For Public Distribution

Privacy & Access Office

Cancer Care Ontario

2011 Prescribed Entity 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

ACRONYMS

ATC	Access To Care
CCC	ColonCancerCheck
CCO	Cancer Care Ontario
CEO	Chief Executive Officer
CIHI	Canadian Institute for Health Information
CIO	Chief Information Officer
CPO	Chief Privacy Officer
CPOE	Computerized Physician Order Entry
CTO	Chief Technology Officer
EDW	Enterprise Data Warehouse
EDW-ALC	Enterprise Data Warehouse - Alternate Level of Care
DSA	Data Sharing Agreement
EISO	Enterprise Information Security Office
ERNI	Emergency Room National Ambulatory Reporting System Initiative
FIPPA	*Freedom of Information and Protection of Privacy Act*
ISAAC-HL7	Interactive Symptom Assessment and Collection – Health Level 7
HIC	Health Information Custodian
IPC	Information and Privacy Commissioner / Ontario
LHIN	Local Health Information Network
Manual	*Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*
MOHLTC	Ontario Ministry of Health and Long-Term Care
MOU	Memorandum of Understanding between CCO and the MOHLTC dated December 2, 2009
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
PPCIP	Provincial Palliative Care Integration Project
SCT	Stem Cell Transplant
WTIO	Wait Times Information Office

INTRODUCTION

Cancer Care Ontario (**CCO**) is the provincial agency responsible for continually improving cancer services. Formally launched and funded by the Ontario government in 1997, CCO is governed by the *Cancer Act* (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 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. 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 Tomography (**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 45(1) of PHIPA permits health information custodians to disclose PHI without consent to certain prescribed entities for the purpose of analysis or compiling statistical information with respect to the management, evaluation or monitoring of the allocation of resources to or planning for all or part of the health system, including the delivery of services (“health system planning and management purposes”), provided the prescribed entities meet the requirements of subsection 45(3).

CCO is designated as a ‘prescribed entity’ for the purposes of subsection 45(1) of the Act, under subsection 18(1) of Ontario Regulation (**O.Reg.**) 329/04. The large majority of CCO’s programs operate under its prescribed entity authority. In this capacity, CCO collects PHI from health care organizations that are directly involved in the care and treatment of patients and from government institutions and agencies, such as the MOHLTC or the Canadian Institute for Health Information (**CIHI**), for health system planning and management purposes.

Subsection 45(3) of PHIPA requires each prescribed entity to have in place practices and procedures to protect the privacy of individuals whose PHI it receives and to maintain the confidentiality of that information. Subsection 45(3) further requires each prescribed entity to ensure that these practices and procedures are approved by the Information and Privacy Commissioner/Ontario (**IPC**) on a triennial basis in order for health information custodians, and other persons authorized under PHIPA, to disclose PHI to the prescribed entity without consent and for the prescribed entity to collect, use and disclose such PHI, as permitted under PHIPA and O.Reg. 329/04. CCO’s privacy practices and procedures must be reviewed by the IPC every three years from the date of their initial approval.

The first three-year approval of CCO’s practices and procedures as a prescribed entity was received from the IPC effective November 1, 2005. CCO had its status renewed by the IPC 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 entity role.

CCO is also designated as a “prescribed person” under PHIPA with respect to CCO’s role in compiling and maintaining the Colorectal Cancer Screening Registry (“prescribed registry”) as part of Ontario’s colorectal cancer screening program entitled ColonCancerCheck (**CCC**). The CCC program is currently in transition and will be expanded, starting in 2011, into an Integrated Cancer Screening program which encompasses CCO’s Ontario Breast Screening and Cervical Screening programs. A separate CCO Prescribed Person Triennial Review Report will be submitted to the IPC, later in 2011, for the 2011 approval process in respect of CCO’s prescribed person 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.

- Privacy Specialists who report to the Director, Privacy & Access and support CCO's Privacy Program.

- A Chief Data Steward who assigns a Data Steward to each CCO data-holding who is responsible for authorizing both internal and external requests for access to CCO data in accordance with CCO's Data Use and Disclosure Policy.

- Program Area Privacy Leads who are responsible for ensuring that the CCO Privacy Program is implemented in their Program Areas.

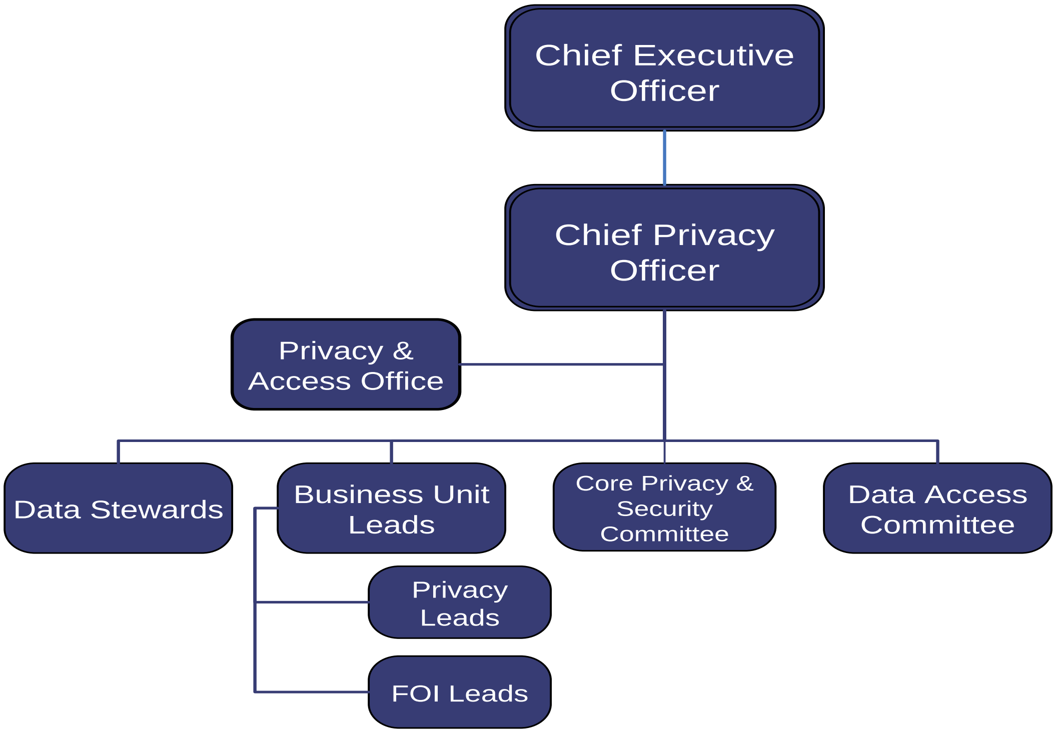
- A Facilities Department which is responsible for ensuring the physical integrity of CCO's premises.

- Systems Security Specialists who report to the Chief Technology Officer (**CTO**) and oversee IT security safeguards for CCO data.

- The Core Privacy & 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, supported by an Information Management Coordinator, which is responsible for reviewing and approving requests for access to CCO data by researchers.

PRIVACY ORGANIZATIONAL CHART



The key components of CCO’s Privacy Program include:

- CCO’s Privacy Policy and 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 which generates and monitors system audit logs; and
- privacy impact assessments on existing and proposed CCO data holdings and/or programs.

STATUS OF THE CCO 2008 PRESCRIBED ENTITY TRIENNIAL REVIEW RECOMMENDATIONS

The IPC's 2008 triennial review of CCO's practices and procedures resulted in 8 recommendations to be addressed prior to the next triennial review of CCO's practices and procedures. 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 Recommendations – Privacy

2008 IPC Compliance Recommendation	CCO Enhancement	Status		Expected Date of Completion
		Complete	In Progress	

1. Privacy Policy Section 5.6: Data Destruction:
a. Include the type of shredding for PHI records in paper format
b. Ensure the shredding employed is cross-cut or for highly sensitive documents pulverized or incinerated
c. Ensure electronic records or wireless media are destroyed either by physical damage or wiping before re-using
d. Note the importance of disposing of documents in a secure manner where it is not reasonably foreseeable to recreate records after they have been disposed of
e. Require third party service providers to securely destroy records of PHI
f. Require agents to notify CCO if an agent believes there
	All requirements have been met through:
	– *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition;
	– CCO's Breach Management Procedure;
	– CCO's Media Destruction Policy and Procedure;
	– CCO's Information Security Code of Conduct;
	– CCO's Information Security Policy;
	– CCO's Template Schedule for Third Party Agreements;
	– CCO's Security Operations Standard CCO's Information Security Disk Wipe Procedure;
	– CCO's Digital Media Disposal Guidelines; and
		✓		

may have been a breach of this policy or its procedures				
2. Amend the Privacy Audit and Compliance Standard and the Wait Times Information Office (**WTIO**) Privacy Compliance Procedure: a. To expand the privacy audit program to review all privacy policies and procedures implemented by CCO on an annual basis b. To document the procedures used in conducting the operational effectiveness and physical security reviews	All requirements have been met through: – Integration of WTIO and CCO privacy policies and procedures	✓		
3. Frequent review of system audit trails commensurate with the amount and sensitivity of the PHI collected, the number and nature of individuals who have access to PHI and the threats and risks associated with the PHI, in order to detect unauthorized access to data holdings containing PHI, and to detect information security incidents in a timely manner	All requirements have been met through: – PHI Access Monitoring and Audit Project; and – Logging, Monitoring and Auditing Standard	✓		
4. Amend Privacy Breach Management Procedure**:** a. Broaden the definition of privacy breach to include the collection, use, disclosure, retention or disposal of PHI, not simply use or disclosure b. Identify what information with respect to an information breach must be reported c. Require notification to HIC that provided the PHI d. Ensure consistency between procedures applicable to WTIO and remainder of CCO	All requirements have been met through: – Amendments to CCO's Privacy Breach Management Procedure	✓		

