrong address.	Result letter returned	11/16/2009	11/16/2009	11/17/2009	Yes	11/17/2009 - 11/22/2009	None	N/A
36	12/23/2009	12/23/2009 - 12/28/2009	External	FOBT test result sent to	Result letter returned	12/23/2009	12/23/2009	01/07/2010	Yes	01/07/2010 - 01/12/2010	Advise Laboratory of inputti	Dec 30, 2009 – Laboratory confirmed that staff has been

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				the wrong address.							ng incorr ect addres s into LRT	reminded and notified of the procedure for data entry.
3 7	1/20/2010	1/20/2010 - 1/25/2010	None	FOBT test result letter	Result letter returned	1/20/2010	1/20/2010	1/26/2010	No	1/26/2010 - 1/31/2010	None	N/A
3 8	2/8/2010	2/8/2010	External	FOBT test result sent to wrong address	Result letter returned	2/8/2010	2/8/2010	2/8/2010	Yes	2/8/2010 - 2/13/2010	None	N/A
3 9	2/24/2010	2/24/2010	Internal	FOBT Test result to wrong address – participa nt moved	The result letter was shredde d by the Recipien t	2/24/2010	2/24/2010	2/24/2010	Yes	2/24/2010 - 3/01/2010	None	N/A
4	3/11/2010	3/11/2010 -	External	FOBT test	Result letter	3/11/2010	3/11/2010	3/11/2010	Yes	3/11/2010 -	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
0		3/11/2010		result sent to wrong address – NCOA	returned					3/16/2010		
41	3/24/2010	3/24/2010 - 3/29/2010	External	FOBT test result – 3 results sent in one envelope	Result letter returned	3/24/2010	3/24/2010	3/31/2010	Yes	3/31/2010 - 4/05/2010	FH to use only the intelligent insert for CCO mailings.	Mar 31, 2010 – FH agreed with the recommendation to only use intelligent inserter for CCO mailings. Mar 31st, 2011 - FH reviewed significance of mailing PHI with operators as well as committed to conducting a quarterly review of PHI and security measures for CCO mailings to ensure that FH remains

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
											FH to review significance of PHI mailing with operators involved with CCO mailing FH to put in place a quarterly review of PHI and security measures for	vigilant in checking and double checking any issues with processing stops.

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
											CCO mailings	
42	3/24/2010	3/24/2010 - 3/29/2010	External	FOBT test result – 3 results sent in one envelope	Result letter returned	3/24/2010	3/24/2010	3/31/2010	Yes	3/31/2010 - 4/05/2010	FH to use only the intelligent insert for CCO mailings. FH to review	Mar 31, 2010 – FH agreed with the recommendation to only use intelligent inserter for CCO mailings. Mar 31st, 2011 - FH reviewed significance of mailing PHI with operators as well as committed to conducting a quarterly review of PHI and security measures for CCO mailings to ensure that FH remains vigilant in checking and

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
											significance of PHI mailing with operators involved with CCO mailing FH to put in place a quarterly review of PHI and security measures for CCO mailin	double checking any issues with processing stops.

