Privacy & Access Office

Ontario

2014 Prescribed Entity and Prescribed Person Triennial Review Report

December 2014
Final version

CCO Legal & Privacy Office
620 University Avenue, 13th floor
Toronto, ON M5G 2L7
Phone: 416.217.1816
Fax: 416.971.6888
Email: privacyandaccessoffice@cancercare.on.ca

Ontario
Cancer Care Ontario
Action Cancer Ontario

Table of Contents

Table of Abbreviations

ACCU	Aboriginal Cancer Control Unit
AEAD	Agency Establishment & Accountability Directive
ALR	Activity Level Reporting
ATC	Access to Care
ATSCP	Aboriginal Tobacco Smoking Cessation Program
BCWF	Breast Cancer Well Follow-up Care
CAPE	Client Agency Program Enrolment
CBCRP	Case-by-Case-Review Program
CBCF	Canadian Breast Cancer Foundation
CC	CSP Contact Centre
CCC	Colon Cancer Check
CCO	Cancer Care Ontario
CHDB	Claims History Data Base
CIHI	Canadian Institute for Health Information
CIO	Chief Information Officer
CIRT	Colonoscopy Interim Reporting Tool
CKD	Chronic Kidney Disease
CMS	Content Management System
CPDB	Corporate Provider Database
CPO	Chief Privacy Officer
CPOE	Computerized Physician Order Entry
CPSO	College of Physicians and Surgeons of Ontario
CRC	Colorectal Cancer
CSR	Contact Centre Representative
CSP	Cancer Screening Program (formerly known as ICS)
DAC	Data Access Committee
DAD	Discharge Abstract Database
DAP	Diagnostic Assessment Program

DAP-EPS	Diagnostic Assessment Program – Electronic Pathway Solution
DOB	Date of Birth
DSA	Data Sharing Agreement
EBP	Evidence Building Program
EDW	Enterprise Data Warehouse
eCCO	CCO's Intranet
EISO	Enterprise Information Security Office
EISP	Enterprise Information Security Program
EMPI	Enterprise Master Patient Index
EMRs	Electronic Medical Records
ERM	Enterprise Risk Management
ERNI	Emergency Room National Ambulatory Reporting System Initiative
ESAS	Edmonton Symptom Assessment System
ET	CCO's Executive Team
FH	Fulfillment House for CSP
FIT	Fecal Immunologic Test
FIPPA	*Freedom of Information and Protection of Privacy Act*
FOBT	Fecal Occult Blood Test
FPP	FIT Pilot Participant
HIC	Health Information Custodian
HINP	Health Information Network Provider
HL7	Health Level 7
HO-011	PHIPA Order HO-011
HRIS	Human Resources Information System
ICMS	Integrated Client Management System
ICR	Interval Cancer Review
ICS	Integrated Cancer Screening (former name of the CSP)
ICP	Integrated Cancer Plan
IDAR	Internal Data Access Request

IM	Information Management
IM/IT	Information Management and Information Technology
IMRT	Intensity Modulated Radiation Therapy
IPC	Information and Privacy Commissioner/Ontario
ISAAC	Interactive Symptom Assessment and Collection
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JRC	Joint Review Committee
LHIN	Local Health Integration Network
LMAS	Logging, Monitoring, and Auditing System
LMG	Lowe-Martin Group, FH for CSP
LRA	Local Registration Agent
LRT	Lab Reporting Tool
Manual	*Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*
MCC	Multidisciplinary Case Conference
MD	Doctor
MDS	Minimum Data Set
MGR	Manager
MIS	Management Information Systems in Canadian Health Service Organizations
MMs	Mammograms and Mammogram Reports
MOHLTC	Ministry of Health and Long-Term Care
MOU	Memorandum of Understanding
MRN	Medical Record Number
NACRS	National Ambulatory Care Reporting System
NCOA	National Change of Address
NDFP	New Drug Funding Program
OBSP	Ontario Breast Screening Program
OCR	Ontario Cancer Registry
OCRIS	Ontario Cancer Registry Information System

OCSP	Ontario Cervical Screening Program
OCSR	Ontario Cancer Screening Registry
ODDAR	Online Direct Data Access Request (the former version of IDAR)
OFCCR	Ontario Familial Colorectal Cancer Registry
OHD	OPIS Help Desk
OHIN	Ontario Health Insurance Number
OHP	Out of Hospital Premises
OLIS	Ontario Laboratories Information System
OOC	Out-of-country
OPIS	Oncology Patient Information System
ORBC	Operating Room Benchmark Collaborative
ORN	Ontario Renal Network
O.Reg.	Ontario Regulation
ORRS	Ontario Renal Reporting System
ORRS R.3.0	ORRS Release 3.0
PACS	Picture Archiving and Communication System
PAF	Personnel Action Form
PAO	Privacy & Access Office
PCCIP	Prevention & Cancer Control Information Program
PCP	Primary Care Physician
PDRP	Provincial Drug Reimbursement Program
PE	Prescribed Entity
PEBC	Program in Evidence-Based Care
PEM	Patient Enrollment Model
PHI	Personal Health Information
PHO	Public Health Ontario
PHIPA	*Personal Health Information Protection Act, 2004*
PI	Personal Information
PIA	Privacy Impact Assessment

PIMS	Pathology Information Management System
PP	Prescribed Person
PPAF	Preliminary Privacy Assessment Form
QA	Quality Assurance
RCC	Regional Cancer Centre
RD	Regional Director
REB	Research Ethics Board
RFC	Request for Change
RFP	Request for Proposals
RPCL	Regional Primary Care Lead
RTS	Return to Sender
SAR	Screening Activity Report
SAS	Statistical Analysis System
SCRCP	Survivorship Colorectal Cancer Pilot
SCT	Stem Cell Transplant
SDM	Substitute Decision-Maker
SEER*Stat	Surveillance, Epidemiology, and End Results Statistical
SETP	Surgical Efficiency Targets Program
SNMP	Simple Network Management Protocol
SOW	Statement of Work
SPPRMC	Strategic Planning, Performance & Risk Management Committee
SQL DB	Structured Query Language Data Base
Sr.	Senior
SRI	Sunnybrook Research Institute
STIP	Systemic Treatment Information Program
TRA	Threat Risk Assessment
UHN	University Health Network
VA	Vulnerability Assessment
VIP	Very Important Person

WAHA	Weeneebayko Area Health Authority
WTIS	Wait Times Information Strategy/System

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 Ontario *Cancer Act*. 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 $950 million public health care dollars to hospitals and other cancer care providers to deliver high quality, timely cancer services;
- Implements provincial cancer prevention and screening programs designed to reduce cancer risks and raise screening participation rates;
- Works with cancer care professionals and organizations to develop and implement quality improvements and standards;
- Uses electronic information and technology to support health professionals and patient self-care and to continually improve the safety, quality, efficiency, accessibility and accountability of cancer services;
- Plans cancer services to meet current and future patient needs, and works with health care providers in every Local Health Integration Network (**LHIN**) to continually improve cancer care for the people they serve; and
- Rapidly transfers new research into improvements and innovations in clinical practice and cancer service delivery.

In addition to cancer, CCO has other core lines of business including supporting and hosting the provincial Access to Care (**ATC**) program, which is a part of the Government of Ontario's Wait Times Information Strategy (**WTIS**).

CCO has also worked with renal leadership in Ontario to operate the Ontario Renal Network (**ORN**). In 2010, the MOHTLC formally transferred the provincial oversight and co-ordination of the Chronic Kidney Disease (**CKD**) Management Program to the ORN under the auspices of CCO. As part of this process, CCO entered into an accountability agreement with the MOHLTC dated January 29, 2010 in order for CCO to establish, manage and coordinate the ORN as a work unit within CCO and to support the growth of CKD services across Ontario.

CCO also administers the Provincial Drug Reimbursement Program (**PDRP**), which includes the New Drug Funding Program (**NDFP**), the Evidence Building Program (**EBP**), and the Case-by-Case-Review Program (**CBCRP**) for cancer drugs, on behalf of the MOHLTC. Beyond CBCRP, CCO offers ad-hoc support (*e.g.*, reviewer identification) to out-of-country (**OOC**) requests when required for non-drug funding requests, such as cancer-related tests, radiation, and surgery. CCO is currently developing the OOC program, which it will administer on behalf of the MOHLTC, in order to enhance timeliness, consistency, and quality of decision-making; ensure decisions are being guided by best evidence; reduce inappropriate requests, and support patient access to treatments/services that can and should be offered outside Canada while supporting integration and introduction of new cancer programs/services into Ontario.

Each of these programs is 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 the Ontario *Personal Health Information Protection Act, 2004* (**PHIPA**).

Prescribed Entity

Subsection 45(1) of PHIPA permits health information custodians (**HIC**) 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 (**Prescribed Entity or PE**). Many 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, for health system planning and management purposes.

Prescribed Person

CCO is also designated as a 'prescribed person' under clause 39(1)(c) of PHIPA with respect to its role in compiling and maintaining screening information for colorectal, cervical and breast cancer in the Ontario Cancer Screening Registry (**OCSR**) under s. 13(1) of O.Reg. 329/04 (**Prescribed Person or PP**). This designation grants CCO the authority to collect, use and disclose PHI for the purposes of facilitating or improving the provision of health care with respect to colorectal, cervical and breast cancer.