5. Amend the Privacy Training and Awareness Procedures to make explicit that agents must receive privacy training prior to being given access to PHI	All requirements have been met through: – CCO’s Privacy and Security Training and Awareness Procedure	✓		
6. Clarify in the Privacy Training and Awareness Procedures that contractors and consultants also receive annual privacy training	All requirements will be met through: – Amendments made to CCO’s Privacy and Security Training and Awareness Procedure	✓		
7. Amend the Privacy Training and Awareness Procedures to state that consultants and contractors are required to sign a Privacy Acknowledgement or WTIO Privacy Acknowledgement	All requirements have been met through: – Amendments to CCO’s Privacy and Security Training and Awareness Procedure; and – The integration of WTIO and CCO privacy policies and procedures	✓		
8. Amend the Privacy Training and Awareness Procedures to state the consequences imposed on consultants and contractors for failing to attend privacy training and failing to execute a Privacy Acknowledgement or WTIO Privacy Acknowledgement	All requirements have been met through: – Amendments to CCO’s Privacy and Security Training and Awareness Procedure; and – Through the integration of WTIO and CCO privacy policies and procedures	✓		
9. Amend the Privacy Acknowledgement or WTIO Privacy Acknowledgement to state that immediate notification of a breach or suspected breach to a Privacy Office or a WTIO Privacy Lead is required	All requirements have been met through: – Amendments to CCO’s Privacy and Security Training and Awareness Procedure; and – Through the integration of WTIO and CCO privacy policies and procedures	✓		
10. Amend the De-Identification Guidelines:	All requirements have been met through:	✓		

a. Include criteria for making the determination (i.e. who do agents consult with in making the determination?) as to whether or not to treat the report or data sets as PHI, in circumstances where the risk of identification is moderate b. Require agents to ensure that PHI is not disclosed if other information, such as de-identified information or aggregate information, will serve the purpose	– Amendments to CCO's De-Identification Guidelines			

2008 IPC Recommendations – Security

2008 IPC Compliance Recommendation	CCO Enhancement	Status		Expected Date of Completion
		Complete	In Progress	
1. Policy and procedure for review of security policies and procedures and for secure transfer of PHI	Requirements have been partially met through: – CCO 's Information Security Policy; – CCO's Information Classification and Handling Standard (Draft); and – CCO's Information Classification and Handling Guideline (Draft)		✓	

2. Amend the Information Security Incident Response Policy:
a. Have one person to report to in cases of an information security incident
b. Format and information reported on to report the
	Requirements have been met through:
	– Information Security Policy;
	– Security Operations Standard;
	– CCO's Incident Management
		✓		

security incident c. Consider whether the information security incident involves the unauthorized collection, use, disclosure, retention or disposal of PHI in violation of the Act and its regulation d. Include notification to the HICs where there are security incidents involving PHI e. Responsible person for assigning individuals to implement the recommendations, timelines and ensuring that the recommendations are being implemented	Framework			
3. Implement a comprehensive security training policy that**:** a. Encompasses both initial security training for all new employees, consultants b. Encompasses ongoing security training c. Emphasizes attendance for security training is mandatory d. States when the initial security training will be provided, namely prior to being given access to PHI e. States the frequency of ongoing training f. Identifies the individuals that will be doing the initial and ongoing training g. Describes the process that will be used to track attendance at both the initial and ongoing training sessions h. Sets out the responsible person for tracking	All requirements have been met through: – Amendments to CCO’s Privacy and Security Training and Awareness Procedure	✓		

attendance and the consequences for failing to attend				
4. Amend the Security Acknowledgement Form: a. Require persons signing to comply with all the security policies and procedures implement by CCO and not simply those enumerated in the form b. Require that the CTO or Systems Security Specialist be notified in the event of a breach or suspected breach of the Security Acknowledgement Form	All requirements have been met through: – Privacy and Security Acknowledgement form (updated November 2009)	✓		
5. Recommendation on the on-going security training: a. Role-based in order to ensure that agents understand how to apply the security policies, procedures, and practices implemented in their day-to-day work b. Addresses any new security policies, procedures and practices implemented by CCO and significant amendments to existing security policies, procedures and practices c. Includes content that considers any training related recommendations from security reviews, vulnerability assessments and threat and risk assessments	All requirements have been met.	✓		

2008 IPC Recommendations – Human Resources Requirements

2008 IPC Compliance Recommendation	CCO Enhancement	Status		Expected Date of Completion
		Complete	In Progress	
1. Amend the Confidentiality Policy or Privacy Training and Awareness Procedure: a. Make explicit that the Statement of Confidentiality must be executed upon the commencement of the relationship with CCO and prior to being given access to PHI b. Set out the process that will be used to track execution of the Statement of Confidentiality including the person(s) responsible for tracking execution and the consequences for failing to execute the Statement of Confidentiality	Requirements have been met through: – Amendments to CCO's Confidentiality Policy	✓		
2. Amend the Statement of Confidentiality to: a. Require agents to immediately notify the Privacy Unit in the Event of a breach or suspected breach of the Statement of Confidentiality b. Require employees who cease their work with CCO to set out the secure manner in which the PHI must be returned, or to state that the PHI must be destroyed c. Require the agent to provide written and signed confirmation that the PHI is permanently destroyed in a secure manner	a. Requirements have been met through: – Amendments to CCO's Statement of Confidentiality	✓		

CCO 2011 PRESCRIBED ENTITY TRIENNIAL REVIEW 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 Entities, such as CCO, to protect the privacy of individuals and to maintain the confidentiality of the PHI received by the Prescribed Entity.

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 CCO'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 a full briefing on the scope of the review, 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* – The final CCO 2011 Prescribed Entity Triennial Review Report was drafted and finalized, after all of the requirements were reviewed and responded to.

The structure of the CCO 2011 Prescribed Entity 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 to 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 if certain indicators are not reported on and, where appropriate, the measures to be implemented to permit future reporting of such indicators.

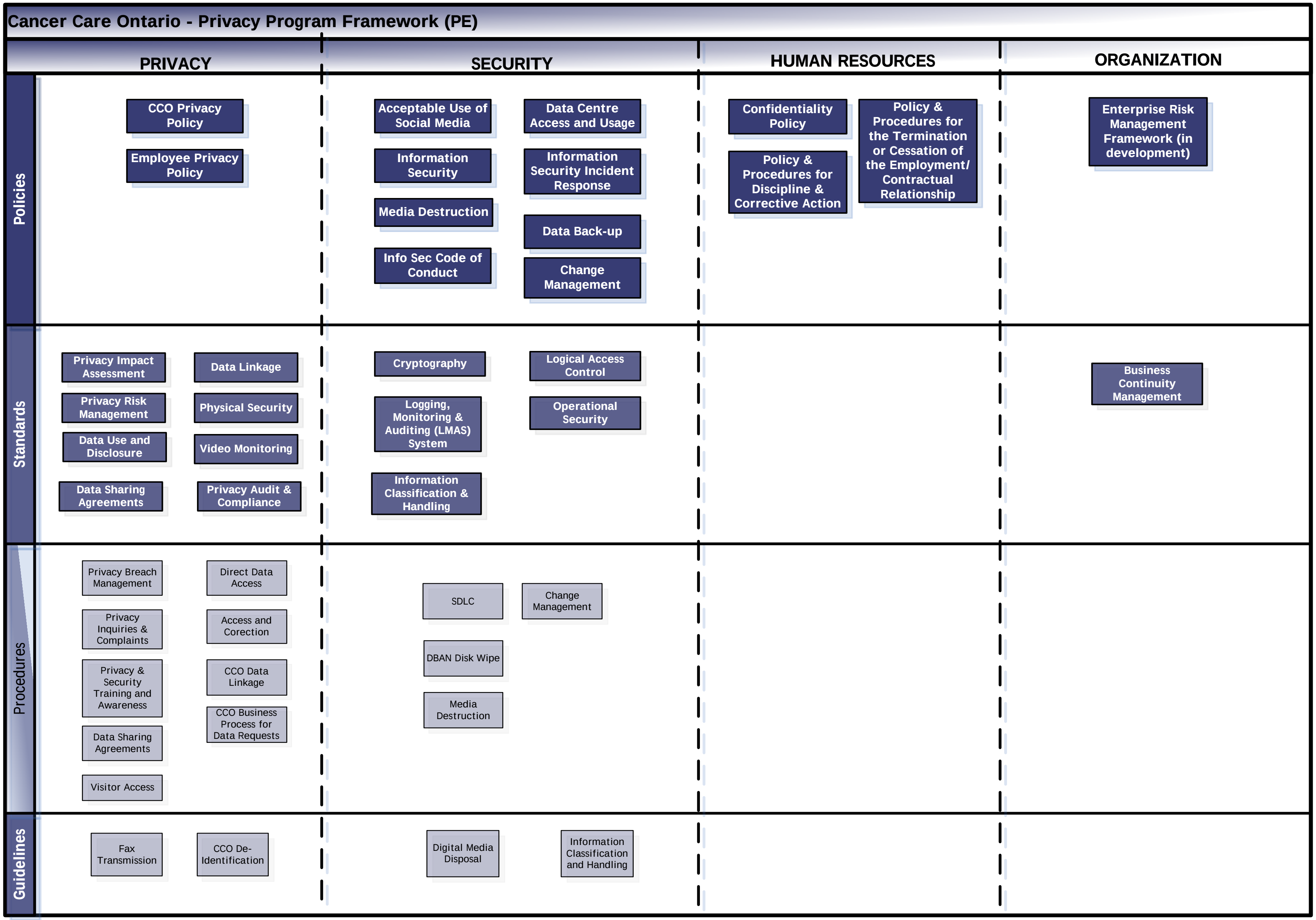
Lastly, a list and summary of all CCO documents and tools that were reviewed as part of this exercise has been included in the appendices of this report.

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 is to streamline a particular process.

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



Cancer Care Ontario - Privacy Program Framework (PE)

	PRIVACY	SECURITY	HUMAN RESOURCES	ORGANIZATION
Policies	CCO Privacy Policy Employee Privacy Policy	Acceptable Use of Social Media Data Centre Access and Usage Information Security Information Security Incident Response Media Destruction Data Back-up Info Sec Code of Conduct Change Management	Confidentiality Policy Policy & Procedures for the Termination or Cessation of the Employment/ Contractual Relationship Policy & Procedures for Discipline & Corrective Action	Enterprise Risk Management Framework (in development)
Standards	Privacy Impact Assessment Data Linkage Privacy Risk Management Physical Security Data Use and Disclosure Video Monitoring Data Sharing Agreements Privacy Audit & Compliance	Cryptography Logical Access Control Logging, Monitoring & Auditing (LMAS) System Operational Security Information Classification & Handling		Business Continuity Management
Procedures	Privacy Breach Management Direct Data Access Privacy Inquiries & Complaints Access and Corection Privacy & Security Training and Awareness CCO Data Linkage CCO Business Process for Data Requests Data Sharing Agreements Visitor Access	SDLC Change Management DBAN Disk Wipe Media Destruction		
Guidelines	Fax Transmission CCO De-Identification	Digital Media Disposal Information Classification and Handling		

Figure 1. Privacy Program Framework (PE)

PART 1: PRIVACY DOCUMENTATION

Privacy Documentation Matrix

CCO 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
Application for Disclosure for Information from CCO for Research Purposes													x	x																			
Business Process for Data Requests												x	x											x									
Data Access Committee Terms of Reference													x																				
Data Linkage Standard																						x											
Data Linkage Procedure																						x											
Data Sharing Agreement Initiation Form				x								x					x																
Data Sharing Agreement Procedure				x								x				x	x	x											x				
Data Sharing Agreement Standard				x												x	x																
Data Sharing Agreement Template												x					x																
Data Steward Terms of Reference	x			x				x																									
Data Use & Disclosure Standard	x							x				x	x						x					x									
Decision Criteria for Data Requests	x											x	x											x									
De-Identification Guidelines	x											x												x									