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
											gs	
43	3/30/2010	3/30/2010 - 3/31/2010	External	FOBT test result sent to wrong address – Lab Data entry error	None as intended recipient received the result letter from his neighbour	N/A		3/31/2010	No	N/A	N/A	N/A
44	3/31/2010	3/31/2010	External	FOBT test result sent to wrong address – ineligible address on requisition	Letter shredded	3/31/2010	3/31/2010	3/31/2010	Yes	3/31/2010 - 4/05/2010	None	N/A
45	4/9/2010	4/9/2010	External	FOBT test result sent to wrong	Result letter returned	4/9/2010	4/9/2010	4/9/2010	Yes	4/9/2010 - 4/14/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				address – Lab Data entry error								
46	4/13/2010	4/13/2010 - 4/14/2010	External	FOBT test result sent to wrong address – Canada Post delivered letter to wrong address	Result letter returned	4/13/2010	4/13/2010	4/14/2010	Yes	4/14/2010 - 4/19/2010	None	N/A
47	4/14/2010	4/14/2010 - 4/16/2010	External	FOBT test result sent to wrong address – Missing Unit number	Letter was provided to the participant by the neighbour	4/14/2010	4/14/2010	4/16/2010	Yes	4/16/2010 - 4/21/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
48	4/19/2010	4/19/2010 - 4/20/2010	External	FOBT test result sent to wrong address – Lab Data entry error	Letter was provided to the participant by the neighbour	4/19/2010	4/19/2010	4/20/2010	No	N/A	None	N/A
49	4/21/2010	4/21/2010	External	FOBT test result sent to wrong address – NCOA	Recipient shredded the letter	4/21/2010	4/21/2010	4/21/2010	Yes	4/21/2010 - 4/26/2010	None	N/A
50	4/21/2010	4/21/2010	External	FOBT test result sent to wrong address – ineligible address on requisiti	Result letter returned	4/21/2010	4/21/2010	4/21/2010	Yes	4/21/2010 - 4/26/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				on								
51	4/26/2010	4/26/2010	External	FOBT test result sent to wrong address – Lab Data entry error	Result letter returned	4/26/2010	4/26/2010	4/26/2010	Yes	4/26/2010 - 5/01/2010	None	N/A
52	5/3/2010	5/3/2010 - 5/7/2010	External	FOBT test result sent to wrong address – Wrong Unit number	Result letter returned	5/3/2010	5/3/2010	5/7/2010	Yes	5/7/2010 - 5/12/2010	None	N/A
53	5/6/2010	5/6/2010	External	FOBT test result sent to wrong address – NCOA	Result letter returned	5/6/2010	5/6/2010	5/6/2010	Yes	5/6/2010 - 5/11/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
54	5/17/2010	5/17/2010 - 5/22/2010	External	FOBT test result sent to wrong address – Lab Data entry error	Result letter returned	5/17/2010	5/17/2010	6/1/2010	Yes	6/1/2010 - 6/6/2010	None	N/A
55	5/19/2010	5/19/2010 - 5/24/2010	External	FOBT test result sent to wrong address – Lab Data entry error	Result letter returned	5/19/2010	5/19/2010	5/26/2010	Yes	5/26/2010 - 6/01/2010	None	N/A
56	5/25/2010	5/25/2010 - 5/30/2010	External	FOBT sent to wrong address as participant moved	Result letter returned	5/25/2010	5/25/2010	6/01/2010	No	N/A	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				and did not update the address with any of the healthcare providers								
57	6/1/2010	6/1/2010	External	FOBT sent to wrong address as participant moved and did not update the address with any of the healthcare provider	Result letter returned	6/1/2010	6/1/2010	6/1/2010	Yes	6/1/2010 - 6/6/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				s								
58	6/2/2010	6/2/2010 - 6/4/2010	External	FOBT sent to wrong address as participant moved and did not update the address with any of the healthcare providers	Anonymous caller notified of the breach	N/A	6/2/2010	6/4/2010	Yes	6/4/2010 - 6/9/2010	None	N/A
59	6/7/2010	6/7/2010	External	FOBT test result sent to wrong address – Lab Data	Result letter returned	6/7/2010	6/7/2010	6/7/2010	Yes	6/7/2010 - 6/12/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				entry error								
60	6/7/2010	6/7/2010	External	FOBT sent to wrong address as participant moved and did not update the address with any of the healthcare providers	Result letter returned	6/7/2010	6/7/2010	6/7/2010	Yes	6/7/2010 - 6/12/2010	None	N/A
61	6/7/2010	6/7/2010	External	FOBT sent to wrong address as participant	Result letter returned	6/7/2010	6/7/2010	6/7/2010	Yes	6/7/2010 - 6/12/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				moved and did not update the address with any of the healthcare providers								
62	6/8/2010	6/8/2010	External	FOBT test result sent to wrong address – Lab Data entry error	Result letter returned	6/8/2010	6/8/2010	6/8/2010	Yes	6/8/2010 - 6/13/2010	None	N/A
63	7/21/2010	7/21/2010	External	FOBT test result sent to wrong address	Result letter returned	7/21/2010	7/21/2010	7/21/2010	Yes	7/21/2010 - 7/26/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				– Wrong Unit number								
64	8/6/2010	8/6/2010	External	FOBT test result sent to wrong address – Wrong Unit number	Result letter returned	8/6/2010	8/6/2010	8/6/2010	Yes	8/6/2010 - 8/11/2010	None	N/A
65	8/10/2010	8/10/2010	External	FOBT test result sent to wrong address – Lab Data entry error	Result letter returned	8/10/2010	8/10/2010	8/10/2010	Yes	8/10/2010 - 8/15/2010	None	N/A
66	8/16/2010	8/16/2010	Internal	FOBT test result sent to wrong address	Result letter returned	8/16/2010	8/16/2010	8/16/2010	Yes	8/16/2010 - 8/21/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				– LRT address not uploaded into address screen								
67	8/23/2010	8/23/2010	External	FOBT sent to wrong address as participant moved and did not update the address with any of the healthcare providers	Recipient shredded the letter	8/23/2010	8/23/2010	8/23/2010	Yes	8/23/2010 - 8/28/2010	None	N/A
68	8/30/2010	8/30/2010 - 9/01/2010	External	FOBT test	Result letter	8/30/2010	8/30/2010	9/1/2010	Yes	9/1/2010 - 9/6/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				result sent to wrong address – Lab Data entry error	returned							
69	9/7/2010	9/7/2010 - 9/12/2010	External	FOBT sent to wrong address as participant moved and did not update the address with any of the healthcare providers	Result letter returned	9/7/2010	9/7/2010	9/23/2010	No	9/23/2010 - 9/28/2010	None	N/A
7	9/8/2010	9/8/2010 -	External	FOBT	Result	9/8/2010	9/8/2010	9/17/2010	Yes	9/17/2010 -	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
0		9/13/2010		test result sent to wrong address – Incorrect address on requisition	letter returned					9/22/2010		
71	9/16/2010	9/16/2010 - 9/21/2010	External	FOBT test result sent to wrong address – Incorrect address on requisition	Result letter returned	9/16/2010	9/16/2010	9/23/2010	No	N/A	None	N/A
72	9/21/2010	9/21/2010 - 9/23/2010	External	FOBT test result sent to wrong	Result letter returned	9/21/2010	9/21/2010	9/23/2010	No	N/A	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				address – Incorrect address on requisition								
73	9/21/2010	9/21/2010 - 9/23/2010	External	FOBT test result sent to wrong address – Ineligible address on requisition	Recipient shredded the letter	9/21/2010	9/21/2010	9/23/2010	Yes	9/23/2010 - 9/28/2010	None	N/A
74	9/22/2010	9/22/2010 - 9/23/2010	External	FOBT test result sent to wrong address – Lab Data entry	Recipient provided the letter to the participant	9/22/2010	9/22/2010	9/23/2010	Yes	9/23/2010 - 9/28/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				error								
75	9/27/2010	9/27/2010 - 9/28/2010	External	FOBT test result sent to wrong address – NCOA	Result letter returned	9/27/2010	9/27/2010	9/28/2010	Yes	9/28/2010 - 10/03/2010	None	N/A
76	9/30/2010	9/30/2010 - 10/4/2010	External	FOBT test result sent to wrong address – NCOA	Recipient shredded the letter	9/30/2010	9/30/2010	10/4/2010	Yes	10/4/2010 - 10/9/2010	None	N/A
77	10/5/2010	10/5/2010	External	FOBT test result sent to wrong address – Incorrect address on requisition	Recipient shredded the letter	10/5/2010	10/5/2010	10/5/2010	Yes	10/5/2010 - 10/10/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
78	10/14/2010	10/14/2010	External	FOBT test result sent to wrong address – NCOA	Result letter returned	10/14/2010	10/14/2010	10/14/2010	Yes	10/14/2010 - 10/19/2010	None	N/A
79	11/2/2010	11/2/2010 - 11/7/2010	External	FOBT test result sent to wrong address – Incorrect address on requisition	Result letter returned	11/2/2010	11/2/2010	12/1/2010	No	12/1/2010 - 12/6/2010	None	N/A
80	11/11/2010	11/11/2010	Internal	FOBT test result sent to wrong address – InScreen migratio	Result letter returned	11/11/2010	11/11/2010	11/11/2010	Yes	11/11/2010 - 11/16/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				n error								
81	11/29/2010	11/29/2010 - 12/04/2010	External	FOBT test result sent to wrong address – Lab Data entry error	Result letter returned	11/29/2010	11/29/2010	12/6/2010	Yes	12/6/2010 - 12/11/2010	None	N/A
82	12/6/2010	12/6/2010	External	FOBT test result sent to wrong address – Lab Data entry error /ineligible requisition	Result letter returned	12/6/2010	12/6/2010	12/6/2010	Yes	12/6/2010 - 12/11/2010	None	N/A
83	12/21/2010	12/21/2010	External	FOBT sent to wrong	Result letter	12/21/2010	12/21/2010	12/21/2010	Yes	12/21/2010 - 12/26/2010	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				address as participant moved and did not update the address with any of the healthcare providers	returned							
84	1/4/2011	1/4/2011	External	FOBT sent to wrong address	Result letter returned	1/4/2011	1/4/2011	1/4/2011	Yes	1/4/2011 - 1/13/2011	None	N/A
85	1/18/2011	1/18/2011 – 1/23/2011	External	FOBT sent to wrong address	Result letter returned	1/18/2011	1/18/2011	1/31/2011	Yes	1/24/2011 - 1/29/2011	None	N/A
86	1/26/2011	1/26/2011 - 2/1/2011	External	FOBT recall sent to wrong	Recall letter returned	1/26/2011	1/26/2011	2/4/2011	No	N/A	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				address								
87	1/27/2011	1/27/2011 - 2/2/2011	External	FOBT result sent to wrong address	Letter returned	1/27/2011	1/27/2011	3/3/2011	Yes	2/17/2011-2/22/2011	None	N/A
88	2/10/2011	2/10/2011 - 2/15/2011	External	FOBT result sent to wrong address	Letter shredded	2/10/2011	2/10/2011	2/10/2011	No – Client refused to provide his new address	N/A	None	N/A
89	2/11/2011	2/11/2011 - 2/16/2011	External	FOBT recall letter sent to the wrong address	Letter Shredded	2/11/2011	2/11/2011	3/22/2011	No	N/A	None	N/A
90	2/14/2011	2/14/2011 - 2/17/2011	External	FOBT reminder letter sent to the wrong address	Letter shredded	2/14/2011	2/14/2011	2/17/2011	No	N/A	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				– PCP provided wrong address								
91	2/14/2011	2/14/2011 - 2/17/2011	External	FOBT result sent to the wrong address – Incorrect address on the requisition	Letter returned	2/14/2011	2/14/2011	2/17/2011	Yes	2/14/2011 - 2/19/2011	None	N/A
92	2/22/2011	2/22/2011 - 2/27/2011	External	FOBT sent to the wrong address – Incorrect address received from Lab	Letter Returned	2/22/2011	2/22/2011	3/1/2011	Yes	2/27/2011 - 3/1/2011	None	N/A
9	2/23/2011	2/23/2011 -	External	FOBT Recall/R	Letter Returne	2/23/2011	2/23/2011	3/3/2011	Yes	2/28/2011 –	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
3		2/28/2011		eminder sent to wrong address – Incorrect address provided by Lab	d					3/3/2011		
94	3/1/2011	3/1/2011 - 3/5/2011	External	FOBT Recall/Reminder	Letter Returned	3/1/2011	3/1/2011	3/1/2011	No	N/A	None	N/A
95	3/8/2011	3/13/2011	External	FOBT test result sent to wrong address – Incorrect address received from Laboratory	Letter Returned	3/8/2011	3/8/2011	3/24/2011	Yes	3/19/2011 - 3/24/2011	None	N/A
96	3/14/2011	3/14/2011 - 3/18/2011	External	FOBT Recall/Reminder	Letter shredde	3/14/2011	3/14/2011	3/18/2011	Yes	3/14/2011 - 3/18/2011	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				sent to incorrect address	d							
97	3/14/2011	3/14/2011 - 3/19/2011	External	FOBT Recall/Reminder Letter – InScreen Migration Error	Letter Shredded	3/14/2011	3/14/2011	3/29/2011	No – Unable to locate the client	N/A	None	N/A
98	4/6/2011	4/6/2011 - 4/11/2011	External	FOBT Result sent to wrong address – Incorrect address received from laboratory	Letter Returned	4/6/2011	4/6/2011	4/21/2011	No – Unable to confirm the correct address	N/A	None	N/A
99	4/20/2011	4/20/2011 - 4/23/2011	External	FOBT result sent to wrong address	Letter Shredded	4/20/2011	4/20/2011	4/21/2011	Yes	4/20/2011 - 4/21/2011	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
100	4/26/2011	4/26/2011 - 4/28/2011	External	FOBT Result sent to the wrong address – PCP provided incorrect address	Letter Returned	4/26/2011	4/26/2011	4/27/2011	Yes	4/26/2011 - 4/27/2011	None	N/A
	4/26/2011	5/25/2011 – 5/1/2011	External	Reportscontaining PHI was misplaced by Canada Post	Contact every physician to confirm receipt of report.	Ongoing	4/26/2011	Ongoing	Ongoing	Ongoing	N/A	N/A
101	5/2/2011	5/4/2011	External	FOBT result letter sent to wrong address – Lab provided incorrect address	Letter Returned	5/2/2011	5/2/2011	5/3/2011	Yes	5/2/2011-5/4/2011	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
102	5/3/2011	5/3/2011 - 5/8/2011	External	FOBT result sent to wrong address – PCP provided incorrect address	Letter Returned	5/3/2011	5/3/2011	6/1/2011	No – Unable to locate the client	N/A	None	N/A
103	5/9/2011	5/9/2011 - 5/13/2011	External	FOBT Recall/Reminder – Wrong address in the system	Letter Shredded by client	5/9/2011	5/9/2011	5/11/2011	No – Unable to locate the client	N/A	None	N/A
104	5/10/2011	5/10/2011 - 5/17/2011	External	FOBT Result to wrong address – Laboratory data entry error	Letter Returned	5/10/2011	5/10/2011	5/17/2011	Yes	5/12/2011 - 5/17/2011	None	N/A
10	5/11/2011	5/11/2011 - 5/15/2011	External	FOBT Recall/R	Letter Returne	5/11/2011	5/11/2011	5/3/2011	No	N/A	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
5				eminder	d							
106	5/12/2011	5/12/2011 - 5/15/2011	External	FOBT result letter – Laboratory provided incorrect address	Letter Returned	5/12/2011	5/12/2011	5/13/2011	Yes	5/12/2011 - 5/15/2011	None	N/A
107	5/17/2011	5/17/2011 - 5/22/2011	External	FOBT result sent to the wrong address – PCP office provided incorrect address	Letter Returned	5/17/2011	5/17/2011	6/13/2011	No – Unable to locate the client	N/A	None	N/A
108	5/24/2011	5/24/2011 - 5/29/2011	External	FOBT result sent to wrong address – Incorrect address	Letter Returned	5/24/2011	5/24/2011	6/13/2011	No – Unable to locate the client	N/A	None	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
				on the requisition								
109	5/31/2011	5/31/2011 - 6/5/2011	External	FOBT result to wrong address – NCOA change	5/31/2011	Letter Returned	5/31/2011	6/6/2011	Yes	5/31/2011 – 6/6/2011	None	N/A
110	6/01/2011	6/01/2011	External	Canada Post cannot confirm the delivery of SAR physician packages	No further SAR's sent	N/A	6/14/2011	8/23/2011	Yes	07/25/2011 -	Yes	TBC – once IPC releases finding of their review.
111	6/2/2011	6/2/2011 - 6/7/2011	External	FOBT result sent to wrong address – NCOA changed the address	None	N/A	6/2/2011	Ongoing	N/A	N/A	N/A	N/A