In 2011, the cancer screening program entitled ColonCancerCheck (**CCC**) was expanded into what is now the Cancer Screening Program (**CSP**) more broadly encompassing CCO's Ontario Breast Screening (**OBSP**) and Cervical Screening (**OCSP**) programs. The CSP is an expansion of the service delivery model used by the CCC program, which invites, recalls and reminds a target population of Ontarians to proactively be screened for colorectal cancer. The CSP also sends out results letters to individuals who have had preliminary screening tests for colorectal cancer and cervical cancer; implementation of this model for breast cancer screening is planned for 2014/15.

The CSP is comprised of 3 screening modules: i) breast screening ii) cervical screening and iii) colorectal cancer screening. As a Prescribed Person, CCO has the authority to collect, use and disclose PHI for the purpose of facilitating or improving this provision of breast, cervical and colorectal cancer screening services and care for Ontarians. The CSP's mandate includes:

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

The operational status of each of the 3 cancer screening modules is as follows:

1. Colorectal Screening: The CCC program is fully operational and has robust privacy controls embedded within the administrative, processing and technical infrastructure. This program was reviewed in 2008 by the Information and Privacy Commissioner of Ontario (**IPC**) and received its first three-year approval of its privacy practices. It was subsequently approved for another three years in 2011.

2. Cervical Screening: The OCSP was integrated into the existing screening infrastructure in September 2013. On July 27, 2012, CCO sent the Office of the IPC a copy of the Privacy Impact Assessment (**PIA**) on Cervical Screening Correspondence – Phase 1 dated June 19, 2012 (the "Cervical Correspondence PIA"). The authorities analysis contained in the Cervical Correspondence PIA contained statements questioning CCO's authority to use and disclose PHI under s. 49(1) of PHIPA.. On August 30, 2012, the Office of the IPC sent CCO a letter stating that the Office had reviewed the Cervical Correspondence PIA, and concurred with the comments contained in the Cervical Correspondence PIA questioning CCO's reliance on s. 49(1). The IPC recommended that the authorities analysis contained in the Cervical Correspondence PIA be amended so as to rely on certain provisions of FIPPA in place of s. 49(1) of PHIPA.

   On September 11, 2012, counsel for CCO discussed the IPC Letter with counsel for the Office of the IPC. In this discussion, counsel for CCO explained that the recommendation contained in the IPC Letter concerning s. 49(1) of PHIPA would affect all of the Prescribed Person PIAs, not just the Cervical Correspondence PIA. Counsel for CCO suggested that instead of amending the Cervical Correspondence PIA, CCO should prepare a General Addendum to all of its "Prescribed Person" PIAs to comprehensively address the issue of reliance on s. 49(1) of PHIPA. Counsel for the Office of the IPC was supportive of this approach. This General Addendum was provided to the IPC in December, 2012.

3. Breast Screening: The OBSP will be integrated into the existing screening infrastructure in 2014-15. The breast screening module follows a similar service delivery methodology as the one in place for colorectal and cervical screening. The PIA for the OBSP is expected to be completed in the fourth quarter of 2013/14. Once completed, a copy of the OBSP PIA will be provided to the Office of the IPC for its review.

Prescribed Entity and Prescribed Person Triennial Review

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 IPC on a triennial basis in order for HICs, 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.

Similarly, subsection 13(2) of O. Reg. 329/04 requires each Prescribed Person to have in place practices and procedures to protect the privacy of the individuals whose PHI it receives and to maintain the confidentiality of that information. Subsection 13(2) further requires each

prescribed person to ensure that these practices and procedures are approved by the IPC on a triennial basis in order for HICs, and other persons authorized under PHIPA, to disclose PHI to the prescribed person without an individual's consent.

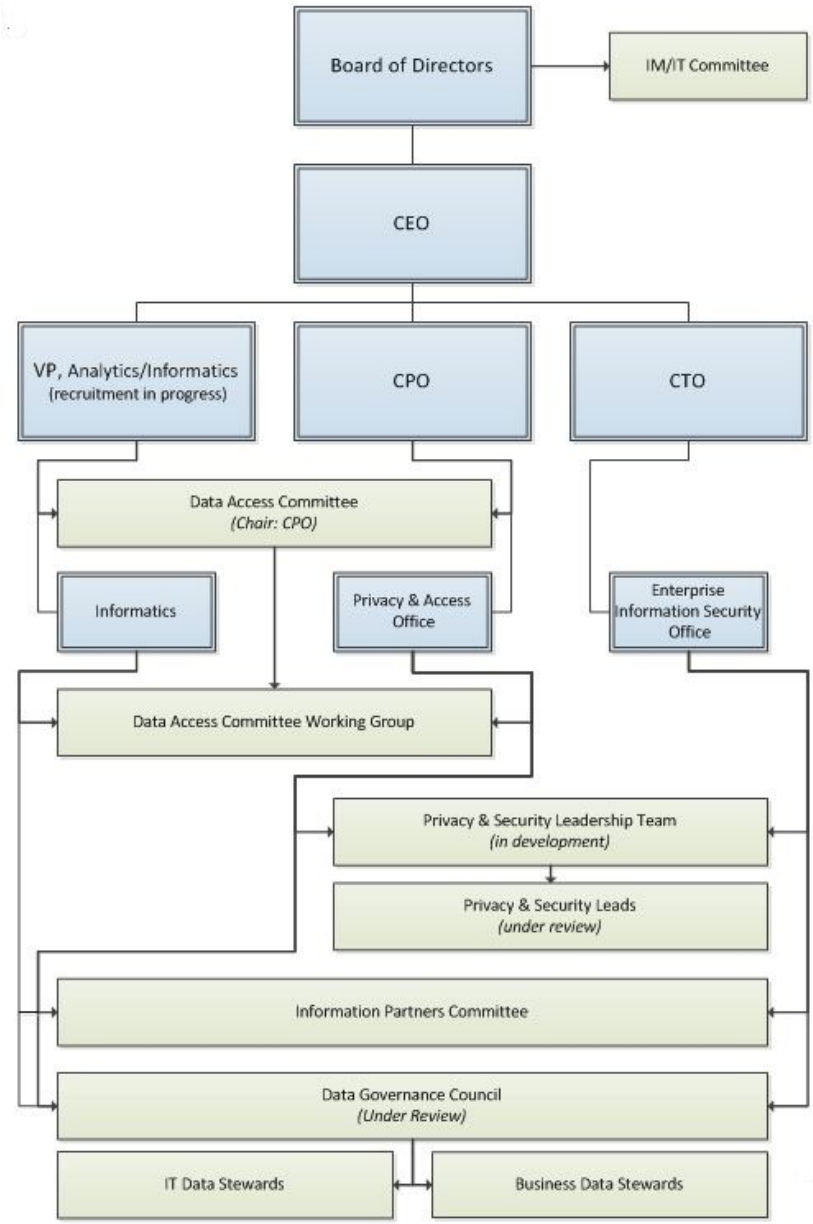
The first three-year approval of CCO's practices and procedures as a Prescribed Entity was received from the IPC effective November 1, 2005. CCO had its status renewed by the IPC on October 31, 2008 and on October 31, 2011 for additional three-year terms, respectively. This report constitutes CCO's submission to the IPC for the 2014 approval process in respect of its Prescribed Entity and Prescribed Person roles.

Separate CCO Prescribed Person and Prescribed Entity Triennial Review Reports were submitted to the IPC for the 2011 triennial review process. For the 2014 review, CCO received approval from the IPC to submit a combined Prescribed Person report and Prescribed Entity report.

CCO's Privacy Program

CCO's privacy governance structure informs its overall privacy management practices, including leadership, strategy, priorities and risk management. The privacy governance structure provides assurance that the strategies, policies, standards, processes and resources to manage privacy risk are aligned with CCO's objectives and are consistent with applicable laws, standards and best practices. The chart below sets out how privacy and security management is organized at CCO, followed by more detail about key aspects of the organizational structure**.**

Privacy and Security Governance Structure*



*CCO's Executive Team has completed a reorganization, which may result in further changes to this structure.

The CCO Board of Directors

CCO's accountability for sound privacy governance practices resides at the highest level of the organization, its Board of Directors. The Board receives a report on privacy matters annually and on an ad-hoc basis, as required. The Annual Privacy Report is delivered by CCO's Chief Privacy Officer (**CPO**) to the Board's Information Management and Information Technology (**IM/IT**) Committee.

The CPO (who is also CCO's General Counsel), provides the Board with relevant information on legal compliance matters, including privacy and security matters, any significant privacy or security breaches, privacy and security audit reports, new legislative, regulatory and industry developments of note, and the status of the IPC's triennial review and any recommendations arising therefrom. The CPO also reports to the Board on privacy and security risks, through its Enterprise Risk Management (**ERM**) Report, which is also provided to the MOHLTC as part of CCO's Annual Business Plan.

The Executive Team

The CCO Executive Team (**ET**) supports and champions the privacy program at CCO, actively advocating a privacy respectful culture. On an annual basis, the Annual Privacy Report is presented to the ET, by CCO's CPO and the Director, Privacy & Access**.**

The ET is briefed as required, and at least annually, through the Annual Privacy Report and the ERM Report, on privacy and security matters, such as proposed major initiatives, significant privacy or security incidents or near incidents, privacy and security audit reports, new legislative, regulatory and industry developments, the status of the Privacy Risk Register and the status of the IPC's triennial review and any recommendations arising therefrom.

The CPO

Accountability for privacy compliance with PHIPA and with CCO policies, at the operational level, ultimately resides with CCO's President and CEO. This function has been formally delegated to CCO's CPO. The CPO is able and expected to provide privacy representation on the most senior decision-making bodies within CCO.