CCO 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
Digital Media Disposal Guidelines	x																																
Direct Data Access Audit Procedure								x																									
Direct Data Access Procedure								x																									
Employee Exit Process								x																									
IM/IT Stage – Gating Policy				x																													
Information Management Coordinator Terms of Reference													x																				
List of Data Linkages																							x										
Media Destruction Policy and Procedure								x				x																					
Non-disclosure/Confidentiality Agreement													x	x																			
Preliminary Privacy Assessment Form				x																													
Privacy & Security Acknowledgement Form																								x									
Privacy Audit and Compliance Standard		x		x		x						x	x			x			x			x		x	x		x		x		x		x
Privacy Breach Management Procedure				x		x							x						x			x		x	x				x	x	x		x
Contract Management System Log																					x												
Privacy FAQs			x																														

CCO 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
Privacy Impact Assessment Standard			x																						x								
Privacy Inquiries and Complaints Procedures	x		x																												x	x	x
Procurement Documentation and Records Management Procedure																			x														
Procurement of Goods and Services Policy																			x														
Statement of Information Practices	x		x																														
Template Schedule for Third Party Agreements																				x													
Logging, Monitoring, and Auditing System Standard		x																									x						
Microsoft Access Log															x																		
Online Direct Data Access Request (ODDAR) form and tool									x																								
Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario, 4th edition	x	x	x	x	x	x	x	x								x	x	x	x					x	x		x		x	x	x	x	x
Privacy & Access Office Remediation Program																					x				x	x	x	x		x		x	
Privacy & Access Office Operational Manual		x																									x						

IPC Requirements

<u>Privacy: IPC Requirement 1</u>: Privacy Policy in respect of CCO's status as a Prescribed Entity.

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of PHI within its custody. A main component of CCO's Privacy Program is its Privacy Policy, which is supported by related policies and procedures that provide additional information on the Privacy Principle in the CCO 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. *Data Use & Disclosure Standard,* Privacy & Access Office and Chief Information Officer (**CIO**)
3. *Decision Criteria for Data Requests,* CIO
4. *Statement of Information Practices*, Privacy & Access Office
5. *Privacy Inquiries and Complaints Procedure*, Privacy & Access Office
6. *De-identification Guidelines*, Privacy & Access Office and CIO
7. *Data Stewards Terms of Reference*, Privacy & Access Office and CIO
8. *Digital Media Disposal Guideline,* 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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

CCO reviews its policies and associated procedures annually to ensure their operational effectiveness and that they reflect both current legislatives requirements 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. *Privacy Audit and Compliance Standard,* Privacy & Access Office
3. *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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

CCO provides information on its Privacy Program and its privacy policies, procedures and practices, to the organization, the public and other stakeholders, through a variety of means, including, through the CCO internal and public websites, CCO's Privacy Brochure, and newsletters, updates and other privacy awareness initiatives.

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. *Privacy Impact Assessment Standard*, Privacy & Access Office
3. *Privacy Inquiries and Complaints Procedure*, Privacy & Access Office
4. *Statement of Information Practices*, Privacy & Access Office

5. *Privacy FAQs*, 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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

CCO policies and procedures articulate its commitment to limit the collection of PHI to only that which is permitted by PHIPA and only to 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. *Data Steward Terms of Reference,* Privacy & Access Office
3. *Privacy Audit and Compliance Standard*, Privacy & Access Office
4. *Privacy Breach Management Procedure* Privacy & Access Office
5. *Data Sharing Agreement Standard,* Privacy & Access Office
6. *Data Sharing Agreement Procedure*, Privacy & Access Office
7. *IM/IT Stage – Gating Policy,* CIO
8. *Preliminary Privacy Assessment Form*, Privacy & Access Office
9. *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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

CCO 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 publicly available for review at http://cancercare.on.ca/common/pages/UserFile.aspx?fileId=13632.

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

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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

CCO has in place policies and procedures which require statements of purpose for data holdings containing PHI to 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. *Privacy Breach Management Procedure*, Privacy & Access Office
3. *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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

CCO 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 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

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
		Complete	In Progress	Scheduled	
All requirements have been met.					

<u>Privacy: IPC Requirement 8</u>: Policy and Procedures for limiting agent access to and use of PHI.

CCO ensures that access to PHI by its employees 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. *Data Use and Disclosure Standard,* Privacy & Access Office and CIO
3. *Direct Data Access Procedure*, Privacy & Access Office and CIO
4. *Direct Data Access Audit Procedure*, Privacy & Access Office and CIO
5. *Data Steward Terms of Reference*, Privacy & Access Office and CIO
6. *Media Destruction Policy and Procedure*, EISO
7. *Employee Exit Process*, 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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

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 documents outline 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
		Complete	In Progress	Scheduled	
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 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.*

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Complete	In Progress	Scheduled	
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*.

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Complete	In Progress	Scheduled	
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 for purposes other than research, is in accordance with PHIPA, its regulation and CCO'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. *Data Use & Disclosure Standard,* Privacy & Access Office and CIO
2. *Business Process for Data Requests,* CIO
3. *De-Identification Guidelines*, Privacy & Access Office and CIO
4. *Data Sharing Agreement Template,* Privacy & Access Office
5. *Data Sharing Agreement Procedure,* Privacy & Access Office
6. *Data Sharing Agreement Initiation Form,* Privacy & Access Office
7. *Decision Criteria for Data Requests,* CIO

8. *Media Destruction Policy and Procedure*, EISO
9. *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
		Complete	In Progress	Scheduled	
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 a Research Ethics Board 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.

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

1. *Data Use & Disclosure Standard,* Privacy & Access Office and CIO
2. *Business Process for Data Requests,* CIO
3. *Application for Disclosure of Information from CCO for Research Purposes,* CIO
4. *Non-Disclosure/Confidentiality Agreement,* CIO
5. *Decision Criteria for Data Requests,* CIO
6. *Information Management Coordinator Terms of Reference,* CIO
7. *Data Access Committee Terms of Reference,* CIO
8. *Privacy Breach Management Procedure*, Privacy & Access Office
9. *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
		Complete	In Progress	Scheduled	
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 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. *Application for Disclosure of Information from CCO for Research Purposes,* CIO
2. *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:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Complete	In Progress	Scheduled	
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 documents outline 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:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Complete	In Progress	Scheduled	
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 between CCO and another 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. *Data Sharing Agreement Standard*, Privacy & Access Office
3. *Data Sharing Agreement Procedure*, Privacy & Access Office
4. *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
		Complete	In Progress	Scheduled	
All requirements have been met.					

Privacy: IPC Requirement 17: Template data sharing agreements.

The CCO 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 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. *Data Sharing Agreement Template*, Privacy & Access Office
3. *Data Sharing Agreement Standard*, Privacy & Access Office
4. *Data Sharing Agreement Procedure*, Privacy & Access Office
5. *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
		Complete	In Progress	Scheduled	
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.

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. *Data Sharing Agreement Procedure*, Privacy & Access Office

3. *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 Requirement	CCO Enhancement	Status			Comments
		Complete	In Progress	Scheduled	
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. *Data Use and Disclosure Standard*, Privacy & Access Office and CIO

3. *Privacy Audit and Compliance Standard*, Privacy & Access Office

4. *Procurement Documentation and Records Management Procedure*, Procurement Office

5. *Procurement of Goods and Services Policy*, Procurement Office

6. *Privacy Breach Management Procedure*, Privacy & Access Office

7. *Privacy & Access Office Operational Manual,* Privacy & Access Office

8. *Template Schedule for Third Party Agreements,* Legal Department

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
		Complete	In Progress	Scheduled	
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. *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
		Complete	In Progress	Scheduled	
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. *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
		Complete	In Progress	Scheduled	
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's 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. *Data Linkage Standard,* CIO
2. *Privacy Breach Management Procedure*, Privacy & Access Office
3. *Privacy Audit and Compliance Standard*, Privacy & Access Office
4. *Data Linkage Procedure,* 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
		Complete	In Progress	Scheduled	
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:

IPC Compliance Requirement	CCO Enhancement	Status			Comments
		Complete	In Progress	Scheduled	
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 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. *Data Use & Disclosure Standard,* Privacy & Access Office and CIO
3. *De-Identification Guidelines,* Privacy & Access Office and CIO
4. *Business Process for Data Requests,* CIO
5. *Privacy & Security Acknowledgment form,* Privacy & Access Office
6. *Decision Criteria for Data Requests,* CIO
7. *Privacy Audit and Compliance Standard*, Privacy & Access Office
8. *Privacy Breach Management 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
		Complete	In Progress	Scheduled	
All requirements have been met.					

<u>Privacy: IPC Requirement 25</u>: 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. *Privacy Impact Assessment Standard*, Privacy & Access Office

3. *Privacy & Access Office Remediation Program – Log of Privacy Impact Assessments*, Privacy & Access Office

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

5. *Breach Management 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
		Complete	In Progress	Scheduled	
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 CCO's compliance with this requirement:

1. *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
		Complete	In Progress	Scheduled	
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 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. *Privacy Audit and Compliance Standard*, Privacy & Access Office

3. *Privacy & Access Office Remediation Program*, Privacy & Access Office

4. *Privacy & Access Office Operational Manual*, Privacy & Access Office

5. *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
		Complete	In Progress	Scheduled	
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. *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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

CCO policies stipulate that it is mandatory to report all privacy breaches or suspected privacy breaches. CCO's 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. *Privacy Breach Management Procedure*, Privacy & Access Office
3. *Privacy Audit and Compliance Standard*, Privacy & Access Office
4. *Data Sharing Agreements 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
		Complete	In Progress	Scheduled	
All requirements have been met.					

Privacy: IPC Requirement 30: Log of privacy breaches.

CCO 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. *Privacy Breach Management Procedure*, Privacy & Access Office
3. *Privacy & Access Office Remediation Program – Log of Privacy Breaches*, 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
		Complete	In Progress	Scheduled	
All requirements have been met.					

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

CCO 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. *Privacy Inquiries and Complaints Procedure*, Privacy & Access Office
3. *Privacy Breach Management Procedure*, Privacy & Access Office
4. *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
		Complete	In Progress	Scheduled	
All requirements have been met.					

<u>Privacy: IPC Requirement 32</u>: Log of privacy complaints.