Breach #	Date of Incident	Date Senior Management was Notified (date range provided)	Internal vs External	Nature of PHI	Containment Measure	Date of Containment	Date Investigation Commenced	Date Investigation Completed	Notification Provided to individual	Date notification provided (date range provided)	Recommendation	Date of Recommendation completion and the manner it was addressed.
112	6/14/2011	6/14/2011 - 6/19/2011	External	FOBT result sent to wrong address	N/A	N/A	6/14/2011	Ongoing	N/A	N/A	N/A	N/A
113	6/15/2011	6/15/2011 - 6/20/2011	External	FOBT result sent to the wrong address	Letter Returned	6/15/2011	6/15/2011	Ongoing	N/A	N/A	N/A	N/A

.

APPENDIX 5 to Indicators – Summary from Log of Privacy Complaints

No.	Date of Complaint	Nature of Complaint	Date Investigation Commenced	Date Letter sent Regarding Commencement of Investigation	Date Investigations Completed	Recommendation	Date Recommendation addressed	Manner Recommendation was addressed	Date of Letter describing Resolution
1	1/17/2011	CCC Birthday Letter	1/17/2011	None - complainant was provided response over the phone	1/17/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.
2	1/18/2011	CCC Birthday Letter	1/18/2011	None - complainant was provided response over the phone	1/18/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.
3	1/18/2011	CCC Birthday Letter	1/18/2011	None – Client refused to provide her name or mailing address	1/18/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.
4	1/20/2011	CCC Birthday Letter	1/20/2011	None – Client refused to provide her name or mailing address	1/20/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.

No.	Date of Complaint	Nature of Complaint	Date Investigation Commenced	Date Letter sent Regarding Commencement of Investigation	Date Investigations Completed	Recommendation	Date Recommendation addressed	Manner Recommendation was addressed	Date of Letter describing Resolution
5	1/24/2011	CCC Birthday Letter	1/24/2011	IPC notified that complaint is being investigated	3/2/2011	• Update Contact Centre FAQs and retrain staff. • Privacy FAQs to be added to B-day letter • Birthday letter to include instruction on how to withdraw from the correspondence	3/5/2011 – ongoing	• FAQs were updated. • Privacy FAQs and instruction to withdraw have been added to the birthday letter.	3/2/2011
6	1/26/2011	CCC Birthday Letter	1/26/2011	None – Client refused to provide her name or mailing address	1/26/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.
7	1/28/2011	CCC Birthday Letter	1/28/2011	None – Client refused to provide her name or mailing	1/28/2011	None	N/A	N/A	N/A – Complainant query addressed

No.	Date of Complaint	Nature of Complaint	Date Investigation Commenced	Date Letter sent Regarding Commencement of Investigation	Date Investigations Completed	Recommendation	Date Recommendation addressed	Manner Recommendation was addressed	Date of Letter describing Resolution
				address					on phone.
8	2/4/2011	CCC Birthday Letter	2/4/2011	None	2/4/2011	None	N/A	N/A	2/9/2011 (withdrawal of confirmation letter was sent)
9	2/9/2011	CCC Birthday Letter	2/9/2011	None	2/9/2011	None	N/A	N/A	2/9/2011 (withdrawal of confirmation letter was sent)
10	2/9/2011	CCC Birthday Letter	2/9/2011	None – Client refused to provide her name or mailing address	2/9/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.
11	2/10/2011	CCC Birthday Letter	2/10/2011	None	2/10/2011	None	N/A	N/A	2/10/2011 (withdrawal of confirmation letter was

No.	Date of Complaint	Nature of Complaint	Date Investigation Commenced	Date Letter sent Regarding Commencement of Investigation	Date Investigations Completed	Recommendation	Date Recommendation addressed	Manner Recommendation was addressed	Date of Letter describing Resolution
									sent)
12	2/14/2011	CCC Birthday Letter	2/14/2011	None – Client refused to provide her name or mailing address	2/14/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.
13	2/14/2011	CCC Birthday Letter	2/14/2011	None	5/3/2011	None	N/A	N/A	5/3/2011
14	2/17/2011	CCC FOBT result letter	2/17/2011	None	3/4/2011	None	N/A	N/A	3/4/2011
15	2/22/2011	CCC Birthday Letter	2/22/2011	None	2/22/2011	None	N/A	N/A	2/25/2011 (withdrawal of confirmation letter was sent)
16	2/28/2011	CCC Birthday Letter	2/28/2011	None	2/28/2011	None	N/A	N/A	2/28/2011 (withdrawal of