The CPO also acts as Head under the Ontario *Freedom of Information and Protection of Privacy Act* (**FIPPA**)*,* as the delegate of the Board Chair. The CPO is a co-chair of CCO's Data Access Committee, which reviews all requests to CCO for access to PHI for research purposes. The CPO oversees the day-to-day operations of the privacy program through the Director, Privacy & Access, and advises on and recommends all enterprise-level privacy-related policy decisions for the organization.

The Director, Privacy & Access

The Director, Privacy & Access manages the Privacy & Access Office (**PAO**) and reports directly to the CPO. The Director, Privacy & Access is specifically responsible for:

(i) Managing the day-to-day operations of CCO's privacy program;

(ii) Ensuring that Business Unit Managers establish, implement, monitor and assess privacy program controls on an ongoing basis;

(iii) Overseeing the provision of privacy advice and support to all business functions;

(iv) Ensuring that the suite of privacy policies is comprehensive, up-to-date and compliant with applicable law and standards;

(v) Overseeing the development and provision of privacy training;

(vi) Advocating for privacy within the organization;

(vii) Ensuring high quality and consistent privacy reviews, audits/compliance monitoring, and benchmarking, as appropriate;

(viii) Ensuring that appropriate vendor management and other privacy-related agreements are in place as required;

(ix) Overseeing the management of access to information requests; and

(x) Monitoring legal and other developments in the privacy arena.

The Privacy & Access Office

The PAO is comprised of the Director, Privacy & Access, supported by eleven staff, including a Senior Legal Counsel, Privacy Managers, Senior Privacy Specialists and a Privacy Analyst. The complete Organizational Structure for the PAO is set out at Appendix A. It has been designed to enable the establishment, maintenance and monitoring of a privacy program that meets PHIPA requirements and other key privacy drivers, and a FIPPA-compliant access program. More specifically, the PAO has the following objectives:

- Build a culture of privacy within the organization;
- Deliver client-oriented privacy-advisory services across CCO;
- Ensure CCO's compliance with privacy and access legislation and policies.

The PAO meets these objectives through close ties to the Business Units and programs at CCO. Every Business Unit at CCO has an assigned Privacy Manager, who meets at least quarterly with each Business Unit Manager to discuss business initiatives and associated privacy needs and challenges. Privacy needs and challenges are reported to the Director, Privacy & Access and inform the annual Privacy Oversight and Review Plan, the Annual Privacy Report, and the Enterprise Risk Management Register.

The PAO is supported by the ET at CCO, all of whom champion privacy within their respective divisions. The PAO is further supported by:

- the CCO Information Partners Committee;
- the Data Stewards Program; and
- a refreshed Privacy & Security Leads program, which is in development.

Information Partners Committee

Responsibility for information governance at CCO is shared by three departments: Enterprise Information Security, Informatics, and Privacy & Access. Each of these departments has its own set of responsibilities; however these areas of responsibility have significant points of intersection. Effective communication and integration between the Information Partners is vital to successful information governance overall. Consequently, CCO has recently established the Information Partners Committee, comprised of the Senior Manager, Enterprise Information Security, the Director, Enterprise Data Management and the Director, Privacy & Access.

The Information Partners Committee meets at least monthly to review CCO information management policies and procedures in accordance with CCO's *Privacy Audit and Review Procedure* and other relevant monitoring policies and procedures. The Information Partners also provide consultation and advice related to (i) the triennial review by the IPC, (ii) CCO's overall information management practices, (iii) the implementation of recommendations or orders by the IPC, (iv) privacy and security breach management, and (v) other information management initiatives.

The Data Stewards Program and Privacy and Security Leads

The PAO, the Enterprise Information Security Office (**EISO**) and the Informatics Centre of Excellence are currently developing an enhanced Data Stewards Program, which includes Privacy and Security Leads.

The Data Stewards Program will be comprised of a Business Data Steward from every program as well as Information Technology (**IT**) Data Stewards. It will be overseen by the Director, Enterprise Data Management and supported by the Director, Privacy & Access and the Senior Manager, Enterprise Information Security. Business Data Stewards will be fully embedded in the Business Unit and familiar with daily operations of their respective programs and also function as Privacy and Security Leads. They will inform the Director, Privacy & Access and the Senior Manager, Enterprise Information Security, and each other, as required, about proposed new business initiatives, privacy and security near-misses, or any new privacy or security risks that have been identified.

Similarly, IT Data Stewards are intended to be deeply knowledgeable about the information technology structures, practices and safeguards relating to data holdings in their business unit and can advise the Director, Privacy & Access, the Senior Manager, Enterprise Information Security, and each other about risks and activities from an information technology perspective. In turn, the Director, Privacy & Access and the Senior Manager, Enterprise Information Security, inform the Business Data Stewards of any new privacy or security program initiatives, new or pending legislative or regulatory developments in the privacy or information security field, new privacy or information security compliance risks to be aware of, and any specific program monitoring expectations. Data Stewards will receive additional privacy and security training and also play a role in advocating a privacy respectful culture within their program. A comprehensive Privacy & Security Leads program is currently in development jointly between the PAO and the EISO and is expected to be implemented in 2014.

The following constitute CCO's key privacy program controls:

(i) Policies, standards, procedures and guidelines

The Privacy Policy Framework follows a tiered approach with enterprise policies at the top, followed by mandatory conformance standards and then unique program area procedures. Each subordinate policy governance tier draws its authority from the higher tiers by providing more deployment details but not establishing conceptually new principles, requirements or responsibilities. 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 designated to support and conform to a policy. Procedures are a series of steps taken to accomplish an end goal. Guidelines are not mandatory, but they provide additional detail or context with the aim to streamline a particular process.

The PAO reviews CCO's privacy policies, standards and procedures on an on-going basis in order to ensure that these documents continue to reflect privacy best practices and PHIPA and FIPPA legislative requirements. Following CCO's last IPC Triennial Review in 2011, the PAO has been reviewing all of its policies, standards and procedures and making amendments where necessary. Review of privacy policies is ongoing.

(ii) Projects, program and process change controls

Privacy assurance & risk management, the core service provided by the PAO, supports individual programs and projects to ensure compliance with applicable privacy legislation and CCO's privacy policies. The PAO provides the following services to support privacy assurance and risk management: contribution to architecture documents; privacy impact assessments; data sharing agreements; procurement support; communication materials; and standard operating procedures.

A PIA provides a framework to ensure that privacy is considered throughout program or system design. In accordance with CCO's *Privacy Impact Assessment Standard*, a PIA is conducted when material changes are made to an existing program or system, or when a new program or system that will collect PHI (and/or "personal information" as that term is defined in FIPPA (**PI**)) is developed. A PIA highlights any privacy risks associated with a program or system and, where required, details mitigating strategies and an action plan.

An Addendum to a PIA is conducted to assess changes to existing programs or information systems for which a PIA has already been conducted, but where the proposed changes are found to be minor and there are no identified changes to the legislative authority. Where there is a change to the legislative authority under which a program is operating, a new PIA is required.

Privacy artifacts, including the PIA and PIA Addendum, are embedded within the IM/IT Gating Process to ensure that projects with an Information Management (**IM**) or IT component are considered by the PAO for compliance, authority to collect, use and/or disclose the data required, and to ensure that appropriate privacy controls are in place.

(iii) External requests – controls that limit access

External requests for CCO data may be made by the public. The Research Data Request Form is used for requests for data for research studies. Requests for data for other purposes may be made on the *General Data Request Form* located on the CCO website. Forms must be signed and submitted to CCO's Information Management Coordinator, who validates completed requests. Upon the completion of a valid research request, the Data Access Committee (**DAC**) at CCO will evaluate the request. The DAC is co-chaired by CCO's CPO and Chief Information Officer (CIO). The DAC may approve a request, deny a request (fails to meet CCO's *Data Use and Disclosure Policy* requirements for disclosure), or request further information or clarification before reaching a decision. Copies of the *Data Use and Disclosure Policy* are available by request from the Information Management Coordinator and also from CCO's website.

(iv) Inventory of data holdings

CCO maintains a central, online repository which describes all CCO data holdings, both PHI and non-PHI. This repository is currently for internal use only, with plans to provide limited access to the public. The Data Catalogue provides a single location for obtaining information about CCO data, including associated programs and subjects, data start and end dates.

(v) Technical and physical safeguards

In order to protect PHI and PI, the PAO works in close partnership with the EISO, which is responsible for the operation and development of CCO's Information Security Program. The Information Security Program at CCO is comprised of a broad range of activities and is delivered under the authority of the Chief Information Officer.

The mandate of the Information Security Program includes the safeguarding of CCO digital assets, including PHI and PI, to ensure the integrity, availability and confidentiality of data and compliance with regulatory obligations. The EISO also supports CCO's daily business and program operations, and provides consultations concerning project activities resulting in new information systems.

(vi) Training and awareness

The PAO provides ongoing privacy communications and training to maintain a culture of privacy across the organization. There are three components of the PAO training program:

(a) Privacy Training for New Employees

As part of the broader Human Resources orientation, this in-person training session introduces new employees to the PAO. The presentation, delivered by a member of the PAO, briefly describes the governance structure of the office, CCO's obligations under PHIPA and FIPPA, and privacy best practices and services offered by the PAO. This presentation also defines important terms, such as 'PHI' and 'privacy breach'; provides examples of common privacy breaches and informs employees of steps to be taken in the event of a privacy incident or breach. All new employees are required to attend this orientation session as part of their onboarding process. CCO hiring managers are responsible for ensuring compliance with this requirement.