CCO 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. *Privacy Inquiries and Complaints Procedure*, Privacy & Access Office
3. *Privacy & Access Office Remediation Program – Log of Privacy Inquiries and Complaints*, 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
		Complete	In Progress	Scheduled	
All requirements have been met.					

<u>Privacy: IPC Requirement 33</u>: Policy and procedures for privacy inquiries.

CCO reviews and responds to all inquiries from the public, on its information practices 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. *Privacy Inquiries and Complaints Procedure*, Privacy & Access Office
3. *Privacy Breach Management Procedure*, Privacy & Access Office
4. *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
		Complete	In Progress	Scheduled	
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															
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													
Data Use and Disclosure Standard					x													
Information Security Policy	x	x	x		x	x	x	x	x	x	x	x	x	x	x		x	
Information Security Program Plan 2010-2011	x																	
Logging, Monitoring, and Auditing Standard	x	x					x		x	x				x	x			
Logical Access Control Standard	x		x			x	x		x									
Operational Security Standard								x			x				x	x		
Information Security Framework	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
Security Risk Management Standard															x	x		
Incident Management Framework	x	x								x							x	
Acquisition, Development and Application Security Standard	x																	
Visitor Access Procedure			x															
Video Monitoring Standard			x															
Change Management Policy												x						
Change Management Process												x						
Data Backup Policy	x				x								x					
Data Backup Process and Standard					x								x					
Direct Data Access Procedure			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															
Information Management Coordinator Terms of Reference					x													
Authorization to Access Data Centre Employee Form			x															
Authorization to Access Data Centre Contractor Form			x															
Personnel Action Form			x															
Data Center Access and Usage Policy			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
Privacy Audit and Compliance Standard			**x**		**x**													
Privacy Breach Management Procedure					**x**													
Template Schedule for Third Party Agreements					**x**			**x**					**x**					
Application for Disclosure of Information From form CCO for Research Purposes					**x**													
Non-Disclosure Confidentiality Agreement					**x**													
Open Media Logs					**x**								**x**					
HP Data Protectors Session Logs					**x**								**x**					
Digital Media Disposal Guidelines								**x**										
Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario, 4th edition															**x**			
Threat Risk Assessment Template															**x**			
Log of Security Audits															**x**			
Senior Team Lead Job Description															**x**			
Security Incident Tracking Spreadsheet																		**x**
Provision of Paging and Mobile Phone with Email						**x**												
Information Classification and Handling Guideline (Draft)					**x**	**x**	**x**							**x**				
Information Classification and Handling Standard (Draft)					**x**	**x**	**x**							**x**				
Privacy & Access Office Remediation Program					**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
Cryptography Standard						**x**												
Provision of Paging & Mobile Phone with Email						**x**												
Operational Security Procedure: Patching											**x**							
Privacy & Access Office Operational Manual													**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 Methodology ,* Project Management Office
8. *Data Backup Policy,* IT 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. *Incident Management Framework,* 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 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,* CCO Facilities
6. *Photo ID Request Form,* Human Resources
7. *Authorization to Access Data Centre Employee Form*, IT Services
8. *Authorization to Access Data Centre Contractor Form*, IT Services
9. *Data Center Access and Usage Policy,* IT Services
10. *Employee Exit Checklist,* Human Resources
11. *Employee Exit Process* , Human Resources
12. *Personal Action Form (PAF)* , Human Resources
13. *Visitor Access Procedure*, CCO Facilities
14. *Video Monitoring Standard,* CCO Facilities
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*, CCO Facilities and IT Services.
2. *EasyLobby Visitor Grid Log,* CCO Facilities
3. *KeyScan System Log,* CCO Facilities

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 Classification and Handling Standard*(Draft), EISO
4. *Information Classification and Handling Guideline* (Draft), EISO
5. *Information Management Coordinator Terms of Reference,* CIO
6. *Non-Disclosure/Confidentiality Agreement,* CIO

7. *Application for Disclosure of Information from CCO for Research Purposes,* CIO
8. *Data Sharing Agreement Template,* Privacy & Access Office
9. *Data Sharing Agreement Procedure,* Privacy & Access Office
10. *Data Sharing Agreement Standard,* Privacy & Access Office
11. *Data Use and Disclosure Standard,* Privacy & Access Office and CIO
12. *Privacy Audit and Compliance Standard,* Privacy & Access Office
13. *Privacy Breach Management Procedure,* Privacy & Access Office
14. *Data Back-up Policy*, IT Services
15. *Data Back-up Process and Standard*, IT Services
16. *Open Media Logs*, IT Services
17. *HP Data Protectors Session Logs*, IT Services
18. *Template Schedule for Third Party Agreements,* Legal Department
19. *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.					

***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 March 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,* EISO
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

<u>Security: IPC Requirement 7</u>: 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. – Whether the agent transferring records of PHI is	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

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 March 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. *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.					

<u>Security: IPC Requirement 9</u>:   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.					

<u>Security: IPC Requirement 10</u>:   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 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 March 2011.

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

1. *Information Security Policy*, EISO
2. *Operational Security Standard,* EISO
3. *Information Security Code of Conduct,* 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. *Data Backup Process and Standard,* Technology Services

4. *Template Schedule for Third Party Agreements,* Legal Department
5. *HP Data Protector Session Logs,* Technology Services
6. *Open Media Logs*, Technology Services and Third Party Service Provider
7. *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.					

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 March 2011.

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

1. *Information Security Policy*, EISO
2. *Security Risk Management Standard*, EISO
3. *Information Security Framework,* EISO
4. *Operational Security Standard*, EISO
5. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
6. *Logging, Monitoring, and Auditing Standard,* EISO
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 March 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 March 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 March 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
Code of Conduct											x
Confidentiality Policy					x						
Contract Management System							x				
Employee Exit Process										x	
Employee Exit Checklist										x	
Information Security Code of Conduct			x	x							
Information Security Policy			x	x							
Intranet-Human Resources Workflow: How Do I Hire a new Employee?					x						
Personnel Action Form					x					x	
Privacy & Access Office Remediation Program	x	x	x	x							
Privacy & Access Office Operational Manual	x										
Privacy and Security Training and Awareness Procedure	x	x	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
Privacy Audit and Compliance Standard	x		x								
Privacy Breach Management Procedure	x										x
Privacy Training Curriculum	x										
Procurement of Goods and Services Policy					x						
Progressive Discipline Policy											x
Security Training Curriculum			x								
Statement of Confidentiality						x					
Template Schedule for Third Party Agreements						x					
Termination of Employment Policy										x	
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		

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
Principles and Policies for the Protection of Personal Information at Cancer Care Ontario, 4th edition	**x**	**x**									
Secondment Policy					**x**						
Unpaid Student Intern Policy					**x**						
Privacy & Security eLearning Module						**x**	**x**				
Termination Monthly Reports										**x**	

IPC Requirements

Human Resources: IPC 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. 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 within 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. *Privacy and Security Training and Awareness Procedure*, Privacy & Access Office
3. *Privacy Training Curriculum*, Privacy & Access Office
4. *Privacy Audit and Compliance Standard*, Privacy & Access Office
5. *Privacy Breach Management Procedure*, Privacy & Access Office
6. *Privacy & Access Office Remediation Program – Log of Privacy and Security Training Completion*, Privacy & Access Office
7. *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.					

Human Resources: IPC 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 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. *Privacy and Security Training and Awareness Procedure*, Privacy & Access Office
3. *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. *Information Security Policy*, EISO
3. *Information Security Code of Conduct,* EISO
4. *Privacy and Security Training and Awareness Procedure,* Privacy & Access Office
5. *Security Training Curriculum*, EISO
6. *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. *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 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. *Confidentiality Policy*, Privacy & Access Office and Human Resources
2. *Personnel Action Form*, Human Resources
3. CCO's Intranet - Human Resources Workflow: *How do I hire a new employee*?[1], Human Resources
4. *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. *Statement of Confidentiality*, Human Resources
2. *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. *Contract Management System*, Procurement Office
2. *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 systems 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. *Employee Exit Process*, Human Resources
2. *Employee Exit Checklist*, Human Resources
3. *Personnel Action Form*, Human Resources

4. *Termination of Employment Policy,* Human Resources
5. *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.					

<u>Human Resources: IPC Requirement 11</u>*:* 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. *Code of Conduct*, Human Resources
2. *Progressive Discipline Policy*, Human Resources
3. *Privacy Breach Management 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.					

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
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**						
Architecture Review Board Terms of Reference			**x**					
Core Privacy Committee Terms of Reference			**x**					
Information Security Policy		**x**	**x**					
Information Security Program Plan		**x**	**x**					
Privacy & Access Office Remediation Program						**x**	**x**	
Privacy & Access Office Operational Manual						**x**		
Privacy Audit and Compliance Standard						**x**		
Privacy Breach Management Procedure						**x**		
Statement of Information Practices	**x**							

CCO Organizational and Other Documentation Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8
Privacy & Access Office Remediation Program Logs					**x**			
Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario, 4th edition	**x**		**x**			**x**	**x**	
Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program		**x**						
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 and 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. *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.					

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

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.					

<u>Organizational and Other: IPC Requirement 3</u>: 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. *Information Security Policy*, EISO
2. *Information Security Program Plan 2010-2011*, EISO
3. *Architecture Review Board Terms of Reference,* IT Services
4. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario*, 4th edition, Privacy & Access Office
5. *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 inventory which was 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 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 and 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 inventory which was 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 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 and 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. *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. *Privacy & Access Office Operational Manual*, Privacy & Access Office
3. *Privacy & Access Office Remediation Program*, Privacy & Access Office
4. *Privacy Breach Management Procedure*, Privacy & Access Office
5. *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.					

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
   - *Log of Privacy Impact Assessments*
   - *Log of Privacy Breaches*
   - *Log of Privacy Inquiries and Complaints*
   - *Log of IPC Recommendations*

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"). It is expected that by March 2011, the Plan will be tested and operational. The revised Plan documents and implements the appropriate processes which manage every phase of a disaster from response through to restoration.

1. *Business Continuity and Disaster Recovery Plan*, Technology Services
2. *Business Continuity Service Framework*, Technology Services
3. *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 current as of August 31, 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 2 annual reviews of CCO's privacy policies and/or procedures since the IPC's last review of CCO in October 2008.
		• 2009 and 2010
		• *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario, 3rd edition* :
		o Privacy Breach Management Procedure;
		o Privacy and Security Training and Awareness Procedure;
		o Audit and Compliance Procedure;
		o Inquiries and Complaints Procedure;
		o CCO's Privacy Impact Assessment Standard;
		o Direct Data Access Procedure; and
		o Data Use and Disclosure Standard.