No.	Date of Complaint	Nature of Complaint	Date Investigation Commenced	Date Letter sent Regarding Commencement of Investigation	Date Investigations Completed	Recommendation	Date Recommendation addressed	Manner Recommendation was addressed	Date of Letter describing Resolution
									confirmation letter was sent)
17	3/10/2011	CCC Birthday Letter	3/10/2011	None	3/10/2011	None	N/A	N/A	3/10/2011 (withdrawal of confirmation letter was sent)
18	3/22/2011	CCC Birthday Letter	3/22/2011	None – individual provided response on the phone	3/22/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.
19	4/4/2011	CCC Birthday Letter	4/4/2011	None – Client refused to provide her name or mailing address	4/4/2011	None	N/A	N/A	N/A – Complainant query addressed on phone.
20	4/8/2011	CCC Birthday Letter	4/8/2011	None	4/12/2011	None	N/A	N/A	4/12/2011 (withdrawal of confirmation

No.	Date of Complaint	Nature of Complaint	Date Investigation Commenced	Date Letter sent Regarding Commencement of Investigation	Date Investigations Completed	Recommendation	Date Recommendation addressed	Manner Recommendation was addressed	Date of Letter describing Resolution
									letter was sent)

APPENDIX 6 to Indicators – Summary from the Log of Security Audits

Project	Type of Audit	Date Completed	Recommendations Descriptions	Mitigation Dates
Lab Interim Reporting Tool (LIRT)	TRA	Jul-08	Recommendations are logged within each assessment.	Mitigation dates typically coincide with dates of assessments.

APPENDIX 7 to Indicators – Summary from the Log of Information Security Breaches

	Incident Description	Date of Incident	Extent of Incident	PHI	Breach	Senior Management Notification Date	Containment Measures	Containment Date	External Notification Date	Investigation Dates (start to finish)	Recommendations	Date of Implementation of Recommendations	Manner of Implementation of Recommendations
1	An out-dated user role was assigned to WTIS users, allowing access to data no longer needed by the users	3-Dec-08	High	Yes	Yes	3-Dec-08	Gateway access was shut down	3-Dec-08	N/A	3-Dec-08	Remove old user access groups	3-Dec-08	Ran a script to remove old user access groups within the WTIS application
2	Dormant accounts discovered for individu	15-Dec-09	Low	No	Yes	15-Dec-09	Disabled dormant accounts; verified inactivity after employee	15-Dec-09	N/A	Dec 15-18, 2009	Manager training on exit processes; process gap analysis; AD cleanup	Already underway before incident	Service Desk-driven training for managers; updated account termination

	Incident Description	Date of Incident	Extent of Incident	PHI	Breach	Senior Management Notification Date	Containment Measures	Containment Date	External Notification Date	Investigation Dates (start to finish)	Recommendations	Date of Implementation of Recommendations	Manner of Implementation of Recommendations
	als no longer with CCO						exits						processes; AD cleanup
3	Virus instance affecting the network	15-Jul-10	Low	No	No	15-Jul-10	Disconnect infected PC and others as a precaution; verified blocking of outbound traffic to prevent data leakage	15-Jul-10	N/A	July 15-19, 2010	Re-image infected PC; review policies with user	15-Jul-10	PC was re-imaged
4	Missing loaner laptop (not reported until Aug 26, 2010)	25-Aug-10	Low	No	No	26-Aug-10	Verified absence of PHI	26-Aug-10	N/A	Aug 26-31, 2010	Enable whole disk encryption on all loaner laptops	1-Jul-11	Upgrade from Windows XP to Windows 7 and enable BitLocker

	Incident Description	Date of Incident	Extent of Incident	PHI	Breach	Senior Management Notification Date	Containment Measures	Containment Date	External Notification Date	Investigation Dates (start to finish)	Recommendations	Date of Implementation of Recommendations	Manner of Implementation of Recommendations
5	Malware detected on VP laptop (infection on Sept 4, 2010; automated notification on Sept 7, 2010)	4-Sep-10	High	No	No	7-Sep-10	Verified currency of AV protection and lack of outbound/remote activity	7-Sep-10	N/A	Sept 7-9, 2010	Re-image laptop	Sept 8-9, 2010	Re-image laptop
6	Laptop left on GO Train (lost Jan 28, 2011; reported Feb 2, 2011)	28-Jan-11	Low	No	No	2-Feb-11	Verified that whole disk encryption was enabled on the laptop; verified absence of PHI	2-Feb-11	N/A	Feb 2-3, 2011	Educate user on safeguarding CCO assets and prompt incident reporting	3-Feb-11	Laptop was returned to CCO on Feb 3, 2011; user was advised regarding care of CCO assets and incident reporting

	Incident Description	Date of Incident	Extent of Incident	PHI	Breach	Senior Management Notification Date	Containment Measures	Containment Date	External Notification Date	Investigation Dates (start to finish)	Recommendations	Date of Implementation of Recommendations	Manner of Implementation of Recommendations
7	Personal mobile phone connected to CCO email was lost (lost Feb 4, 2011; reported Feb 7, 2011)	4-Feb-11	Low	No	No	7-Feb-11	User promptly disabled the SIM card by calling his service provider; verified that password protection and device encryption were enabled	4-Feb-11	N/A	Feb 4-7, 2011	Ensure users know to contact CCO Service Desk first to issue a remote wipe command	7-Feb-11	User was advised to contact Service Desk first in the future; user was also shown how to issue a remote wipe command himself
8	Phishing email sent to VP and reported by VP	14-Feb-11	Low	No	No	14-Feb-11	Phishing site was added to blacklist; submitted site to Microsoft and Google for analysis and filtering	14-Feb-11	N/A	14-Feb-11	Update security awareness training	Q1 2011	Updated security awareness training

	Incident Description	Date of Incident	Extent of Incident	PHI	Breach	Senior Management Notification Date	Containment Measures	Containment Date	External Notification Date	Investigation Dates (start to finish)	Recommendations	Date of Implementation of Recommendations	Manner of Implementation of Recommendations
9	Missing projector (noticed as missing on March 1, 2011)	Sometime after Feb 3, 2011	Low	No	No	1-Mar-11	N/A	N/A	N/A	N/A (Facilities Investigation)	Update incident management program with physical security concerns	TBD	TBD
10	Laptop left on GO Train	10-Jun-11	Low	No	No	10-Jun-11	Verified that whole disk encryption was enabled on the laptop; verified absence of PHI; user's accounts were disabled	10-Jun-11	N/A	10-Jun-11	N/A	N/A	N/A

	Incident Description	Date of Incident	Extent of Incident	PHI	Breach	Senior Management Notification Date	Containment Measures	Containment Date	External Notification Date	Investigation Dates (start to finish)	Recommendations	Date of Implementation of Recommendations	Manner of Implementation of Recommendations
11	Unusual behavior caused by an automated process detected through auditing and monitoring (activity on July 11, 2011; detection on July 12, 2011)	11-Jul-11	Low	No	No	12-Jul-11	Contacted user for more information; disabled the account in question	15-Jul-11	N/A	July 12-15, 2011	TBD	TBD	TBD

CONCLUSION

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of the PHI that it maintains. CCO meets these commitments through its comprehensive and multi-faceted privacy program. As 2008 triennial review of CCO's practices and procedures, with respect to its role as a prescribed person, CCO has strived to improve and expand its Privacy Program to enrich its capacity to protect the privacy of those individuals whose PHI we hold and to ensure that CCO's privacy and security infrastructure is at the leading edge of industry standards.

CCO has demonstrated compliance with the IPC's requirements through its privacy program, which is supported by numerous departments across the organization. Specifically, the interplay of the governing documents implemented and maintained by the Privacy & Access Office, the Enterprise Information Security Office, Office of the Chief Information Officer, the Procurement Office, Facilities Department and the Legal and the Human Resources Departments, ensure that CCO has in place a robust privacy program and a strong culture of privacy and security across the entire organization.