(b) Core Privacy & Security Training eLearning Curriculum

The *Core Privacy & Security Training eLearning Curriculum* at CCO is a web-based, compulsory training program for new employees, including service providers with access to PHI, students, researchers and others with access to CCO systems, addressing CCO's Privacy and Information Security Programs. They are informed of this training requirement at the new employee orientation session, as well as through CCO's intranet site and the on-boarding package for new employees.

The eLearning curriculum describes CCO's status under PHIPA and its obligations under the Act. The training also defines terms, such as PHI, and describes the applicable privacy and security principles and the privacy and security breach management program at CCO. When the *Core Privacy & Security eLearning Training Curriculum* is completed, a Privacy and Security Acknowledgement form must be read and digitally accepted. This form includes an acknowledgment that the individual has understood CCO's *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (*CCO's Privacy Policy) and the Information Security Code of Conduct and has completed and understood the *Core Privacy & Security Training eLearning Curriculum*. The form also includes terms relating to access, use and disclosure of PHI during the individual's employment or affiliation with CCO. All CCO employees, as well as consultants, students, volunteers, researchers and others with access to CCO systems, must complete the *Core Privacy & Security Training eLearning Curriculum* and accept the Privacy and Security Acknowledgement form prior to receiving access to PHI at CCO. The following components are included in the *Core Privacy & Security Training Curriculum*:

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

(c) Annual Privacy and Security Refresher Training eLearning Curriculum

The Annual Privacy & Security Refresher Training eLearning Curriculum provides a mandatory refresher training module for all CCO employees, as well as service providers with access to PHI, students, researchers and others with access to CCO systems, on their privacy and security obligations. It also provides an update on relevant privacy and security current events and any CCO PAO and EISO initiatives launched that year. Users are required to read and digitally accept a Privacy and Security Acknowledgement form upon completion of the training. Those who do not comply with this training requirement by the stated due date have their CCO system access revoked. The PAO tracks and reports on the training completion status for this curriculum.

(vii) Breach management

Another important component of the Privacy Assurance & Risk Management service is the identification, management and resolution of privacy breaches that occur as a result of the misuse or improper/unauthorized collection, use, retention, disclosure or disposal of PHI in CCO's custody or control. CCO policies stipulate that it is mandatory for employees, and third parties working under contract with CCO, to report all privacy breaches or suspected privacy breaches to the PAO. Employees and third parties are

trained on what constitutes a privacy breach through CCO's privacy and security training program and they are made aware of each individual's responsibility for reporting a breach or suspected breach.

Additionally, the CCO *Privacy Breach Management Procedure* was amended in 2011, expanding on the definition of a privacy breach, to include definitions on what constitutes a suspected privacy breach or a privacy risk. The procedure was amended in response to PHIPA Order HO-011 (**HO-011**), which was issued by the IPC on October 13, 2011. In particular, the Order required CCO to review its *Privacy Breach Management Procedure* "to clarify and ensure that those having an employment, contractual or other relationship with CCO are fully aware of their responsibility to immediately report any privacy breaches, suspected privacy breaches and/or privacy risks to appropriate individuals at CCO with responsibility for privacy issues". CCO provided the IPC with a copy of the amended procedure. In February 2012, the IPC confirmed that CCO had complied with the requirements of HO-011.

(viii) Vendor management

The PAO is engaged in the procurement process for every requested procurement that may involve the use or disclosure of PHI or PI. Embedded within the eProcurement Tool, the Procurement Privacy and Security Intake form must be completed, along with a Procurement PIA, prior to the business unit receiving approval and moving forward with their requested procurement. Where PHI or PI will be used or disclosed, a Privacy Manager will work with the requesting business unit to ensure that appropriate controls are in place through a variety of mechanisms, including specific privacy requirements for vendors within the Request For Proposals (**RFP**), involvement in the selection of vendors, privacy and security training of vendors, and the signing of confidentiality agreements.

(ix) External communication & transparency

All of the privacy content on CCO's external website is in the process of being updated. This update will be completed prior to October 31, 2014. CCO maintains the following documents on its public website:

- CCO's *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario* (i.e., CCO's Privacy Policy)
- Frequently Asked Questions related to its privacy policies, procedures and practices
- A list of the data holdings of PHI that CCO maintains
- CCO's *Statement of Information Practices*
- Contact information for the PAO for inquiries
- Information about the CCO's approval status based on the IPC triennial review and the contact information for the IPC
- Program-specific privacy information, where necessary to clarify privacy practices related to a specific initiative
- *Annual Privacy Reports*

(x) Privacy and Security risk management

CCO's *Privacy and Information Security Risk Management Framework* defines the approach by which CCO identifies, assesses, responds to and monitors Privacy and Security Risks. The Framework establishes a foundation for mitigating and managing Privacy and Security Risks and sets the boundaries for risk-based decisions in respect of privacy and security within CCO. The Framework is designed to assist CCO Business Units in meeting their obligations under CCO's *Enterprise Risk Management Framework* through the proper identification, assessment and treatment of Privacy and Security Risks.

Together, the *Enterprise Risk Management Framework* and the *Privacy and Information Security Risk Management Framework* provide CCO with a comprehensive process to (i) manage Privacy and Security Risk and (ii) document the roles and responsibilities of CCO Staff, Management and Board Members in identifying, assessing, mitigating (to the extent possible) and monitoring Privacy and Security Risks.

When the *Privacy and Information Security Risk Management* Framework is fully implemented (estimated to occur by November 2014), the assessment of privacy risk will be embedded in each of the PAO and EISO deliverables and centralized in a privacy and security risk register. Efforts are currently underway to harmonize the risk management practices of the PAO, the EISO and the Informatics Centre of Excellence to ensure consistency of both risk reporting and risk management.

(xi) Monitoring and reporting, including an annual Privacy Management, Oversight and Review Plan and the Annual Privacy Report

At the conclusion of each calendar year, the PAO produces an Annual Privacy Report, which is presented to the ET and the Board. It is also shared with the MOHLTC and the IPC. The purpose of this report is to describe CCO's Privacy Program and highlight the privacy milestones for the current year. The Annual Privacy Report concludes with a summary of the key privacy initiatives for the next year. Contributions from CCO's Informatics Department and EISO are critical to the CCO Privacy Program and are acknowledged within relevant sections of this Report.

The Privacy Management, Oversight and Review Plan was first implemented for the 2013/14 fiscal year. Intended to be developed annually by the Director, Privacy & Access, the Privacy Management, Oversight and Review Plan sets out the tactics for the review and improvement of the CCO privacy management program. This Plan complements and operationalizes both the initiatives outlined in the Annual Privacy Report, as well as CCO's *Privacy Audit and Compliance Policy*. This Plan is submitted to the CPO for approval, support and the funding necessary to permit the privacy program to be successful.

The Plan includes:

(i) A schedule of when privacy policies and program controls will be reviewed

(ii) The privacy and security training awareness plan for the year

(iii) Any scheduled program and initiative reviews,

(iv) Any scheduled enterprise review (i.e. the IPC Triennial Review),

(v) Steps to be taken to ensure monitoring of the program includes:

a) Whether program controls are addressing latest threats and risks

b) Whether program controls are addressing the latest orders, recommendations and guidance from the IPC as well as recommendations arising from any breach, audit, privacy impact or other risk assessment, or new industry-standard best practices.

c) Whether new processes involve personal information

d) Whether training is occurring and if it is effective

e) Whether policies and procedures are being followed

f) Key privacy processes are being followed

STATUS OF THE CCO 2011 PRESCRIBED ENTITY AND REGISTRY TRIENNIAL REVIEW RECOMMENDATIONS

The IPC's 2011 triennial review of CCO's practices and procedures resulted in 6 recommendations, one that applied solely to CCO's role as a Prescribed Person, and the other 5 that applied to CCO as both a Prescribed Entity and Prescribed Person. 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.

Status of 2011 IPC Recommendations

2011 IPC Compliance Recommendation	CCO Enhancement	Status		Expected Date of Completion
		Complete	In Progress	
Prescribed Entity and Prescribed Person				
1. Review the *Privacy Breach Management Procedure* and any related policies and procedures to clarify and ensure that those having an employment, contractual or other relationship with CCO are fully aware of their responsibility to immediately report any privacy breaches, suspected privacy breaches and/or privacy risks to appropriate individuals at CCO with responsibility for privacy issues and provide the Information and Privacy Commissioner of Ontario with proof of compliance by January 13, 2012.	CCO's *Privacy Breach Management Procedure* was amended in response to HO-011, which was issued by the IPC on October 13, 2011. CCO provided the IPC with a copy of the amended procedure. On February 8, 2012, the IPC confirmed that CCO had complied with the requirements of HO-011.	✓		
2. Conduct additional training with those having an employment, contractual or other relationship with CCO to ensure that they	CCO has incorporated additional training into its established process of providing	✓		

are fully aware of their duties and responsibilities under the Privacy Breach Management Procedure and provide the Information and Privacy Commissioner of Ontario with proof of compliance by January 13, 2012.	mandatory privacy refresher training to all CCO staff on an annual basis. The additional privacy refresher training specifically addresses the issues identified by the IPC. On February 8, 2012, the IPC confirmed that CCO had complied with this requirement.			
3. Develop and implement a policy and procedures for the secure transfer of records of personal health information in a manner consistent with the Manual and Order HO-011, by April 1, 2012 and report to the Information and Privacy Commissioner of Ontario on the practices and procedures it is contemplating implementing, on or before February 1, 2012 and, in any event, prior to implementation.	CCO has developed and implemented a comprehensive policy suite for the secure transfer of records of PHI: *- Secure Transfer of Personal Health Information Policy* *- Secure Transfer of Personal Health Information Standard* *- Courier Transfer of Personal Health Information Procedure* *- Exchanging Personal Health Information via Application Services Procedure* *- Exchanging Encrypted Personal Health Information on Digital Media* *- Exchanging Personal Health Information via Secure Managed File Transfer Procedure* *- Fax Transmission of Personal Health Information Procedure* *- In Person Transfer of Personal Health Information Procedure* *- Transfer of Personal Health Information by Regular Mail Procedure* The Policy and Standard were submitted to the IPC on June 19, 2012. In a letter from the IPC dated July 18, 2012 the IPC stated that it had completed its review of the draft Policy and Standard and had no comments at that time.	✓		