2	Log of amendments, date of amendment and description of amendment, as a result of the prior review of the IPC.	Four privacy policies and/or procedures were amended as a result of the IPC's last review of CCO in October 2008. These amendments were made to the following policies/procedures: • 2009 and 2010 reviews - minor and substantive amendments to o *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario, 3rd edition* • 2009 and 2010 reviews - minor amendments to: o Privacy Breach Management Procedure; o Privacy and Security Training and Awareness Procedure; and o Inquiries and Complaints Procedure.
3	Record of new policies and procedures developed as a result of the prior review of the IPC.	No new privacy policies or procedures have been developed as a result of the IPC's 2008 review of CCO. **Note:** CCO's Logging, Monitoring and Auditing Standard has been developed in response to one of the IPC's findings from its 2008 review of CCO. This document has been referenced below in the in Security Indicator #3 - General Security Policies and Procedures.
4	Record of dates and nature of communication regarding amendments.	Four privacy policies and/or procedures which were amended and approved have been communicated through CCO's intranet and/or public-facing website, per CCO's dissemination procedure. The

		following policies/procedures have been published: • *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario,* 3rd edition; June 2009, intranet and public-facing website • Privacy Breach Management Procedure, November 2009, intranet website; • Privacy and Security Training and Awareness Procedure, November 2009, intranet website; and • Direct Data Access Procedure, November 2009, intranet website.
5	Record of changes to public communication materials, as a result of the prior review of the IPC.	The IPC's 2008 review of CCO did not recommend any changes to CCO's public communication materials.

Collection

	IPC Key Indicator Required	CCO's Response
1	The number of data holdings containing personal health information.	CCO has 44 data holdings which are operating under the PHIPA authority of a prescribed entity.
2	The number of statements of purpose developed for data holdings containing personal health information.	22 statements of purpose have been developed for CCO's data holdings, specifically the programs operating under the PHIPA authority of a prescribed entity. **Note**: CCO's technical infrastructure is set up such that there may be multiple data holdings for one program.
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.	22 statements of purpose for CCO's data holdings operating under the PHIPA authority of a prescribed entity 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 entity.
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	No amendments to CCO's statements of purpose were required as a result of the IPC's last review of CCO in October 2008.

	IPC.	

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.	As of October 31, 2008 to August 31, 2011, CCO's Online Direct Data Access Request (ODDAR) system has recorded 962 requests made for access to use PHI for purposes other than research. **Note:** Per the Direct Data Access Procedure, internal users must request and receive approval for direct access to each individual CCO 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 CCO 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 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 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.	CCO received 351 requests for PHI for purposes other than research, since the IPC’s last review of CCO in October 2008. Of the 351 requests 306 requests were for genetics counseling purposes and 45 requests were for the return of PHI to HICs (who had originally provided the data).
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.	All 351 requests received for PHI for purposes other than research, since the IPC’s last review of CCO in October 2008, were approved. There were 0 requests denied.
3	The number of requests received for the disclosure of personal health information for research purposes, since the prior review of the IPC.	There were 109 research requests received by CCO for PHI since the IPC’s last review of CCO in October 2008.
4	The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied, since the prior review of the IPC.	There were 91 research requests approved for the disclosure of PHI, since the IPC’s last review of CCO in October 2008. The remaining numbers of requests are either under review or at the approval stage. There were 0 requests denied.
5	The number of Research Agreements executed with researchers to whom personal health information was disclosed, since the prior review of the IPC.	There were 82 Research Agreements executed with researchers since the IPC’s last review of CCO in October 2008. The remaining Research Agreements are in development or in the approval stage. Research data is not disclosed until the final agreement is 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.	There were 949 requests received for de-identified and/or aggregate information for both research and other purposes since the IPC’s last review of CCO in October 2008.
7	The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and	There were 225 acknowledgements or agreements executed with persons whom CCO disclosed de-identified and/or aggregate information for research and other purposes, since the IPC’s last review of CCO in October 2008.

	other purposes, since the prior review of the IPC.	132 agreements were signed for SEER*Stat data, 3 research agreements were signed and 90 General Data Request Forms were signed.

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.	Since the IPC's last review of CCO in October 2008, there have been 5 Data Sharing Agreements executed or amended for the collection of PHI by CCO, under the PHIPA authority of a prescribed entity: • 3 Data Sharing Agreements were executed for the collection of PHI by CCO • 2 were amending agreements
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.	Since the IPC's last review of CCO in October 2008, there have been 14 Data Sharing Agreements executed or amended for the disclosure of PHI by CCO, under the PHIPA authority of a prescribed entity: • 10 Data Sharing Agreements were executed for the disclosure of PHI by CCO • 4 were amending agreements

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.	CCO has conducted a manual review of the number of agreements executed with third party service providers with access to PHI. Since the last review of the IPC up until August 31, 2011 thirty four agreements, were executed with third party service providers. **Note:** CCO has controls in place to ensure third parties who are provided with access to PHI on CCO's systems receive privacy

		and security training and sign agreements that include confidentiality terms, within their third party agreements. CCO also ensures that access privileges to CCO's data holdings are renewed on an annual basis through the Online Direct Data Access Request (ODDAR) system. Enhancements are currently being made (as noted in the Privacy: Requirement #21) to the processes for tracking agreements executed with third party service providers that have access to PHI, including enhancing the tracking and logging capabilities of the current Contract Management System (CMS).

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.	There have been 31data linkages approved since the IPC's last review of CCO in October 2008. Of the 31 approved data linkages that occurred at CCO, 2 were Production Linkages, and 29 were Analytic Linkages. Categories of linkages can be found in CCO's Data Linkage Standard. Please refer to Appendix 2 to Indicators – List of Data Linkages, for a list of the approved data linkages.

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: • The data holding, information system, technology or program, • The date of completion of the privacy impact	CCO has completed eight PIAs since the IPC's last review of CCO in October 2008 for programs operating under the PHIPA authority of a prescribed entity. These are as follows: 1. CPOE – Addendum to 2007 PIA, April 2009 2. WTIS-ALC – Addendum to 2008 PIA, November 2009 3. ERNI – PIA, November 2009 4. ISAAC – Addendum to 2007 PIA, November 2009 5. EDW – Addendum to 2008 PIA, November 2009 6. ISAAC, Addendum to 2007 PIA, August 2010

	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.	7. EB-PET – PIA, December 2010 8. SCT – PIA, May 2011 Please refer to Appendix 3 to 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.	CCO has undertaken but not completed four PIAs since the IPC's last review of CCO in October 2008 for programs operating under the PHIPA authority of a prescribed entity. These are as follows: 1. Brachytherapy PIA 2. Dyspnea PIA 3. ePath PIA 4. Cancer Stage PIA
3	The number and list of privacy impact assessments that were not undertaken but will be completed and the proposed date of completion.	Five PIAs are scheduled to be completed for programs operating under the PHIPA authority of a prescribed entity: 1. EDW Integration, 2011 2. EDW-ALC, 2011 3. New Drug Funding Program, 2011 4. WTIS, 2011 5. CPOE, 2011
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, 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. Since the IPC's last review of CCO in October 2008, there have not been any completed PPAFs from which the determination has been made that a PIA or Addendum to a PIA is not required.
5	The number, list and a brief description of privacy impact assessments reviewed, since the prior review of the IPC.	There have been four PIAs for programs operating under the PHIPA authority of a prescribed entity since the IPC's last review of CCO in October 2008: 1. ISAAC – Addendum to 2007 PIA, November 2009 2. EDW – Addendum to 2008 PIA, November 2009 3. ISAAC, Addendum to 2007 PIA, August 2010 4. OBSP, Review of Program, December 2010

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.	Per CCO’s Direct Data Access Audit Procedure, the following audits of users granted approval, through CCO’s ODDAR system, to access and use PHI, were conducted since the IPC’s last review of CCO in October 2008: 1. 2008 – 4 data holdings audited • September: CCN • September: OCRIS • October: ISAAC • March: EDW 2. 2009 – 3 data holdings audited • December: CCO Active Directory • December: iPort • December: CCN 3. 2010 – 1 data holding audited • February: WTIS 4. 2011 – 1 data holding audited • January – August: EDW **Note:** 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.
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, • 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.	Per CCO’s Audit and Compliance Procedure, the following types of privacy audits were completed since the IPC’s last review of CCO in October 2008: 1. **Annual policy reviews** -2009 – 1 review completed -2010 – 1 review completed 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.

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.	There have been 8privacy incidents and 7 privacy breaches reported at CCO since the IPC's last review of CCO in October 2008 for program operating under the PHIPA authority of a prescribed entity. 1. **November & December 2008:** none reported 2. **2009:** 2 were determined to be privacy incidents, 2 were determined to be privacy breaches 3. **2010:** 3 were determined to be privacy incidents, 2 were determined to be privacy breaches 4. **2011:** 3 were determined to be privacy incidents, 3 were determined to be privacy breaches. **Note:** CCO's Privacy & Access Office defines privacy incidents and privacy breaches as follows: - *Incident* – A suspected breach, where an investigation conducted by the Privacy & Access Office determines that there was no breach of PHI. - *Breach* – The misuse or improper / unauthorized collection, use, disclosure, retention or disposal of PHI in the custody of CCO
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 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	CCO's Remediation Program maintains a comprehensive log of all reported privacy breaches and incidents. The root cause of privacy breaches are noted as follows: 1. **2009:** 2 program procedure infractions and 4 policy infractions 2. **2010:** 2 policy infractions 3. **2011:** 3 policy infractions Please refer to Appendix 5 to Indicators- Summary from the Log of Privacy Breaches for a list of privacy breaches.

	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 prior review of the IPC.	No privacy complaints received
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,	No privacy complaints received

	• 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.	
3	Of the privacy complaints received, the number of 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.	No privacy complaints received

Part 2 - SECURITY INDICATORS

As per the IPC's request, all Indicators are current as of August 31, 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 two 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 – August 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 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.	All of the new security policies, standards and/or procedures which were developed and approved have been communicated through CCO's intranet. The following policies/procedures were published in July 2010: • Information Security Code of Conduct; • Acceptable Use of Social Media Policy: • Information Security Policy; • Logical Access Control Standard; • Cryptography Standard; • Logging, Monitoring, and Auditing Standard
5	Whether communication	No externally available communication materials were amended

	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.	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.	Per CCO's Direct Data Access Audit Procedure, the following system audits were conducted since October 2008: 1. 2008 – 4 data holdings audited • September: CCN • September: OCRIS • October: ISAAC • March: EDW 2. 2009 – 3 data holdings audited • December: CCO Active Directory • December: iPort • December: CCN 3. 2010 – 1 data holding audited • February: WTIS 4. 2011 – 1 data holding audited • January – August: EDW **Note:** 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	53 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 6 to Indicators – Summary from the Log of Security Audits, for a list of security audits completed since the IPC's last review of CCO.

	addressed or is expected to be addressed.	