The following is a summary of the measures to be implemented, and the timelines for implementation, to fully meet the requirements as provided by the IPC:

Documentation	IPC Requirement	CCO Enhancement	Timelines for Implementation
Security	**Requirement 6:** Policy and Procedures for Secure Retention of Records of PHI on Mobile Devices	Development of *Remote Access Standard* *Information Classification and Handling Standard* (Draft) *Information Classification and Handling Guideline* (Draft)	Completion Date: 2012
	Requirement 7: Policy and Procedures for Secure Transfer of Records of PHI	*Information Classification and Handling Standard* (Draft) *Information Classification and Handling Guideline* (Draft)	Completion Date: 2012
Organizational and Other Documentation	**Requirement 4:** Corporate Risk Management Framework	Implementing a Privacy Risk Management Standard	Completion Date: 2012

APPENDIX A – SUPPORTING DOCUMENTATION

1. ***CCO's Acceptable Use of Social Media Policy*** outlines the expected behaviour for CCO Employees participation in, and use of, Social Media.

---

2. **CCO's Access Card Procedure** outlines the procedures that must be followed by all Cancer Care Ontario staff, including employees, students, third party service providers, secondees to CCO and independent contractors working for or on behalf of CCO (collectively, "CCO Staff") with respect to the use of CCO Photo ID and elevator access cards.

---

3. ***CCO's Acquisition, Development, and Application Security Standard*** defines the baseline for the acquisition and development phase in which applications are procured, designed, customized or developed.

---

4. ***CCO's Application for Disclosure for Information from CCO for Research Purposes*** is used specifically for researchers. It sets out the terms and conditions that a researcher must abide by when using PHI disclosed by CCO. This Application, along with the CCO Non-disclosure/Confidentiality Agreement, forms the agreement between CCO and a researcher.

---

5. ***CCO's Architecture Review Board (ARB) Terms of Reference*** sets out the responsibilities of the ARB. The ARB is an approval board for CCO Enterprise Architecture and Information Technology Standards. One of the ARB's responsibilities to certify the physical design of a project is internally consistent and in alignment with the logical architecture and information, application, technology and security standards and methods.

---

6. ***CCO's Authorization to Access Data Centre Contractor Form*** is required to be completed by all CCO contractors who require specific access to data centres. The Form tracks the type of access granted to the data centre, the reasons for the access request, and it requires the signatures of the IT Manager, CTO and contractor.

---

7. ***CCO's Authorization to Access Data Centre Employee Form*** is required to be completed by all CCO employees who require specific access to data centres. The Form tracks the type of access granted to the data centre, the reasons for the access request, and it requires the signatures of the IT Manager, CTO and employee.

---

8. ***CCO's Business Continuity and Disaster Recovery Plan*** guides the business continuity and recovery operations for mission critical processes and services in the event of a disaster that compromises the ability for to meet minimum production requirements. Specifically, it provides all of the necessary lists, tasks, and reports used for response, resumption, or recovery in the event of a disaster. Additionally, it defines the roles and responsibilities for assigning available personnel and the activities to be conducted during each phase of a disaster. Lastly, contact processes for the fan out phase are delineated, message templates are included, system recovery dependencies, system recovery approaches for the class of services, vendor and key staff contact information, and routine recovery tests are also found in the appendices.

---

9. ***CCO's Business Continuity and Discovery Recovery Test Strategy for 2011/2012*** is a comprehensive test strategy for the implementation of the Business Continuity and Disaster Recovery Plan which includes a telephone procedure to notify Technology Services staff of an emergency out of business hours. It is supported by new upgrades to the Emergency Preparedness Database (EPD), specifically with respect to the creation of lists of staff and their relevant contact information. This list can be emailed or printed and delivered to managers to utilize to call and log contact success. Communication and training plans will be developed to supplement the Test Strategy.

---

10. ***CCO's Business Continuity Service Framework*** contains supporting information for the Business Continuity and Disaster Recovery Plan that is constant and not subject to frequent revisions. This document describes types of disaster scenarios and how Technology Services would move from operations to a continuity focus during time of a business disruption or disaster. It outlines the phases of a disaster from response through to restoration.

---

11. ***CCO Board of Director's Orientation Handbook*** is provided to all CCO board members annually. The Handbook provides information to board members on the history of CCO, CCO's legislative compliance, the governance and corporate structure and a description of all programs at CCO.

---

12. ***CCO's Business Process for Data Requests*** outlines the procedures for receiving, processing, filing, deferring, rejecting, logging and following up on requests for CCO data

including requests for PHI for research purposes.

---

13. ***CCO Change Advisory Board Terms of Reference*** describes role of each program area including Privacy plays in approval of changes to IT system.

14. ***CCO's Code of Conduct*** applies to all CCO employees and indentifies the principles that guide the decisions and actions of all CCO employees in order to maintain an atmosphere that is conducive to excellent work practices.

---

15. ***CCO's Confidentiality Policy*** defines confidential information and establishes the requirement for persons working for or on behalf of CCO to preserve the confidentiality of all information not normally available to the public, including all PHI.

---

16. ***CCO's Core Privacy Committee Terms of Reference*** stipulates the committee's role in respect of the privacy program at CCO. The terms of reference includes the membership of the committee, the mandate and responsibilities of the committee in respect of the privacy program, the frequency with which the committee meets, to whom the committee reports and the types of reports produced by the committee.

---

17. ***CCO's Cryptography Standard*** broadly defines the appropriate cryptographic methods for addressing security requirements and generally defines acceptable means of using or implementing such methods. Compliance with this Standard will:

    Ensure the consistent application of cryptographic safeguards across CCO;

    i. Establish a minimum baseline for cryptographic security at CCO that is in line with industry standards and best practices; and
    ii. Facilitate necessary transitions to stronger or newer cryptographic methods as older methods become obsolete.

---

18. ***CCO's Data Access Committee Terms of Reference*** outlines the major responsibilities of this committee. The Data Access Committee is responsible for ensuring data requests, including those made by researchers, are consistent with PHIPA. The Data Access Committee is also responsible for reviewing and approving data request related to the disclosure of PHI for research requests.

---

19. ***CCO's Data Backup Policy*** provides a standardized means of backing up and maintaining data that is critical to the viability and operation of CCO.

20. ***CCO's Data Backup Process and Standard*** defines the operational processes and standards relating to CCO's backup and recovery services.

21. ***CCO's Data Centre Access and Usage Policy*** provides administrative controls for accessing CCOs data centres and applies to all persons accessing the data centres. There are three levels of access to the data centre, based on the nature of work to be performed, its frequency, duration, and time of day at which access is required.

22. ***CCO's Data Linkage Standard*** defines the circumstances in which the data linkage of records of PHI is permitted. The Standard also outlines the purpose of linking data at CCO, and disclosure of that linked data by CCO.

23. ***CCO's Data Linkage Procedure*** describes how requests for Data Linkage of CCO records of PHI are received, processed, and completed. The Procedure includes procedures related to the disclosure of data held by CCO in its capacity as a prescribed entity and data from CCO as a prescribed registry.

24. ***CCO's Data Sharing Agreement Initiation Form*** identifies the information required for review of a proposed data exchange, in addition to identifying the appropriate the terms and conditions to be included in the completed Data Sharing Agreement (DSA).

25. ***CCO's Data Sharing Agreement Procedure*** outlines the specific processes to be followed when a data exchange with an external party is being considered by CCO, or where a new use of data, for a purpose other than that set out in an existing DSA, is proposed. The procedure prescribes the duties of each responsible party at CCO throughout the DSA lifecycle.

26. ***CCO's Data Sharing Agreement Standard*** defines the instances where a DSA is required at CCO, specifically where a data exchange with an external party is being considered or where a new use of data, for a purpose other than that set out in an existing DSA, is proposed.

27. ***CCO's Data Sharing Agreement Template*** specifies the terms and conditions that must be included in each DSA executed by CCO when collecting or disclosing PHI for purposes other than research.

28. ***CCO's Data Steward Terms of Reference*** outlines the duties and responsibilities of the individual who is accountable for oversight and management of data stewards and the data stewardship structure. Data Stewards are responsible for maintaining the privacy and security of data by monitoring access to, and use of, PHI within their assigned data holding.

---

29. ***CCO's Decision Criteria for Data Requests*** provides the criteria to be considered when determining whether to approve a request for PHI, de-identified and / or aggregate data for research purposes under section 44 of PHIPA.

---

30. ***CCO's De-Identification Guidelines*** supplement CCO's Data Use & Disclosure Standard to enable employees to more clearly identify if individuals may be re-identified if data with small cell is disclosed. Analysts and developers use the Guidelines when they are asked to disclose reports or data sets containing de-identified information.