4. Develop and implement a policy and procedures for the secure retention of records of personal health information on mobile devices in accordance with the requirements of the Manual.	CCO has developed and is in the process of implementing a standard and procedure, in accordance with the requirements of the Manual, for the handling of PHI inclusive of the secure retention of records of PHI on mobile devices. - *PHI Handling Standard* - *PHI Handling Procedure*	✓		
5. Develop and implement a comprehensive and integrated corporate risk management framework in accordance with the requirements of the Manual.	CCO has developed and is in the process of implementing a comprehensive and integrated risk management framework: *- Privacy and Information Security Risk Management Framework* *-Privacy Risk Register* *- Security Risk Management Standard* *- Security Risk Register* *- Enterprise Risk Management Framework, including risk tolerance statements* *- Enterprise Risk Register*	✓		
Prescribed Person Only				
6. Provide a full report to the Information and Privacy Commissioner of Ontario on the advantages and disadvantages of transferring screening reports in electronic format via the OntarioMD web portal, as compared to the proposed CCO web portal. This report is to include a complete assessment of the security and privacy protective measures that will be built into the architecture of the proposed CCO web portal. It should also contain a comparison of those measures against the existing and potentially enhanced security	For primary care physicians who had not yet registered for eHealth Ontario's ONE ID service, CCO's proposed alternative methods of transfer were outlined in a letter to the IPC dated June 26, 2012. In a letter dated June 28, 2012, the IPC indicated its support for these proposed alternative methods of transfer. In a letter dated July 3, 2012, Assistant Commissioner Brian Beamish indicated that, in accordance with provision 2 of Order HO-11, CCO could resume the transfer of the	✓		

and privacy measures of the OntarioMD web portal. CCO must obtain the approval of the Information and Privacy Commissioner of Ontario prior to resuming the transfer of screening reports to primary care physicians.	Screening activity Reports to primary care physicians.			

CCO 2014 PRESCRIBED ENTITY AND PRESCRIBED PERSON 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 processes to be followed when reviewing the practices and procedures used by Prescribed Entities and Prescribed Registries, such as CCO, to protect the privacy of individuals and to maintain the confidentiality of the PHI received by the Prescribed Entity and Prescribed Person.

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

The PAO undertook the review of CCO's procedures and practices along with other supporting departments. The PAO added further detail to the comprehensive reference checklist that it had created in 2008 based on the full requirements outlined in the Manual for the purposes of creating a tracking mechanism for each requirement. Process improvements, organizational changes, and technological upgrades had changed some of CCO's practices and resulted in new policies and procedures. Accordingly, CCO chose to complete the 2014 review from a blank checklist newly assessing each requirement on its merits. 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 PAO 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 could more explicitly meet a requirement, minor amendments were made or new documents were developed.

iv. *Report drafting* – The final CCO 2014 Prescribed Entity and Prescribed Person Triennial Review Report was drafted and finalized, after all of the requirements were reviewed and responded to.

The structure of the CCO 2014 Prescribed Entity Prescribed Person Triennial Review Report follows the *List of Required Documentation* provided in Appendix "A" of the Manual. The Report

is presented in a table format, wherein each required document listed in Appendix “A” is organized in a separate table. It is recommended that this report be reviewed along with the Manual, as requirements have not been duplicated verbatim in this report.

As noted in the Manual, each requirement includes a minimum set of criteria or content, as provided in Appendix “B” of the Manual. CCO complies fully with every applicable requirement, and all documents which meet the criteria of that requirement are listed. 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 GOVERNANCE FRAMEWORK

Since the last review, CCO undertook to document the essential governance elements of its privacy program and, in 2013, implemented a new Privacy Governance Framework. The Framework is designed to give enhanced effect to CCO's *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario* (CCO's Privacy Policy) and, more generally, to its commitment to privacy. The Framework contains, in a single document, all core elements of the CCO privacy program, many of which are set out, above, under the heading CCO's Privacy Program. The Framework enables the effective integration and coordination of CCO's PAO, policies, and programs with the organization as a whole.

The Privacy Governance Framework sets out the privacy governance structure at CCO, as well as the operational governance structure, outlining all of the core program controls. Finally, it outlines how CCO conducts ongoing monitoring and reporting and mandates an Annual Privacy Management, Oversight and Review Plan and Annual Privacy Report.

CCO has recently undergone an Executive-Level re-organization, so parts of this structure may change over the coming year.

CCO'S PRIVACY POLICY FRAMEWORK

The ability of the PAO to fulfill its commitment to respecting personal privacy, safeguarding confidential information, and ensure the security of PHI within its custody or control, is supported by EISO and the Human Resources, Facilities, Legal and Procurement departments within CCO. This Privacy Policy Framework (**Figure 1**) demonstrates this interconnectivity 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 PAO works towards fulfilling its commitment.

The Privacy Policy 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 provide additional detail or context with the aim to streamline a particular process.

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

Cancer Care Ontario – Privacy Policy Framework (PE)				
Privacy/Informatics	*Information Security*	*Technical Services*	*Human Resources*	*Corporate, Legal, Procurement, Facilities*
Policies				
▪ *IM/IT Stage – Gating Policy* ▪ *Internal Data Access Policy* ▪ *Policy on Retention of Records Containing PHI* ▪ *Principles and Policies for the Protection of PHI at CCO (CCO's Privacy Policy)* ▪ *Privacy Governance Framework* ▪ *Privacy and Information Security Risk Management Framework* ▪ ▪ *Secure Transfer of PHI Policy* ▪ *Data Linkage Policy* (Informatics)	▪ *Acceptable Use of Social Media Policy* ▪ *Information Security Policy* ▪ *Incident Management Framework* ▪ *Information Security Code of Conduct and Acceptable Use* ▪ *Information Security Framework*	▪ *Business Continuity Services Framework* ▪ *Change Management Policy* ▪ *Data Backup Policy* ▪ *Data Center Access an Usage Policy* ▪ *Mobile Devices and Pager Policy*	▪ *Code of Conduct* ▪ *Confidentiality Policy* ▪ *Progressive Discipline Policy* ▪ *Secondment Policy* ▪ *Termination of Employment Policy* ▪ *Unpaid Student Intern Policy*	▪ *Access Card Procedure* (Facilities) ▪ *Enterprise Risk Management Framework* (Legal) ▪ *Physical Security Policy* (Facilities)
Standards				
▪ *CSP Privacy Breach Management Standard Operating Procedure* ▪ *Data Sharing Agreement Standard* ▪ *Data Use & Disclosure Standard* ▪ *Privacy Audit and Review Standard* ▪ *Privacy Impact Assessment Standard* ▪ *Secure Transfer of PHI Standard*	▪ *Acquisition Development and Application Security Standard* ▪ *Cryptography Standard* ▪ *Digital Media Destruction Standard* ▪ *Information Security Incident and Breach Response Standard* ▪ *Logging, Monitoring and Auditing Standard* ▪ *Logical Access Control Standard* ▪ *Security Audit, Testing and Compliance Standard* ▪ *Security Risk Management Standards*	▪ *Operational Security Standard* ▪ *PHI Handling Standard* ▪ *Mobile Devices and Pager Standard*	▪ *Statement of Confidentiality* (Legal)	▪ *Services Agreement – Template Schedule for Third Party Agreements* (Legal) ▪ *Statement of Confidentiality* (Legal) ▪ *Video Monitoring Standard* (Facilities)

Procedures				
▪ *Business Process for Data Requests* ▪ *Courier Transfer of Personal Health Information Procedure* ▪ *Data Sharing Agreement Procedure* ▪ *Decision Criteria for Data Requests* ▪ *Direct Data Access Audit Procedure* ▪ *Exchanging PHI via Application Services Procedure* ▪ *Exchange PHI via Secure Managed File Transfer Procedure* ▪ *Fax Transmission of PHI Procedure* ▪ *IM/IT Stage – Gating Process and Project Lifecycle Methodology* ▪ *In Person Transfer of PHI Procedure* ▪ *Internal Data Access Procedure* ▪ *Privacy and Security Training and Awareness Procedure* ▪ *Data Linkage Procedure* (Informatics) ▪ *Privacy Breach Management Procedure* ▪ *Privacy Inquiries and Complaints Procedure* ▪ *Transfer of PHI by Regular Mail Procedure*	▪ *Digital Media Destruction Procedure* ▪ *Logging, Monitoring and Auditing Procedure*	▪ *Business Continuity Plan* ▪ *Change Management Process (Standard Change)* ▪ *Acceptable Use of Social Medial Policy* ▪ *Data Backup Procedure* ▪ *Disaster Recovery Plan* ▪ *Existing Employee Data Management* ▪ *Operational Security Procedure: Patching* ▪ *PHI Handling Procedure*	▪ *Employee Exit Checklist*	▪ *Hard Copy PHI Disposal Procedure* (Facilities) ▪ *Visitor Access Procedure* (Facilities)
Guidelines				
▪ *De-identification Guidelines* ▪ *Data Sharing Agreement Template*	▪ *Threat Risk Assessment Template*	▪ *IT Change Control Process Instructions*		