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.	As of August 31, 2011 there have been 14 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 • 9 were determined to be security incidents • 5 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 9 security incidents and 5 security breaches. **Note:** CCO's Enterprise Information Security Office 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 personal health information at issue,	CCO's Enterprise Information Security Office has determined that policy violations are the root cause of all 5 security breaches which have occurred at CCO since the IPC's last review of CCO in October 2008. **Note:** A comprehensive Incident Response process and management program is being implemented at CCO to capture all the information required by this indicator. Descriptions of the 14 suspected information security breaches (including the 5 breaches) are captured in Appendix 7 to Indicators – Log of Information Security Breaches.

	– 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 current as of August 31, 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 August 31, 2011, all CCO employees (includes PE and PR) have received initial privacy orientation since the IPC's last review of CCO in October 2008. • **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:** 124 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 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 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 privacy training each year, since the prior review of the IPC.	As of August 31, 2010, the number of CCO employees 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) **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) **2010:** • Developed and published two privacy newsletters (internal) • 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 August 31, 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:** 124 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 August 31, 2010, 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 November 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.	The number of Confidentiality Agreements executed since the IPC's last review of CCO in October 2008 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 Aug 31, 2011 – 163 Confidentiality Agreements executed **Note:** The numbers noted above include CCO employees and 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 August 31, 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 August 31, 2011 534 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.

Part 4 – ORGANIZATIONAL INDICATORS

As per the IPC's request, all Indicators are current as of August 31, 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 description of the amendments made.	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 is expected to be completed by March 2011. 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

Data Holding	Data	Source	Statement of Purpose
Dyspnea Management Program	This dataset contains: -Clinical data -Demographic data	-Hospitals	1. The purpose of the data holding is to securely store data (including PHI) collected from 6 hospital sites for the dyspnea management pilot project. 2. PHI is collected to evaluate the impact that dyspnea management has on lung cancer patients, whether a subset of patients benefit from counselling and to determine if counselling results in any secondary impacts on the health system.
Stem Cell Transplant (SCT)	This dataset contains: -Patient Demographic data -Clinical / Stem Cell Transplants data -File Descriptor data	-Hospitals	1. The purpose of the SCT data set is to support planning, funding and forecasting of stem cell transplants within Ontario. 2. PHI is collected to calculate specific indicators and measures that are required to support the Goals and Objectives framework for the SCT project.
Brachytherapy Funding Program	This dataset contains: -Clinical data -Demographic data	-Referring physicians	1. The purpose of this data holding is to provide reimbursement for eligible prostate cancer patients that meet the program guidelines. 2. PHI is collected to ensure there is no duplication of cases, to reimburse eligible patients and to confirm products used when issues/ questions arise.
Ontario Cancer Symptom Management Collaborative (OCSMC) Symptom	This dataset contains: -Demographic data -Clinical data	-Hospitals	1. The Symptom Management Reporting Database was developed in order to assess the goal of OCSMC, which is to improve symptom management and collaborative palliative care planning through earlier identification, documentation and communication of patients' symptoms and performance status.

Data Holding	Data	Source	Statement of Purpose
Management Reporting Database			2. PHI is collected to evaluate the provision of symptom management and palliative care planning for cancer patients in Ontario.
New Drug Funding Program (NDFP)	This dataset contains: - administrative data - clinical data (eligibility criteria) - demographic data	-Hospitals	1. The NDFP database stores patient and treatment information about systemic therapy drug utilization at Ontario hospitals, for which reimbursement is being sought through the NDFP according to strict eligibility criteria. 2. PHI is collected for CCO NDFP to reimburse hospitals for those patients who have met the eligibility criteria.
Ontario Breast Screening Program (OBSP)	This dataset contains: -Clinical data (test(s) and results, clinical history, performance data for OBSP radiologists, nurse examiners, screening sites, and assessment sites; program outcomes data) -Demographic data (appointment scheduling, physician contact data, correspondence data)	-Data entry by OBSP sites -Ontario Cancer Registry (OCR) data linkage -Death registry linkage	1. The purpose of this data holding is to screen and assess clients in order to operate the program. 2. PHI is collected to implement, plan, manage, evaluate, allocate resources to, and report on performance of, the OBSP.
Ontario Positron Emission Tomography Scan Evidence-Based	This dataset contains: -Clinical data -Patient demographic data -Physician	-Referring physicians -Diagnostic centres	1. The purpose of this data holding is to carry out CCO's mandate to operate the evidence-based PET Scans Ontario Program: • Information to PET Access Reviewers for adjudication of scans • Reimbursement to PET Centres and PET

Data Holding	Data	Source	Statement of Purpose
Program (EB-PET Program)	demographic data -Administrative data		Access Reviewers • Provision of information to PET Steering and/or MOHLTC 2. PHI is collected by CCO to: • Communicate approved PET scan requests to designated PET Centres. • Provide sufficient information for the adjudication process (some demographic and clinical data). • Link to other data holdings for reporting and analysis for the evaluation and management of the PET Scans Ontario Program.
Ontario Cervical Screening Program	This dataset contains: - Administrative data - Clinical data - Demographic data	-CytoBase -Registered Persons Database (RPDB) -OCR	1. The purpose of this data holding is to gather information on pap tests for Ontario women from 1997 onwards. 2. PHI is collected to implement, plan, manage, evaluate, allocate resources to, and report on performance of, the program.
Collaborative Staging	This dataset contains: - administrative data - clinical data - demographic data - facility data	-OCR -Pathology Datamart -Hospital patient health records	1. The Collaborative Staging dataset is a standardized set of data elements that describe how far a cancer has spread at the time of diagnosis. It contains patient, tumour and additional disease-site specific factors that together derive the stage of the patient at the time of diagnosis. 2. CCO submits provincial stage data annually to North American Association of Central Cancer Registries (NAACCR) and Statistics Canada. Along with data from the Ontario Cancer Registry, cancer stage data is necessary to support cancer system surveillance, planning and management. PHI is necessary to enable comprehensive analysis and for linking to the Ontario Cancer Registry,

Data Holding	Data	Source	Statement of Purpose
			screening, and treatment data.
Pathology Information Management System (PIMS)	This dataset contains: - administrative data - clinical data - demographic data - facility data	-Hospitals -Some commercial laboratories	1. The PIMS Database is comprised of patient and tumour information for cancer and cancer-related pathology reports (tissue, cytology), submitted from public hospital (and some commercial) laboratories. PIMS documents patient, facility, and report identifiers, and tumour identifiers, such as site, histology and behaviour. 2. PHI is used to support management decision-making, planning, disease surveillance and research, as well as contributing to resolved incidence case data in the Ontario Cancer Registry.
National Ambulatory Care Reporting System (NACRS)	The dataset contains: - administrative data - demographic data - clinical data	-Canadian Institute for Health Information (CIHI)	NACRS contains summary diagnostic and treatment information about patients who have received outpatient surgery or selected other treatments (chemotherapy, emergency department visits, dialysis and cardiology) in Ontario hospitals.
Discharge Abstract Database (DAD)	The dataset contains: - administrative data - demographic data - clinical data	-CIHI	DAD contains summary diagnostic and treatment information about patients who have received healthcare services as an inpatient (including acute care, chronic care and rehabilitation care) in Ontario hospitals.
Ontario Cancer Registry Information System (OCRIS)	This dataset contains: - administrative data - clinical data - demographic data	-CIHI (DAD, NACRS) -Activity Level Reporting (ALR) (Regional Cancer Centre and Princess Margaret Hospital reporting through Databook) -PIMS, anatomical pathology reports from Ontario public and private laboratories -Ontario Registrar General's Office,	1. OCR is a computerized database of information on all Ontario residents who have been newly diagnosed with cancer ("incidence") or who have died of cancer ("mortality"). All new cases of cancer are registered, except non-melanoma skin cancer. This information is used to support management decision-making, planning, disease surveillance and research. 2. PHI is collected to link records and establish which records belong to which patient. The PHI is

Data Holding	Data	Source	Statement of Purpose
		Mortality files enhanced by death certificate notifications from Statistic Canada for Ontario residents deaths in other provinces/territories -Out of Province, notifications from other provinces/territories of Ontario residents diagnosed or treated in the notifying P/T	frequently required by internal and external researchers. The Canadian Cancer Registry MOU contains the requirement that PHI be included in CCO annual submissions of newly diagnosed patients.
Mortality Data	The dataset contains: - administrative data - demographic data	-Ministry of Government Services -Office of the Registrar General	1. The purpose of this data holding is for CCO to receive mortality data which contains the date of death and cause of death for Ontario residents who have died in Ontario for planning and management purposes. 2. PHI is collected to identify cases for the Ontario Cancer Registry and for measuring cancer survival.
Out of Province (OOP) Data	This dataset will contain: - administrative data - clinical data - demographic data	-Out of Province -Notifications from other provinces/territories of Ontario residents diagnosed or treated for cancer in the notifying P/T	1. This data holding contains persons with OCR reportable diseases. The purpose of these records is to serve as source records to create incident cases for the Enterprise Data Warehouse (EDW)-OCR. Both alone, and as source records for incident cases, OOP data support management decision-making, planning, disease surveillance and research. 2. PHI is collected to ensure accuracy in linking records in EDW. PHI is used by internal and external researchers at the source record level.
Pathology Datamart	This dataset contains -administrative data -clinical data -demographic data	-PIMS	1. This data holding is derived from the PIMS data holding and uploaded into the EDW for planning and management purposes. 2. PHI is used to support management decision-making, planning, disease surveillance and research, as well to contribute to resolving

Data Holding	Data	Source	Statement of Purpose
	-facility data		incidence case data in the OCR.
RPDB Datamart	The dataset contains: - Ontario Health Insurance Number - administrative data - demographic data	-Ministry of Health and Long-Term Care	The RPDB is a listing of all persons insured under OHIP. This data is used to ensure that individuals in other data sources are identified correctly and to support analysis by demographic groups and geography.
Interim Annotated Tumour Project (ATP) Database	The dataset contains: - administrative data - clinical data - demographic data	-OICR -CCO's Cancer Registry	1. The Interim ATP Database provides an integrated set of data, combining tumour information from the Ontario Institute for Cancer Research's Tumour Bank with CCO's Cancer Registry, for the purpose of increasing the accuracy and utility of the information for both researchers and CCO planners. 2. PHI is used by researchers to study the association between genetics and response to cancer drugs. CCO also uses the PHI in this data holding to create clinical guidelines for the care and treatment of cancer patients in Ontario.
Ontario Renal Network (ORN)	The dataset contains: -Clinical data -Demographic data	-Hospitals	1. The purposes of the ORN data holding are • Performance measurement and management; • Monitoring of system quality; • System planning; and • Chronic Kidney Disease (CKD) funding model development. 2. PHI is used to support management decision-making, planning, disease surveillance and research activities.
Wait Times	The dataset contains:	-Hospitals	1. The purpose of this data holding is to enable the

Data Holding	Data	Source	Statement of Purpose
Information System (WTIS)	- administrative data - clinical data - demographic data	- Enterprise Master Patient Index (EMPI)	monitoring of wait times; the Ontario Wait Time Strategy implemented the web-based Wait Time Information System (WTIS) to facilitate wait time management and to provide the public with wait time information on surgical and diagnostic procedures. 2. PHI is collected from hospitals and the EMPI (which interfaces with the WTIS in order to organize patient information) and is used for the planning and management of the health care system.
Emergency Room National Ambulatory Reporting System Initiative (ERNI)	The dataset contains: - clinical data - demographic data	Hospital sites submit to CIHI-NACRS. Extract of file is transferred securely from CIHI to Access to Care (ATC) Informatics within CCO using Tumbleweed	1. The purpose of this data holding is to evaluate ER wait times for provincial ER/ALC Strategy, including but not limited to return on investment, performance improvement, Ministry LHIN Performance Agreements and data quality assessment. 2. PHI is collected to determine and remove duplicate data entry errors from the analysis as well as to calculate percentage of patients returning to an ER within a specified time period as a measure of quality of care and potential negative impact of ER focus.