---

31. ***CCO's Digital Media Disposal Guideline*** sets forth the recommended practices for securely disposing digital storage media and/or the information contained within.

---

32. ***CCO's Direct Data Access Procedure*** describes the process and tool (**ODDAR**) used to request direct access to CCO data holdings of PHI for all internal users, including CCO employees, consultants and contractors. Specifically, the procedure prohibits access to or use of more PHI than is reasonably necessary to meet the identified purpose, sets out the process for approving or denying a request for access to and use of PHI and identifies the conditions or restrictions for internal users who have been granted approval to access and use PHI.

---

33. ***CCO's Direct Data Access Audit Procedure*** describes the process that is to be used to audit direct access to CCO data holdings. It applies to all data holdings under the care and custody of CCO and outlines the responsible departments for completing the audits.

---

34. ***CCO's Employee Exit Process*** ensures that a systematic uniform exit procedure is followed for all employees and volunteers, upon the cessation of their employment or other

relationship with CCO. The process sets out the roles and responsibilities of departing employees, volunteers, managers and other departments, including the return of CCO property and deactivation of system access permissions, upon cessation of the individual's employment, volunteer or other relationship.

---

35. ***CCO's Employee Exit Checklist*** includes a list of action items for managers to complete when an individual's employment, volunteer or other relationship with CCO has ended.

---

36. ***CCO's IM/IT Stage-Gating Policy*** outlines the process each IM/IT project need to undergo for completion of the project. The policy also outline privacy stream, which identify privacy artifacts required for completion of the project.

---

37. ***CCO's Information Classification and Handling Guideline*** (Draft) applies to all information owned by, or under the custody or control of CCO. This document provides guidelines for the implementation of the *Information Classification and Handling Standard*, providing instructions and examples on how to:

    i. Classify CCO information assets; and

    ii. Protect information assets during its lifecycle (e.g. creation, storage, transmission, transport and disposition).

---

38. ***CCO's Information Classification and Handling Standard*** (Draft) specifies requirements for the classification and handling of information within CCO. The purpose of the Standard is to:

    i. Provide an information classification scheme that is consistent with CCO's privacy and security policies and legislative requirements outlined in PHIPA and FIPPA;

    ii. Enable employees to quickly and easily identify and classify information and assets; and

    iii. Promote the implementation of appropriate security measures.

---

39. ***CCO's Incident Management Framework*** establishes a series of pre-determined process steps which are initiated when CCO is notified about a potential incident which either threatens or could threaten the confidentiality, integrity or availability of CCO's information assets.

40. ***CCO's Information Management Coordinator Terms of Reference*** outlines the major responsibilities of this job role. The Information Management Coordinator manages the Data Use & Disclosure Standard, and monitors adherence to the Privacy and Data Use & Disclosure Standard. Specifically, the Information Management Coordinator works with researchers to ensure the conditions or restrictions imposed on the disclosure of PHI for research purposes are being satisfied.

41. ***CCO's Information Security Code of Conduct*** supports CCO's commitment to safeguarding its information assets by establishing clear behavioural expectations for authorized individuals using CCO information systems and assets. This Code of Conduct fosters an understanding of security practices at CCO, including a practical understanding of the expectations of individuals who, in the course of their work at CCO, must protect the information they create, use, access, disclose or otherwise manage. The document defines high level principles, provides pertinent examples of accepted behaviour, and establishes the responsibilities of management and employees.

42. ***CCO's Information Security Framework*** defines the foundational components of the information security program and contains informational elements useful to the understanding and administration of the program.

43. ***CCO's Information Security Policy*** is a framework of enforceable rules and best practices that regulate how CCO and its employees collaboratively support the enterprise information security objectives at all organizational levels. The policy is a concise statement of the requirements that must be met in order to satisfy those objectives, including:

    i. The safeguarding of sensitive information assets and service assets;
    ii. Documenting the corporate consensus on baseline information security;
    iii. Managing organizational information security risks;
    iv. Supporting CCO's policies and legislative compliance requirements;
    v. Defining information security roles and responsibilities within CCO; and
    vi. Defining and authorizing the consequences of violating the policy.

This governing policy is supported by a hierarchy of standards, procedures and guidelines.

44. ***CCO's Information Security Program Plan 2010-2011*** is a planning document, refreshed on an annual basis, to provide a strategic framework within which the CCO information security program operates. The document itself contains three main components:

    i. EISO Description and Program Goals: introduces the current security program organization, goals and components that constitute the foundational elements of the Enterprise Information Security Office;

    ii. Program Details: describes the information security program plan, approach and implementation phases which follow the ISO 27001:2005 standard for Information Security Management Systems (ISMS); and

    iii. Scheduled Projects and Work: highlights key work planned for the fiscal year.

---

45. ***CCO's Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program.*** CCO has detailed job descriptions for positions which have been delegated day-to-day duties with respect to the operations of its Privacy Program, including descriptions for the:

    - Director, Privacy & Access
    - Privacy Team Lead
    - Senior Privacy Specialist
    - Privacy Specialist

---

46. ***CCO's Job Description for the Positions (s) Delegated Day-to-Day Authority to Manage the Security Program.*** CCO has prepared detailed job descriptions for positions which have been delegated day-to-day duties with respect to the operations of its Security Program, including descriptions for the:

    - Senior Information Security Specialist/Security Architect
    - Intermediate Information security Specialist
    - Associate Information Security Specialist
    - Security Team Lead

---

47. ***CCO's Logging, Monitoring, and Auditing Standard*** defines the logging, monitoring and auditing requirements for CCO IT systems. The objectives are to:

    i. Monitor accountability of users actions using IT systems;

    ii. Detect unauthorized and inappropriate access to sensitive information (e.g. personal health information);

iii. Detect information security incidents in a timely manner; and

iv. Provide forensic evidence for investigations of unauthorized or inappropriate use of CCO assets.

---

48. ***CCO's Logical Access Control Standard*** sets the baseline security requirements for access control to systems and applications owned by, or under the security control of CCO. The objectives of the Standard are to:

i. Ensure compliance with both regulatory requirements and CCO's Information Security policies with regards to the protection of confidentiality, integrity and availability of information;

ii. Promote a culture in which responsibility for the use of IT resources is understood and users are held accountable for their actions; and

iii. Defines identification and authentication controls for logical access to information, computing resources and network facilities.

---

49. ***CCO's Media Destruction Policy and Procedure*** defines the requirements and process for the destruction of data storage media, prior to disposal or re-use, of all CCO data stored on magnetic or optical data storage media. Specifically, it stipulates that all CCO employees, contractors, consultants and suppliers are to provide all data storage media to the Office of the Chief Technology Officer so it can be destroyed in a secure manner, consistent with industry standards.

---

50. ***CCO's New Employee Facilities & Information Technology Services Form*** is required to be completed by all new employees at CCO (including permanent full time employees, permanent part time employees, consultants, contractors, students, temporary employees and guest accounts). The Form tracks all related new employee information such as assigned business equipment, email account name, remote access capability, as well as the employee's access privileges within the CCO premises.

---

51. ***CCO's Non-Disclosure/Confidentiality Agreement*** is used when CCO discloses information to researchers for research studies under section 44 of PHIPA. This Agreement sets out the terms and conditions pertaining to the protection of information provided by CCO to a researcher.

---

52. ***CCO's Operational Security Standard*** sets baseline security requirements for secure operations of network and computing resources owned by, or under the control of CCO. In particular, this Standard aims to promote the following goals:

i. Compliance with regulatory requirements and CCO's Information Security policies with regards to the protection of confidentiality, integrity and availability of information;

ii. Define requirements for the secure operations of computing resources and network facilities (e.g. vulnerability management, change management, etc.).

---

53. ***CCO's Personnel Action Form (PAF)*** must be completed by managers and sent to CCO's Human Resources Department when a new employee is hired, when an employee transfers to another department, or when an employee is departing or taking a leave of absence, For new employees, the form must be completed and provided to the Human Resources Department once the candidate has accepted CCO's offer of employment.

---

54. ***CCO's Photo ID Request Form*** is required to be completed by all CCO employees. Photo ID cards are required in order to be granted access into all CCO buildings.