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 of Information from CCO for Research Purposes													x	x																			
Business Process for Data Requests												x	x											x									
Consulting Agreement																				x													
Contract Management System																					x												
CSP Privacy Breach Management Standard Operating Procedure						x							x									x		x	x				x	x	x		x
CSP Privacy FAQs			x																														
Data Access Committee Terms of Reference													x																				
Data Linkage Policy (Draft)																						x											
Data Linkage Procedure (Draft)																						x											
Data Sharing Agreement Initiation Form																	x																
Data Sharing Agreement Procedure				x								x				x	x	x											x				
Data Sharing Agreement Standard				x								x				x	x																
Data Sharing Agreement Summary Chart																		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
Data Sharing Agreement Template				**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 (Under Revision)	**x**											**x**	**x**											**x**									
Digital Media Disposal Procedure	**x**							**x**				**x**																					
Digital Media Disposal Standard	**x**							**x**				**x**																					
Direct Data Access Audit Procedure								**x**																									
eCCO Data Access Request Tool (Log of Access Requests)									**x**						**x**																		
Employee Exit Checklist								**x**																									
Employee Exit Process								**x**																									
Enterprise Information Security Policy	**x**																																
Exiting Employee Data Management								**x**																									
IM/IT Stage – Gating Policy				**x**																													
Internal Data Access Request Form									**x**																								
Internal Data Access Policy								**x**																									
Internal Data Access Procedure								**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
List of Data Linkages																							**x**										
Log of Privacy Breaches																													**x**				
Log of Privacy Impact Assessments																									**x**	**x**							
Log of Privacy Inquiries and Complaints																																**x**	
Log of Third Party Service Providers with Access to PHI																					**x**												
Logging, Monitoring and Auditing Standard		**x**																									**x**						
Non-disclosure/Confidentiality Agreement													**x**	**x**																			
PHI Handling Procedure	**x**																							**x**									
PHI Handling Standard	**x**																		**x**					**x**									
Physical Security Policy	**x**							**x**																									
Principles and Policies for the Protection of PHI at CCO (CCO's Privacy Policy)	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**								**x**	**x**	**x**	**x**					**x**	**x**		**x**		**x**	**x**	**x**	**x**	**x**
Privacy & Security Acknowledgement Form																								**x**									
Privacy Audit and Review Standard		**x**		**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**		**x**
Privacy Breach Report Form																												**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 FAQs			**x**																														
Privacy Governance Framework	**x**					**x**																											
Privacy Impact Assessment Standard																									**x**								
Privacy Inquiries and Complaints Procedures	**x**		**x**																												**x**	**x**	**x**
Privacy and Information Security Risk Management Framework	**x**			**x**																													
Privacy Risk Register																											**x**						
Procurement Documentation and Records Management Procedure																			**x**														
Procurement of Goods and Services Policy																			**x**														
Services Agreement – Template Schedule for Third Party Agreements																				**x**													
Statement of Information Practices	**x**		**x**																														
Template Schedule for Third Party Agreements																			**x**														

IPC Requirements

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

CCO is committed to respecting personal privacy, safeguarding confidential information and ensuring the security of PHI within its custody. A key component of CCO's Privacy Program is its *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario* (CCO's *Privacy Policy*), which is supported by related policies and procedures that provide additional information on the Privacy Principles in the CCO context and how it is operationalized.

Since the last triennial review, CCO has also implemented a formalized Privacy Governance Framework. The Privacy Governance Framework is the second key component of CCO's Privacy Program. The Privacy Governance Framework is designed to give effect to CCO's *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario* (CCO's *Privacy Policy*), and, more generally, to its commitment to privacy. The Privacy Governance Framework enables the effective integration and coordination of CCO's PAO, policies, and programs with the organization as a whole.

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 (CCO's Privacy Policy)*, PAO
2. *Privacy Governance Framework,* PAO
3. *Data Use & Disclosure Standard,* PAO and Chief Information Officer (**CIO**)
4. *Decision Criteria for Data Requests,* CIO
5. *Statement of Information Practices*, PAO
6. *Privacy Inquiries and Complaints Procedure*, PAO
7. *De-identification Guidelines (Under Revision)*, PAO and CIO
8. *Information Security Policy,* EISO
9. *PHI Handling Standard and Procedure,* EISO
10. *Digital Media Destruction Standard,* EISO
11. *Digital Media Destruction Procedure*, EISO
12. *Privacy and Information Security Risk Management Framework,* PAO & EISO
13. *Physical Security Policy,* Facilities

✓	**All requirements for this section have been met.**

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

CCO's Privacy Governance Framework requires the creation of an annual Privacy Management, Oversight, and Review plan. The plan includes

(i) A schedule of when privacy policies and program controls will be reviewed
(ii) The privacy and security training awareness plan for the year
(iii) Any scheduled program and initiative reviews,
(iv) Any scheduled enterprise review (i.e. IPC Triennial Review),
(v) Steps to be taken to ensure monitoring of the program includes:
    a. Whether program controls are addressing latest threats and risks
    b. Whether program controls are addressing the latest orders, recommendations and guidance from the IPC as well as recommendations arising from any breach, audit, privacy impact or other risk assessment, or new industry-standard best practices.
    c. Whether new processes involve personal information
    d. Whether training is occurring and if it is effective
    e. Whether policies and procedures are being followed
    f. Key privacy processes are being followed

Since the last triennial review, CCO has revised its *Privacy Audit and Review Standard* to establish a more rigorous program for the review of policies and procedures as well as the auditing of compliance.

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 (CCO's Privacy Policy)*, PAO

2. *Privacy Audit and Review Standard,* PAO

3. *Logging, Monitoring and Auditing Standard and Procedure*, EISO

✓	**All requirements for this section have been met.**

Privacy: IPC Requirement 3: 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, 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Inquiries and Complaints Procedure*, PAO
3. *Statement of Information Practices*, PAO
4. *Privacy FAQs*, PAO
5. *Annual Privacy Report,* PAO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

6. *CSP Privacy FAQs,* PAO

All requirements for this section 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Audit and Review Standard*, PAO
3. *Privacy Breach Management Procedure,* PAO
4. *Data Sharing Agreement Standard,* PAO
5. *Data Sharing Agreement Initiation Procedure*, PAO
6. *Data Sharing Agreement Template*, PAO
7. *IM/IT Stage – Gating Policy,* CIO
8. *Privacy and Information Security Risk Management Framework,* PAO & EISO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

10. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

	**All requirements for this section have been met.**

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

CCO maintains a central, online repository which describes all CCO data holdings, both PHI and non-PHI. This repository is currently for internal use only, with plans to provide limited access to the public. The Data Catalogue provides a single location for obtaining information about CCO data, including associated programs and subjects, data start and end dates.

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

1. *Data Catalogue*, CCO's Intranet (**eCCO**), Informatics

	**All requirements for this section 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Breach Management Procedure*, PAO
3. *Privacy Audit and Review Standard,* PAO
4. *Privacy Governance Framework,* PAO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

5. *CSP Privacy Breach Management Standard Operating Procedure, PAO*

	**All requirements for this section 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 document outlines CCO's compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)*, PAO

All requirements for this section have been met.

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

CCO ensures that access to PHI by its employees is strictly limited in accordance with the "need to know" principle, whereby 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 (CCO's Privacy Policy),* PAO
2. *Data Use and Disclosure Standard,* PAO and CIO
3. *Internal Data Access Policy,* PAO and CIO
4. *Internal Data Access Procedure*, PAO and CIO
5. *Direct Data Access Audit Procedure*, PAO and CIO
6. *Digital Media Destruction Standard,* EISO
7. *Digital Media Destruction Procedure*, EISO
8. *Employee Exit Process, Human Resources*
9. *Employee Exit Checklist, Human Resources*
10. *Exiting Employee Data Management,* Technology Services
11. *Privacy Audit and Review Standard, PAO*
12. *Privacy Breach Management Procedure, PAO*
13. *Physical Security Policy,* Facilities

14. *Log of Access Requests on the eCCO Data Access Request Tool* (*i.e.*, the log of agents granted approval to access and use PHI), Informatics

✓	**All requirements for this section have been met.**

Privacy: IPC Requirement 9: Log of agents granted approval to access and use 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 Internal Data Access Request (**IDAR**) tool logs internal uses and access to PHI (non-research).

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

1. *Internal Data Access Request Form*, Informatics
2. *Log of Access Requests on the eCCO Data Access Request Tool*, Informatics

✓	**All requirements for this section have been met.**

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

All research, as defined in PHIPA, undertaken through 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.

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.*

All research requests for PHI must be accompanied by Research Ethics Board (**REB**) approval; a research plan; and an Application for Disclosure of 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. The DAC Working Group reviews all research requests for access to PHI. Requests are either approved or denied by the DAC, which is co-chaired by the CPO. The Application for Disclosure of Information from CCO for Research Purposes, along with the CCO Non-disclosure/Confidentiality Agreement forms the agreement between CCO and a researcher.