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. Production Linkages (ongoing operational data linkages in support of Prescribed Entity Section 45 activities):

Linkage System	Data Holdings Linked	Year Implemented
Ontario Cancer Registry Information System (OCRIS)	- Activity Level Reporting - CIHI Discharge Abstract Database (DAD) - CIHI National Ambulatory Care Reporting System (NACRS) - Mortality (Office of the Registrar General) - Pathology Information Management System (PIMS) - Registered Persons Database	Operational since 1980's
Ontario Cancer Registry Information System (OCRIS)	- Activity Level Reporting, Access to Care	Operational since 1980's

z

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

Project Name	Data Holdings Linked	Year Approved by DAC
Adjuvant Chemotherapy study	OCR/ALR	2009
Breast Cancer study	OCR	2009
Lung Cancer study	OCR/ALR/NDFP	2009
Cancer Risk Factors study	OCR/OBSP/PIMS	2009
Breast Cancer study	OCR/ALR/NDFP	2009
Access to a Cancer Program study	OCR/ALR	2009
Ovarian Cancer study	OCR/ALR	2009
Cancer Cost study	OCR/ALR/NDFP	2009
Colorectal Cancer study	OCR/ALR/NDFP	2009
Leukemia study	OCR/ALR	2010
Breast Cancer study	PIMS/OCR	2010
Brain Metastasis study	OCR/ALR	2010
Colorectal Cancer study	OCR	2010
Breast Cancer study	OBSP/PIMS	2010
Skin Cancer study	PIMS/OCR	2010
FOBT study	CIRT/LRT	2010
Cancer Systemic Therapy study	OCR/ALR/NDFP	2010
Carcinoma study	OCR/ALR/NDFP	2010
Case Costing study	OCR/ALR/NDFP	2010
Malignant Pleural Mesothelioma study	OCR/ALR	2010

Project Name	Data Holdings Linked	Year Approved by DAC
Breast cancer treatment study	OCR/ALR/NDFP	2010
Chemotherapeutic Agents study	OCR/ALR/NDFP	2010
Prostate Cancer study	OCR/ALR/NDFP	2011
Bladder Cancer study	OCR/PIMS	2011
Colorectal Cancer study	OCR/PIMS	2011
Case Costing study	OCR/CIRT	2011
Chemotherapy study	OCR/ALR	2011
Penile Cancers study	OCR/ALR/PIMS	2011
Pancreatic cancer study	OCR/Mortality	2011

APPENDIX 3 to Indicators – Summary from the Log of PIAs

PIA	Date	Status	Description of Recommendations	Pending	Deferred	N/A	In Process	Complete	To be Started
CPOE	6-Apr-09	PIA Complete	The PIA recommends that CPOE: 1) Assign each patient to one or more locations within a single OPIS 2005 instance; 2) Assign patients VIP status; 3) Improve auditing features; 4) Create additional hospital-agent-accessible reports including patient-centric auditing reports; 5) Update existing license agreement; and 6) Provide additional best practice guidelines	0	4	0	0	2	0
WTIS-ALC	1-Nov-09	PIA Complete	The PIA recommends that WTIP (1) Execute license agreements with the 20 new post-acute facilities.	0	0	0	0	1	0
ERNI	11-Feb-10	PIA Complete	The PIA recommends that ERNI: 1) Amend the current CIHI-CCO DSA; 2) Appoint a CCO Data Steward; 3) Develop a Statement of Purpose for the collection of PHI; and 4) Include ERNI in ODDAR	0	0	0	0	4	0
ISAAC	1-Nov-09	PIA Complete	The PIA recommends that: (1) The amending agreement between the vendor and CCO	0	0	0	0	1	0

PIA	Date	Status	Description of Recommendations	Pending	Deferred	N/A	In Process	Complete	To be Started
			outline the vendor's privacy responsibilities and obligations.						
EDW	11-Feb-10	PIA Complete	The PIA recommends that: 1) The Statement of Purposes be updated, including the new data elements; 2) A TRA be conducted; 3) CCO review the User Agreement Template for iPort™; 4) CCO establish DSAs with external sources where PHI is collected directly for the EDW; 5) CCO designate a Data Steward; 6) develop a Statement of Purposes for the collection of PHI; 7) CCO provide a Statement of the Purpose to the entities that provide PHI directly to the EDW as part of the DSAs; 8) CCO conduct an assessment of the data elements required for the death data set and work with the data provider to eliminate or destroy any data elements that are not required; 9) The provision of PIMS PHI for permanent retention in the Pathology Data Mart be restricted to coded pathology reports; 10) If PHI is proposed for disclosure from the EDW for patient contact for research studies, screening activities or clinical trials, CCO document the business requirements and determine if there is an appropriate authority to disclose under PHIPA; 11) Measures be instituted in	0	0	1	0	13	0

PIA	Date	Status	Description of Recommendations	Pending	Deferred	N/A	In Process	Complete	To be Started
			iPort □ to elir counts less than n=6; 12) The Data Steward establish an inventory for the EDW data holding; 13) The EDW Project conform to the CCO Policy on Offsite Access and Wireless Networks; and 14) The EDW Project ensure that a browser cache is cleared when access to PHI is provided via iPort.						
ISAAC	10-Aug-10	PIA Complete	No privacy risks were identified in the PIA. As such, no recommendations arose from this assessment.	0	0	0	0	0	0
EB-PET	31-Dec-10	PIA Complete	The PIA recommended: 1) CCO to seek clarity on FIPPA's applicability to CCO clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities; 2) The HINP Agreement between the HICs and CCO to explicitly provide that all EB-PET program relevant PHI and PI are in the custody or under the control of the relevant HIC and not CCO, and that all access requests made to CCO for a record of PHI relating to the EB-PET program will be directed to the relevant HIC. 3) All parties to enter into a written services agreement with CCO; 4) A DSA must be executed between CCO (the prescribed entity) and ICES (the prescribed entity); 5) The Program to advise the	0	0	0	2	7	0

PIA	Date	Status	Description of Recommendations	Pending	Deferred	N/A	In Process	Complete	To be Started
			Privacy Office if and when new linkages and whether a permanent data holding will be created following these new linkages; 6) Develop data quality assurance practices; 7) Conduct a TRA; 8) Threat models and threat scenarios be developed; and 9) Develop a plain language description of its policies and procedures. *The finalized PIA included 9 recommendations						
Totals			**35 recommendations**	**0**	**4**	**1**	**2**	**28**	**0**

APPENDIX 4 to Indicators – Summary from the Log of PIAs (PIAs Reviewed since the prior review of the IPC)

Number	PIA	Date	Review	Description of Program
1	**ISAAC**	November 2009	Addendum to 2007 PIA	A web-based symptom screening tool provided by CCO to health care providers (and their patients, where available) to monitor patients' symptoms. Services expanded to include TeleISAAC.
2	**EDW**	November 2009	Addendum to 2008 PIA	The Data Warehouse project will create the necessary infrastructure to support the acquisitions and delivery of information to CCO and external information consumers, through a robust analytic web portal, for the population of cancer indicators, and in support of critical cancer planning, research and decision making.
3	**ISAAC**	August 2010	Addendum to 2007 PIA	A web-based symptom screening tool provided by CCO to health care providers (and their patients, where available) to monitor patients' symptoms. Program implemented HL7 integration solution.
4	**OBSP**	December 2010	Review of Program	The OBSP is a CCO – Ministry of Health and Long-Term Care initiative for the delivery of high quality breast screening to Ontario women. The OBSP cancer screening services are delivered to women age 50 and over at dedicated sites, affiliated hospitals and independent health facilities.

APPENDIX 5 to Indicators – Summary from the Log of Privacy Breaches

Breach #	Date of Notification to Privacy & Access Office	Outcome of Investigation	# of Recommendations Made	# of Recommendations Completed
1	20-Mar-09	Not Breach	3	3
2	02-Apr-09	Not Breach	2	2
3	9-Jun-09	Breach Root Cause: Policy Infraction	2	2
4	9-Nov-09	Breach Root Cause: Program Procedure Infraction	2	2
5	15-Oct-10	Not Breach	4	4
6	29-Oct-10	Not Breach	2	2
7	1-Nov-10	Breach Root Cause: Policy Infraction	1	1
8	2-Nov-10	Breach Root Cause: Policy Infraction	2	2
9	22-Nov-10	Not Breach	5	5
10	7-Jan-11	Not Breach	1	1
11	10-Jan -11	Not Breach	1	1
12	17-Feb-11	Breach Root Cause: Policy Infraction	1	1
13	23-Feb-11	Breach Root Cause: Policy Infraction	1	0
14	5-Aug-11	Not Breach	1	1
15	11- Aug -11	Breach Root Cause: Policy Infraction	2	2