---

55. ***CCO's Preliminary Privacy Assessment Form (PPAF)*** determines whether an initiative involves the collection, use or disclosure of PHI), in addition to determining whether a PIA is required.

---

56. ***CCO's Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario***, **4th edition,** also known as the CCO Privacy Policy, applies to CCO in its capacity as a Section 45 prescribed entity under PHIPA as well as Section 39 prescribed person in respect of Ontario Cancer Screening Registry.

    CCO's Privacy Policy is structured around the 10 privacy principles set out in the Canadian Standards Association *Model Code for the Protection of Personal Information ("CSA Model Code")*. This Policy provides a general statement of CCO's position on each of the principles.

    Each principle identifies the related supporting standards and procedures documents for operationalizing the principle in the CCO context.

---

57. ***CCO's Privacy and Security Training and Awareness Procedure*** provides that all new CCO employees, service providers and other representatives such as consultants, students, volunteers and researchers with access to CCO systems, are advised of their privacy and security obligations through training and contractual means. It also describes the annual refresher training requirement for all CCO system users. Lastly, it outlines the repercussions for not completing the Privacy and Security Training.

---

58. ***CCO's Privacy and Security Training and Awareness Acknowledgement form*** must be read and electronically accepted by all CCO employees, contractors, volunteers and students upon completion of privacy and security training. Acceptance of this signifies that the user agrees to the privacy and security responsibilities and obligations outlined in the form.

---

59. ***CCO's Privacy Audit and Compliance Standard*** describes how CCO reviews and measures the effectiveness of its information management practices, including the operational practices employed in the collection, use and disclosure of PHI by CCO, to ensure compliance with CCO's Privacy Policy and its supporting standards, procedures and guidelines.

---

60. ***CCO's Privacy Breach Management Procedure*** describes the manner in which CCO will identify, manage and resolve privacy breaches resulting from the misuse or improper / unauthorized collection, use and disclosure of PHI that contravene PHIPA and/or CCO's Privacy Policies and procedures. Specifically, the procedure defines a privacy breach, imposes a mandatory requirement on CCO employees, consultants and contractors to notify CCO of a privacy breach, identifies when parties must be notified of a privacy breach, and outlines the steps to be taken by CCO once a privacy breach has occurred, including the nature and scope of the investigation of the breach.

---

61. ***CCO's Privacy Impact Assessment Standard*** requires that CCO conduct and review Privacy Impact Assessments (PIA) on existing and proposed data holdings involving PHI, it describes the components of a PIA, when it is required at CCO, the scope of the assessment, the responsibilities of various departments for conducting PIAs at CCO and the process and responsibilities for implementing PIA recommendations.

---

62. ***CCO's Privacy Training Curriculum*** informs CCO employees of their privacy responsibilities and obligations as a result of their employment with CCO. It includes a description of the status of CCO under PHIPA, the nature of the PHI collected, the purposes for the collection and use of PHI, an overview of the CCO Privacy Program, CCO's privacy policies, procedures and practices, a review of privacy breach management at CCO along with each employees duties and responsibilities in the event of a privacy breaches, and lastly the safeguards implemented by CCO to protect PHI. Training curricula are reviewed annually and updated to reflect changes in CCO's Privacy Program and current privacy related events/issues.

---

63. ***CCO's Procurement Documentation and Records Management Procedure*** supplements CCO's *Procurement of Goods and Services Policy*, to describe how documentation relating to procurements at CCO, including agreements entered into between CCO and third party service providers, are to be managed.

---

64. ***CCO's Procurement of Goods and Services Policy*** ensure that CCO acquires the goods and services required to meet its business needs through the appropriate CCO procurement process.

---

65. ***CCO's Progressive Discipline Policy*** identifies the type of conduct that may result in disciplinary action and establishes the steps to be followed in the progressive discipline process. The Privacy Breach Management Procedure complements the Progressive Discipline Policy as it describes how CCO identifies, investigates, manages and resolves privacy breaches which occur as the result of misuse or improper / unauthorized disclosure of PHI by CCO employees, consultants and contractors.

---

66. ***CCO's Provision of Paging and Mobile Phone with Email*** defines the terms and conditions for authorizing personally owned mobile devices to access CCO corporate services, including a requirment for technical security controls.

---

67. ***CCO Proposal Development Team Terms of Reference*** describes role of various departments including Privacy in assessing impact of new initiatives at CCO.

---

68. ***CCO's Secondment Policy*** sets out the necessary requirements for retaining an employee from an external organization temporarily who transfers to Cancer Care Ontario (CCO) to work in a job for a defined period of time and where CCO reimburses the organization for the Secondee while the individual continues to be employed by their organization, not CCO.

---

69. ***CCO's Security Operational Standard*** sets baseline security requirements for secure operations of network and computing resources owned by, or under the control of CCO. In particular, this Standard aims to promote the following goals:

    i. Compliance with regulatory requirements and CCO's Information Security policies with regards to the protection of confidentiality, integrity and availability of information;

ii. Define requirements for the secure operations of computing resources and network facilities (e.g. vulnerability management, change management, etc.).

---

70. ***CCO's Security Risk Management Standard*** defines the approach by which CCO identifies, assesses, responds to and monitors information security risks. The standard establishes a foundation for managing security risks and delineates the boundaries for risk-based decisions within the organization. It applies strictly to the management of security risks within the purview of the Enterprise Information Security Program.

---

71. ***CCO's Security Training Curriculum*** encompasses three introductory training sessions as well as a number of role specific training sessions. The three introductory sessions include: an EISO lead Information security orientation for new employees, a foundational information security session delivered through CCO's eLearning tool, and a CIO manager training session that includes a security introduction from a management perspective. The role specific training sessions include such topics as cryptography and secure development practices. It is planned for the fiscal 2011 - 2012 year to deliver additional role specific content both in person and through the eLearning tool.

---

72. ***CCO's Statement of Confidentiality*** is an agreement between CCO and persons working for or on behalf of CCO to preserve the confidentiality of all information not normally available to the public, including all PHI that the individual has access to in the course of performing their duties or services.

---

73. ***CCO's Statement of Information Practices*** describes CCO's practices with respect to the collection, use and disclosure of PHI. It also provides information for the public on access to PHI and provides them with the Privacy & Access Office's contact information, should there be any further questions or concerns.

---

74. ***CCO's Technology Services Change Management Policy*** this policy is to control and manage changes to IT systems and services in order to support the business while minimizing the risk of reduced service quality or disruption to services.

    Change Management ensures that standardized methods and procedures are used for efficient and prompt handling of change-related incidents. It also controls and manages the implementation of the changes that are approved through the Change Management Process.

---

75. ***CCO's Technology Services Change Management Process***, Technology Services Change Management Process aims to control and manage changes to IT systems and services to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes so to minimize the impact of change-related incident upon service quality, and consequently improve the day-to-day operations of Technology Services.

---

76. ***CCO's Technology Services Data Backup Policy***, The purpose of this policy is to provide a standardized means of backing up and maintaining data that is critical to the viability and operation of CCO. It governs the data backup and restoration services provided by Technology Services.

---

77. ***CCO's Termination of Employment Policy*** ensures that employees who have had their employment with CCO terminated are approached in a fair and equitable manner. The CCO Employee Exit process and the CCO Employee Exit Check list complement the Termination of Employment Policy and describe the steps that managers must take in the case of termination of an employee.

---

78. ***CCO's Template Schedule for Third Party Agreements*** is a template schedule appended to all agreements entered into between CCO and third parties retained by CCO, such as contractors, consultants and third party service providers that will be permitted to access and use PHI. The template schedule sets out the privacy and security responsibilities of the third party in respect of PHI that it accesses, retains, transfers or disposes of on behalf of CCO, or where the third party provides electronic services to enable CCO to collect, use or disclose PHI.

---

79. ***CCO's Termination Monthly Reports*** are created by CCO's Human Resources Department. It is sent on a monthly basis and summarizes a list of all employees who are no longer with CCO. This is used to ensure that system access has been suspended/deleted for those individuals who no longer work at CCO.

---

80. ***CCO's Threat Risk Assessment Template*** is the EISO template for CCO's Threat and Risk Assessment Reports. It outlines the methodology involved in the security assessment and provides a documentation structure for capturing the analysis of assets, threats, safeguards, vulnerabilities and risks.