This requirement is not applicable to CCO.

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 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.

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

This requirement is not applicable to CCO.

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, are in accordance with PHIPA, its regulation and CCO's *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario* (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,* PAO
2. *Business Process for Data Requests,* CIO
3. *De-Identification Guidelines (Under Revision)*, PAO and CIO
4. *Data Sharing Agreement Template,* PAO
5. *Data Sharing Agreement Initiation Procedure,* PAO
6. *Data Sharing Agreement Standard, PAO*
7. *Decision Criteria for Data Requests,* CIO
8. *Digital Media Destruction Standard,* EISO
9. *Digital Media Destruction Procedure*, EISO
10. *Privacy Audit and Review Standard*, PAO

	**All requirements for this section 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 an REB approval, a research plan, and an Application for Disclosure for Information from CCO for Research Purposes, which sets out the terms and conditions that a researcher must abide by when using the PHI disclosed by CCO for research purposes. The DAC Working Group reviews all research requests for access to PHI. Requests are either approved or denied by the DAC, which is chaired by the

CPO. The Application for Disclosure for Information from CCO for Research Purposes, 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,* PAO 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,* Legal and CIO
5. *Decision Criteria for Data Requests,* CIO
6. *Data Access Committee Terms of Reference,* CIO
7. *Privacy Breach Management Procedure*, PAO
8. *Privacy Audit and Review Standard*, PAO
9. *De-Identification Guidelines (Under Revision),* PAO and CIO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

10. *CSP Privacy Breach Management Standard Operating Procedure,* PAO

	**All requirements for this section 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,* Legal and CIO
3. *eCCO Data Request Tool Log* (*i.e.*, the Log of research agreements), CIO

	**All requirements for this section have been met.**

Privacy: IPC Requirement 15: Log of research agreements.

The eCCO Data Request Tool maintains a log of executed Research Agreements between CCO and all researchers.

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

1. *eCCO Data Request Tool Log*, CIO

✓	**All requirements for this section 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 (CCO's Privacy Policy)*, PAO
2. *Data Sharing Agreement Standard*, PAO
3. *Data Sharing Agreement Initiation Procedure*, PAO
4. *Privacy Audit and Review Standard*, PAO

✓	**All requirements for this section have been met.**

Privacy: IPC Requirement 17: Template data sharing agreements.

The CCO template data sharing agreements specify the terms and conditions to be adhered to for 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 (CCO's Privacy Policy)*, PAO
2. *Data Sharing Agreement Template*, PAO
3. *Data Sharing Agreement Standard*, PAO

4. *Data Sharing Agreement Initiation Procedure*, PAO
5. *Data Sharing Agreement Initiation Form,* PAO

	**All requirements for this section have been met.**

Privacy: IPC Requirement 18: Log of data sharing agreements (**DSAs**).

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 (CCO's Privacy Policy)*, PAO
2. *Data Sharing Agreement Initiation Procedure*, PAO
3. *Log of Data Sharing Agreements,* PAO

	**All requirements for this section 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 (CCO's Privacy Policy)*, PAO
2. *Data Use and Disclosure Standard*, PAO and CIO
3. *Privacy Audit and Review Standard*, PAO
4. *Procurement Documentation and Records Management Procedure*, Procurement Office
5. *Procurement of Goods and Services Policy*, Procurement Office
6. *Privacy Breach Management Procedure*, PAO
7. *Template Schedule for Third Party Agreements,* Legal Department
8. *PHI Handling* Standard and Policy, EISO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

9. *CSP Breach Management Procedure*, PAO

✓	**All requirements for this section 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 documents outline CCO's compliance with this requirement:

1. *Services Agreement- Template Schedule for Third Party Agreements,* Legal Department
2. *Consulting Agreement – Template,* Legal Department

✓	**All requirements for this section 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 documents outline CCO's compliance with this requirement:

1. *Contract Management System*, Procurement Office
2. *Log of Third Party Service Providers with Access to PHI,* PAO

✓	**All requirements for this section 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 Policy (Draft),* CIO
2. *Data Linkage Procedure (Draft),* CIO
3. *Privacy Breach Management Procedure*, PAO
4. *Privacy Audit and Review Standard*, PAO
5. *List of Data Linkages* (*i.e.*, the Log of approved linkages of records of PHI)*,* Informatics

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

6. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

	**All requirements for this section 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,* Informatics

	**All requirements for this section 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.

CCO is in the process of acquiring a de-identification tool in order to facilitate the de-identification of PHI. A new policy suite and de-identification guidelines will accompany the enterprise-wide implementation of the tool which is planned for fiscal year 2015/16.

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 (CCO's Privacy Policy)*, PAO

2. *Data Use & Disclosure Standard,* PAO and CIO
3. *De-Identification Guidelines (Under Revision),* PAO and CIO
4. *Business Process for Data Requests,* CIO
5. *Privacy & Security Acknowledgment Form,* PAO
6. *Decision Criteria for Data Requests,* CIO
7. *Privacy Audit and Review Standard*, PAO
8. *Privacy Breach Management Procedure*, PAO
9. *PHI Handling Standard and Procedure, EISO*

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

10. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

	**All requirements for this section have been met.**

Privacy: IPC Requirement 25: PIA policy and procedures.

CCO has policies in place to identify the circumstances in which PIAs 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Impact Assessment Standard*, PAO
3. *Log of Privacy Impact Assessments*, PAO
4. *Privacy Audit and Review Standard*, PAO
5. *Privacy Breach Management Procedure*, PAO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

6. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

	**All requirements for this section 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 document outlines CCO's compliance with this requirement:

1. *Log of Privacy Impact Assessments*, PAO

	**All requirements for this section 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Audit and Review Standard*, PAO
3. *Logging, Monitoring and Auditing Standard and Procedure,* EISO
4. *Privacy Risk Register* (*i.e.*, the Log of privacy audits), PAO

	**All requirements for this section 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 document outlines CCO's compliance with this requirement:

1. *Privacy Risk Register*, PAO

	**All requirements for this section 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 *Privacy Breach Management Procedure* clearly defines the identification, reporting, containment, notification, investigation and remediation processes to be followed when a privacy breach or suspected privacy breach has occurred.

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

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)*, PAO
2. *Privacy Breach Management Procedure*, PAO
3. *Privacy Audit and Review Standard*, PAO
4. *Data Sharing Agreements Procedure*, PAO
5. *Privacy Breach Report Form*, PAO
6. *Log of Privacy Breaches*, PAO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

7. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

✓	**All requirements for this section 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Breach Management Procedure*, PAO
3. *Log of Privacy Breaches*, PAO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

4. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

✓	**All requirements for this section 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Inquiries and Complaints Procedure*, PAO
3. *Privacy Breach Management Procedure*, PAO
4. *Privacy Audit and Review Standard*, PAO
5. *Log of Privacy Inquiries and Complaints*, PAO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

6. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

✓	**All requirements for this section have been met.**

Privacy: IPC Requirement 32: 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Inquiries and Complaints Procedure*, PAO
3. *Log of Privacy Inquiries and Complaints*, PAO

✓	**All requirements for this section have been met.**

Privacy: IPC Requirement 33: 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 (CCO's Privacy Policy)*, PAO
2. *Privacy Inquiries and Complaints Procedure*, PAO
3. *Privacy Breach Management Procedure*, PAO
4. *Privacy Audit and Review Standard*, PAO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

5. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

	**All requirements for this section have been met.**

PART 2: CCO'S INFORMATION SECURITY PROGRAM

CCO operates digital services within a rapidly changing environment. This environment presents a number of risks, from both internal and external threat sources. CCO's Enterprise Information Security Program (**EISP**) represents a structured approach for managing these risks in a manner that delivers value to CCO's core business. This business value statement includes the protection of information and information technology assets, reduction of risk event impacts, support of compliance objectives, and enablement of new technologies

The following are the drivers for the EISP implementation at CCO.

Business Enablement

Information security is a business enabler. A strong and robust information security program enables the effective management of technology-related risks. The assurance derived from a sound information security program allows the business to take advantage of advances in technology and other information sharing mechanisms to grow the business through new business channels and partner interaction models.

Strategic Alignment

The information security program is driven by CCO's strategic objectives and business direction. This results in an enterprise security architecture based on a holistic approach to information protection focused on business requirements. The business-based approach provides the context for the information security program implementation and assures that the resulting security architecture aligns with CCO's business strategy

Risk Management

CCO follows a risk-based approach to information security. Any identified risks are weighed in relation to CCO's enterprise risk tolerance and managed in proportion to the assessed business impact and cost of mitigation. CCO's appetite and tolerances for information security risks are defined in consultation with the ET.

Operational Effectiveness

CCO strives for effectiveness in the management of information security. This means security services are delivered that protect CCO's assets, reduces risk, and add business value in a meaningful and measurable way. CCO demonstrates the capabilities to deliver on its security program and commitments through effective management and governance.

Compliance with Legal and Regulatory Requirements

CCO's information management practices are subject to regulatory oversight through privacy and access legislation such as PHIPA and FIPPA.

All policy, standard, process, procedure, and guideline documents in support of information security must take into account the relevant legislative and regulatory frameworks as well as the IPC guidelines, fact sheets, and good practices.

CCO also has compliance requirements stemming from financial audit obligations, obligations as a service provider, product certification process, insurance requirements, and through various agreements and contracts with partners. Together these form a significant driver for the implementation and operation of the information security program.