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

Project	Type of Audit	Date Completed	Recommendations Descriptions	Mitigation Dates
Cardiac Care Network (CCN)	TRA	Apr-08	Recommendations are logged within each assessment.	Mitigation dates typically coincide with dates of assessments. Please review report summary for additional information about future risk register implementation.
WTIS Core	TRA	Jun-08		
Lab Interim Reporting Tool (LIRT)	TRA	Jul-08		
Resolink and Linking	TRA	Jul-08		
General Security Posture	TRA	Sep-08		
Annotated Tumour Project (ATP)	TRA	Oct-08		
Collaborative Staging	TRA	Oct-08		
ColonCancerCheck - InScreen	TRA	Aug-09		
OICR	Technical Profile	Sep-09		
Mendeley Online Software	Security Review	Oct-09		
List Management System (LMS)	TRA	Nov-09		
Wait Time Information System Alternative Level of Care	TRA	Dec-09		
Ontario Health Study (OHS)	Security Profile Vulnerability Assessment	Dec-09		
Alternative Level of Care (ALC) Upload Tool	Security Assessment	Jan-10		
Microsoft Bitlocker Encryption	Security Review	Jan-10		
Cardiac Care Network (CCN)	Vulnerability Assessment	Feb-10		
Logging, Monitoring, Audit System (LMAS)	Market Analysis	Mar-10		
CKD/ORN	Security Profile	Mar-10		
Active Directory (AD)	Info Security Review	Apr-10		

Project	Type of Audit	Date Completed	Recommendations Descriptions	Mitigation Dates
Enterprise Data Warehouse (EDW)	High-level Scope Assessment	May-10		
Microsoft Exchange / Outlook	Vulnerability Assessment	May-10		
PET Phase 1	Vulnerability Assessment Security Assessment	Jun-10		
Full Disk Encryption	Security Briefing Note	Jun-10		
Web Filtering Social Media	Security Briefing Note	Jun-10		
Collaborative Staging (CS) Automation	TRA Vulnerability Assessment	Jun-10		
Interactive Symptom Assessment and Collection (ISAAC) HL7	TRA	Jul-10		
Merx Bulk File Tool	Security Assessment	Jul-10		
Mobile Device Assessment - iPhone	Security Review	Jul-10		
Service Desk Express (SDE) Survey	Security Assessment	Aug-10		
Wireless Network Infrastructure	TRA Vulnerability Assessment 3rd party Vulnerability Assessment	Aug-10		
Mobile Device Assessment - Windows Mobile	Security Review	Aug-10		
SharePoint	TRA	Sep-10		
Password Reset	Security Review	Sep-10		
LMAS	TRA	Sep-10		
Statistics Canada	Security Requirements Review	Sep-10		
Mobile Device Assessment - Android	Security Review	Nov-10		
SETP	Vulnerability Assessment	Nov-10		

Project	Type of Audit	Date Completed	Recommendations Descriptions	Mitigation Dates
User Account Audits (4 Applications)	Account Review	Dec-10		
Transana	Security Review	Jan-11		
Esri ArcGIS	Security Review	Feb-11		
Mobile Device Assessment – Symbian (Nokia)	Security Review	Mar-11		
PET Phase 2	TRA Vulnerability Assessment	Apr-11		
DAP-EPS	TRA Vulnerability Assessment	May-11		
Brachytherapy	Security Profile	June-11		
Telecommuting	Risk Assessment	June-11		
Lync	Vulnerability Assessment	July-11		
e-Path	TRA Vulnerability Assessment	Aug-11		
ALC-EDW Expansion	Vulnerability Assessment	Aug-11		
WTIS SIT6 Environment	Vulnerability Assessment	Aug-11		
Microsoft PowerPoint Broadcast	Security Review	Aug-11		
Beyond Compare	Security Review	Aug-11		
Camtasia Studio	Security Review	Aug-11		
CMS	Vulnerability Assessment	Sept-11		

APPENDIX 7 to Indicators – 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 individuals no longer with	15-Dec-09	Low	No	Yes	15-Dec-09	Disabled dormant accounts; verified inactivity after employee exits	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 processes; AD cleanup

	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
	CCO												
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	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

	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
	Aug 26, 2010)												BitLocker
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

	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
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
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

	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
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
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

	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
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
11	Unusual behavior caused by an automated process detected through auditing and monitoring (activity	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

	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
	on July 11, 2011; detection on July 12, 2011)												
12	Hospital uploaded PHI into WTIS/EMPI Conformance	12-Aug-11	Medium	Yes	Yes	12-Aug-11	The environments were shut down; the PHI was deleted; coordination with eHO	12-Aug-11	N/A	Aug 12- , 2011	TBD	TBD	TBD

	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
13	A BA asked another BA to query his personal physician in CCC HUB and reviewed the results for the SAR-OMD Portal integration project	15-Aug-11	Low	No	Yes	15-Aug-11	It was determined in the interview with the employee that his intent was not malicious and that the physician record had no patients attached to it	15-Aug-11	N/A	Aug 15-16, 2011	The employee was advised to obtain proper authorization before taking such actions and informed of the policy; privacy awareness training to be given	TBD	TBD
14	Hospital (same as #12) uploaded PHI into WTIS/EMPI	16-Aug-11	Medium	Yes	Yes	16-Aug-11	The environments were shut down; the PHI was deleted; coordination with eHO	16-Aug-11	N/A	Aug 16- , 2011	TBD	TBD	TBD

	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
	Conformance												

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 of the 2005 and 2008 triennial reviews of CCO's practices and procedures, with respect to its role as a prescribed entity, 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	Implementing a Privacy Risk Management	Completion Date:

	Management Framework	Standard	2012

SWORN AFFIDAVIT

I, Michael Sherar, the President and Chief Executive Officer of Cancer Care Ontario, MAKE OATH AND SAY:

1. Cancer Care Ontario, an entity prescribed under subsection 18(1) of Ontario Regulation 329/04 to the Ontario *Personal Health Information Protection Act, 2004* (PHIPA) for the purposes of subsection 45(1) of *PHIPA*, has in place policies, procedures and practices to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

2. The policies, procedures and practices implemented by Cancer Care Ontario comply with the *Personal Health Information Protection Act, 2004* and the regulations thereto.

3. The policies, procedures and practices implemented by Cancer Care Ontario comply with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* that has been published by the Information and Privacy Commissioner of Ontario.

4. Cancer Care Ontario has submitted a written report to the Information and Privacy Commissioner of Ontario in compliance with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

5. Cancer Care Ontario has taken steps that are reasonable in the circumstances to ensure compliance with the policies, procedures and practices implemented and to ensure that the personal health information received is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

SWORN (OR AFFIRMED) BEFORE ME	)
	)
at the City/Town/Etc. of Toronto, in the	)
	)
Metropolitan Toronto of	)
	)
Ontario, on January 28, 2011.	)

Michael Sherar, in his capacity as President
and Chief Executive Officer of
Cancer Care Ontario and not in his personal capacity

Commissioner for Taking Affidavits
Pamela C. Spencer

APPENDIX A – SUPPORTING DOCUMENTATION

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

2. ***Access Care 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. ***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. ***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. ***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. ***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. ***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. ***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. ***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. ***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. ***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.

14. ***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.

15. ***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.

16. ***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:

    i. Ensure the consistent application of cryptographic safeguards across CCO;

    ii. Establish a minimum baseline for cryptographic security at CCO that is in line with industry standards and best practices; and

    iii. Facilitate necessary transitions to stronger or newer cryptographic methods as older methods become obsolete.

17. ***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.

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

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

20. ***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.

21. ***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.

---

22. ***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. ***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).

---

24. ***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.

---

25. ***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.

---

26. ***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.

---

27. ***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.

---

28. ***Data Use and Disclosure Standard*** applies to disclosures and uses of PHI to internal and external users for research and non-research purposes. The Standard ensures disclosures of PHI comply with PHIPA and CCO’s privacy obligations. The Data Use & Disclosure

Standard sets out the circumstances in which PHI is permitted to be disclosed for research purposes.

---

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

---

32. ***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. ***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. ***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. ***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. ***IM/IT Stage - Gating Process and Project Lifecycle Methodology*** is used at CCO to review projects at various phases of the project lifecycle to ensure risk, status, expenditures and process are appropriately managed and all supporting business units are engaged.

37. ***IM/IT Stage – Gating Policy*** defines the stage-gate review process for approval of projects requiring Information Management **(IM)** and Information Technology **(IT)** deliverables, services or resources, and to ensure that the appropriate review is conducted at critical transition points in the project lifecycle.

38. ***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.

39. ***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).

40. ***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.

41. ***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.

42. ***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.

43. ***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.

44. ***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.

45. ***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.

46. ***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

---

47. ***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

.

---

48. ***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.

---

49. ***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.

---

50. ***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.

---

51. ***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.

---

52. ***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.

---

53. ***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.).

---

54. ***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.

---

55. ***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.

---

56. ***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.

---

57. ***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.

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.

---

58. ***Privacy & Access Office Operational Manual*** articulates all of the components of the CCO Privacy Program and the day to day responsibilities of members of the Privacy & Access Office, including the management and operation of the CCO Privacy & Access Office Remediation program; the privacy training and awareness program; the Privacy Gating processes within the CCO Project Management Lifecycle framework; and all key elements of privacy support services to CCO programs and projects.

---

59. ***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.

---

60. ***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.

---

61. ***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.

---

62. ***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.

---

63. ***Privacy FAQs*** are a list of frequently asked questions which the Privacy & Access Office receives regarding its privacy policies and practices. 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.

---

64. ***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.

---

65. ***Privacy Inquiries and Complaints Procedure*** describes how CCO responds to inquiries and complaints received from individuals who are requesting information or challenging CCO's compliance with its information practices. Specifically, the procedure describes how an individual can make an inquiry or complaint, the steps which the Privacy & Access Office will follow in responding to and tracking the inquiry or complaint and how compliance with the procedure is enforced at CCO.

---

66. ***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.

67. ***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.

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

69. ***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.

70. ***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.

71. ***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.

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

73. ***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.).

74. ***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.

75. ***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.

76. ***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.

77. ***Statement of Information Practices*** describe 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.

78. ***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.

79. ***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.

80. ***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.

81. ***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.

82. ***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.

83. ***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.

84. ***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.

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

---

86. ***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.

---

87. ***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.

APPENDIX B – SUPPORTING TOOLS

1. ***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. ***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. ***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. ***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. ***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. ***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.

7. ***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 Amended Policies & Procedures:* tracks all amendments made to CCO's privacy policies and procedures, including a description of the amendment made and the date it was communicated to CCO employees.

   ii. *Log of Privacy Impact Assessments:* tracks all PIAs initiated and/or completed at CCO, including identified risks and mitigating strategies.

   iii. *Log of Privacy Breaches:* tracks all privacy incidents and breaches reported at CCO, including identified risks and mitigating strategies.

   iv. *Log of Privacy Inquiries and Complaints:* tracks all inquiries and complaints received by CCO in regards to the Privacy Program.

   v. *Log of IPC Recommendations:* tracks the recommendations arising from the IPC's triennial reviews of CCO's information management practices and the manner in which these recommendations will be addressed.

   vi. *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.

   vii. *Log of Third Party Service Providers with Access to PHI:* tracks agreements with third parties that have access to PHI.

---

8. ***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.