---

81. ***CCO's Unpaid Student Intern Policy*** sets out the necessary requirements for retaining an unpaid student intern at CCO.

---

82. ***CCO's Video Monitoring Standard*** outlines the need and purpose for the use of video monitoring technologies on CCO premises, as well as the responsibilities for implementing and reviewing this policy. The Video Monitoring Standard has been drafted in conformance with the IPC's Guidelines for Using Video Surveillance in Public Places as well as CCO's Privacy and Security policies.

---

83. ***CCO's Visitor Access Procedure*** specifies the procedures that must be followed by visitors and deliveries to CCO premises. Specifically, it stipulates the process for signing in (providing their name, date/time of their arrival and the name of the CCO employee they are visiting) and obtaining a visitor's ID badge. The Procedure requires the Facilities Manager to maintain a log (EasyLobby Visitor Grid) of all visitors to CCO's premises.

---

84. ***CCC's Access Control Procedure – Name changed to CSP's Access Control Procedure as of September 2011 - applies*** to CCO as a Section 39 prescribed person in respect of the Colorectal Cancer Screening Registry. The Procedure describes the process CCC will use to grant, deactivate, or change access to the Colorectal Cancer Screening Registry and its associated data holdings by employees, consultants and contractors. This procedure also describes how access to the Registry will be audited.

---

85. ***CCC's Data Request Procedure – Name changed to CSP's Data Request Procedure as of September 2011 -*** applies to CCO in its capacity as a Section 39 prescribed person in respect of the Colorectal Cancer Screening Registry. The procedure describes CCC's process for reviewing, deferring or rejecting, and filling requests for prescribed registry PHI made by prescribed entities, researchers, and the MOHLTC.

---

86. ***CCC's Privacy Acknowledgement Form – Name changed to CSP's Privacy Acknowledgement Form as of September 2011 - must*** be read and electronically accepted by all CSP employees, contractors, volunteers and students upon completion of privacy module specific to CSP. Acceptance of this signifies that the user agrees to the privacy responsibilities and obligations outlined in the form.

---

87. ***CCC's Privacy Breach Management Procedure – Name changed to CSP's Privacy Breach Management Procedure as of September 2011 -*** applies to CCC in its capacity as a Section 39 prescribed person in respect of the Colorectal Cancer Screening Registry. This

procedure describes how CCC will identify, manage and resolve privacy breaches which occur as the result of misuse or improper/unauthorized collection, use and disclosure of PHI by CCO employees, consultants and contractors.

Specifically, the procedure defines a privacy breach, identifies the parties which must be notified of a privacy breach, and outlines the steps to be taken by CCC once a privacy breach has occurred, including the nature and scope of the investigation of the breach.

---

88. ***CCC's Privacy FAQs – Name changed to CSP's Privacy FAQs as of September 2011 -*** are a list of frequently asked questions which the Privacy & Access Office receives regarding its privacy policies and practices in respect of the Colorectal Cancer Screening Registry. It identifies the status of CCO under PHIPA and the purposes of collection, use and disclosure of PHI within the custody and control of CCO. It also provides the Privacy & Access Office's contact information, should there be any further questions or concerns.

---

89. ***CCC's Privacy Inquiries and Complaints Procedure – Name changed to CSP's Privacy Inquiries and Complaints Procedure as of September 2011 -*** apply to CCO in its capacity as a section 39 prescribed person in respect of the CCSR. The procedure details different avenues by which the public can inquire and make complaints to the Privacy Specialist on CCC-related issues. The procedure also details steps that the Privacy Specialist must take to acknowledge, resolve and respond to inquiries and complaints, and additionally requires CCC to maintain a log of all inquiries and complaints.

---

90. ***CCC's Privacy Training Curriculum – name changed to CSP's Privacy Training Curriculum -*** applies to any CCO employees, consultants or contractors assigned to work for the CCC program. The training includes an explanation of the statutory authority to operate CCC and the Colorectal Cancer Screening Registry, CCC staff privacy obligations under PHIPA and the sanctions that will be applied if these responsibilities are not followed; and the privacy practices CCC employees, consultants and contractors are expected to employ to protect the information collected, used, disclosed, retained, and accessed via the Colorectal Cancer Screening Registry. All individuals working for, or under contract with, CCC are required to take CCO's annual privacy refresher training curriculum as well, which includes information relevant to the CCC Privacy Program.

APPENDIX B – SUPPORTING TOOLS

1. ***CCO's Contract Management System*** is a centralized repository of agreements which CCO has entered into with third party service providers together with supporting procurement related documentation.

---

2. ***CCO's Data Sharing Agreement Log*** is a log of executed Data Sharing Agreements (DSAs) in a Data Sharing Agreement Summary chart which maintains up-to-date information related to DSAs executed by CCO, such as the name of the person or organization from whom the PHI was collected or to whom the PHI was disclosed, the date the Data Sharing Agreement was executed, the date the PHI was collected or disclosed, the nature of the PHI subject to the DSA, and the retention period terms and related dates.

---

3. ***CCO's EasyLobby Visitor Grid Log*** is maintained by CCO's Facilities Department and tracks all visitors (i.e. anyone who is not an employee or authorized consultant to CCO) to CCO premises. The log records each visitor's first name, last name, company, title, check in (data and time), check out (date) and the CCO employee who is receiving the visitor.

---

4. ***CCO's KeyScan System Log*** is maintained by CCO's Facilities Department and is based on the information provided in the *New Employee Facilities & Information Technology Services* form, which documents each CCO employee's access permissions to the various floors of CCO's premises.

---

5. ***CCO's List of Data Linkages*** is maintained by the CCO's Informatics Department and tracks the approved data linkages as defined by CCO's Data Linkage Standard.

---

6. ***CCO's Privacy & Access Office Remediation Program*** includes consolidated and centralized logs which track various components of the CCO Privacy Program. Current logs include:

    i. *Log of Privacy Impact Assessments:* tracks all PIAs initiated and/or completed at CCO, including identified risks and mitiStage-Gating strategies.

    ii. *Log of Privacy and Security Training Completion:* electronically tracks the completion of the privacy and security training curriculum through the electronic acceptance of a Privacy and Security Acknowledgement form. Specifically, it electronically reconciles acceptance of the Privacy and Security Acknowledgement form against the CCO Active Directory to ensure that all users of CCO systems have met their privacy training requirements.

    iii. *Log of Third Party Service Providers with Access to PHI:* tracks agreements with third

parties that have access to PHI.

iv. *CCC's Log of Amended Policies & Procedures – Name changed to CSP's Log of Amended Policies & Procedures as of September 2011* - tracks all amendments made to CSP's privacy policies and procedures, including a description of the amendment made and the date it was communicated to CCO employees.

v. *CCC's Log of IPC Recommendations – Name changed to CSP's Log of IPC Recommendations* - tracks the recommendations arising from the IPC's triennial reviews of CSP's information management practices and the manner in which these recommendations will be addressed.

vi. *CCC's Log of Privacy Complaints and Inquiries – Name changed to CSP's Log of Privacy Complaints and Inquiries as of September 2011* tracks all inquiries and complaints received by CCO in regards to the CSP Privacy Program.

vii. *CCC's Privacy Breach Log – Name changed to CSP's Privacy Breach Log as of September 2011* tracks all privacy incidents and breaches reported at CCO, in respect of the CSP Program, including identified risks and mitigating strategies.

---

7. ***CCO's Online Direct Data Access Request*** **(ODDAR)** tool is used for the logging of internal non-research related access and use of PHI. ODDAR is a web-based interactive application allowing CCO employees to fill and submit request forms for direct data access to read and/or modify PHI within any of the existing CCO data holdings. The ODDAR tool logs the name of the employee, job title of the employee, the data holding the employee will have access to, the application that will be used by the individual to access the data, the type of database environment to be accessed, the type of data requested, the expiration of permissions to the data and the current status of the employees' access permissions.

---

8. ***CCO's Security Incident Tracking Spreadsheet*** is a log of information security breaches (including suspected breaches or "incidents").

---

9. ***CCO's VIP Payroll System*** is maintained by CCO's Human Resources Department and tracks all CCO employees who have executed CCO's Statement of Confidentiality.