CCO'S INFORMATION SECURITY GOVERNANCE FRAMEWORK

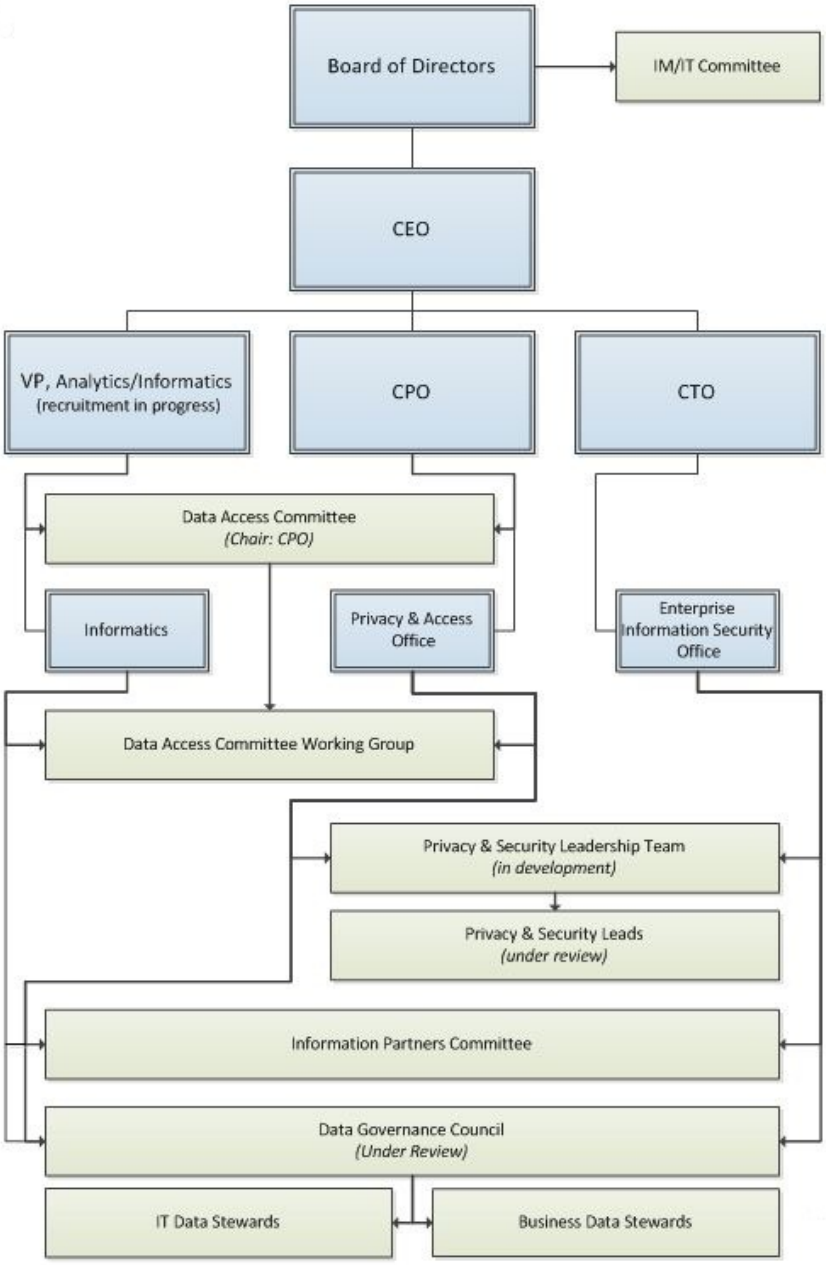
Information security governance ensures that CCO's information security program is aligned with and meets the strategic needs of CCO's business. This includes the establishment of processes that ensure that reasonable actions are taken to protect CCO's information resources, in the most effective and efficient manner, in pursuit of it business goals.

Implementation and management of the security program is accomplished through CCO's EISO. The EISO is responsible for working with CCO's various governance bodies and operational areas to ensure overall information protection is achieved in accordance with CCO's set objectives. The EISO works closely with partners within the PAO and CCO Informatics Center of Excellence.

Projects, operational teams, and program areas execute on the day-to-day security processes through a combination of cross functional roles throughout CCO.

The chart on the following page sets out the how both privacy and security management is organized at CCO, followed by more detail about key aspects of the organizational structure.

Privacy and Security Governance Structure*



*CCO's ET has completed a reorganization, which may result in changes to this structure.

The Board of Directors

CCO's Board of Directors holds accountability for security governance practices in support of CCO's mission. The Board receives a report on privacy related security matters annually, as a component of the Annual Privacy Report, as well as a more general information security status report through the newly established IM/IT Committee, of which Privacy is a full partner. This

new reporting structure will ensure security is reported on in full support of privacy to the same audience.

The ET

The CCO ET supports and champions the security program at CCO, actively advocating a culture of security. The Board receives a report on security matters annually and on an ad-hoc basis, as required. The Annual Privacy Report is delivered by CCO's CPO to the Board's IM/IT Committee and includes updates and key information about the Enterprise Information Security program.

The CPO (who is also CCO's General Counsel), provides the Board with relevant information on legal compliance matters, including privacy and security matters, any significant privacy or security breaches, privacy and security audit reports, new legislative, regulatory and industry developments of note, and the status of the IPC's triennial review and any recommendations arising therefrom. On an annual basis, the CPO also reports to the Board on privacy and security risks, through the Enterprise Risk Management Report, which is also provided to the MOHLTC as part of CCO's Annual Business Plan.

The Chief Technology Officer

Accountability for security compliance, in support of privacy and other compliance regimes, resides with CCO's President and CEO. This function has been formally delegated to CCO's Chief Technology Officer who is appointed by the CEO and reports directly to the CEO. The Chief Technology Officer provides security representation on the most senior decision-making bodies within CCO. The Chief Technology Officer has delegated the day-to-day operations of the security program to the Senior Manager, Information Security.

Senior Manager, Information Security

The Senior Manager, Information Security manages the Enterprise Information Security Office and reports directly to the Chief Technology Officer. The Senior Manager, Information Security is specifically responsible for:

(i) Managing the operations of the information security program;

(ii) Working with the Business Unit Managers and Information Technology in establishing, implementing, monitoring and assessing security program controls on an ongoing basis;

(iii) Providing security advice and support to all business functions;

(iv) Ensuring that the suite of security policies is comprehensive, up-to-date and compliant with applicable law and standards;

(v) Providing security training;

(vi) Advocating for security within the organization;

(vii) Conducting security reviews, audits/compliance monitoring, and benchmarking, as appropriate;

(viii) Ensuring that appropriate security aspects of procurement and vendor management are implemented;

(ix) Overseeing the operational security team with the effective operation of security controls; and

(x) Monitoring the threat environment and other developments in the information security arena.

The Enterprise Information Security Office

The EISO is led by the Senior Manager, Information Security and supported by Senior Information Security Specialists and an Information Security Architect.

The complete Organizational Structure for the EISO is provided within Appendix B.

The EISO has developed over time from a technology focused group embedded within the technical operations team to an enterprise focused information assurance function. The EISO is structured to enable CCO business through the effective management of technology-related risks and facilitating the safe adoption of new technologies. The program is aligned to applicable standards and industry best practices allowing for eventual certification.

The EISO has the following objectives:

- The effective protection of CCO information and information assets from harm.
- Create and nurture a culture of Information Security in all organizational areas of CCO.
- Implement and operate an information security risk management program that takes into account CCO executive risk tolerances and ensures safeguards are selected based on appropriate criteria.
- Develop and maintain Information Security shared services and enterprise information security architecture for reuse and cost-effectiveness.
- Achieve compliance to legal and regulatory requirements a result of an effective information security program.
- Contribute to improving CCO's effectiveness and efficiency by maturing information security practices.

The EISO meets these objectives through integration with CCO's business processes and close relationships with business and corporate partners such as the PAO and the Technology Service Operations team.

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	x														
Acquisition, Development and Application Security Standard	x																	
Application for Disclosure of Information from CCO for Research Purposes					x													
Authorization to Access Data Centre Contractor Form			x															
Authorization to Access Data Centre Employee Form			x															
Change Advisory Board Terms of Reference												x						
Change Management Policy												x						
Change Management Process												x						
Change Management: Change Calendar												x						
Change Management: Change Category and Type												x						
Change Management: Change Request Control Form												x						
Change Management: IT Change Control Process Instructions												x						
*Change Management: Request for Change (**RFC**)*												x						
Change Management: Request for Change Lead Time												x						
Standard Change Application Form												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
Courier Transfer of Personal Health Information Procedure							x											
Cryptography Standard						x	x											
CSP Privacy Breach Management Standard Operating Procedure					x													
Data Backup Policy	x				x								x					
Data Backup Procedure					x								x					
Data Center Access and Usage Policy			x															
Data Sharing Agreement Initiation Procedure					x													
Data Sharing Agreement Template					x													
Data Sharing Agreements Standard					x													
Data Use and Disclosure Standard					x													
De-identification Guidelines						x												
Digital Media Disposal Procedure								x										
Digital Media Disposal Standard								x										
Direct Data Access Procedure			x															
Disaster Recovery Plan													x					
EasyLobby Visitor Grid log				x														
Employee Exit Checklist			x															
Employee Exit Process			x															
Exchanging PHI on Digital Media							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
Exchanging PHI via Application Services Procedure							x											
Exchanging PHI via Secure Managed File Transfer Procedure							x											
Fax Transmission of PHI Procedure							x											
Hard Copy PHI Disposal Procedure								x										
HP Data Protectors Session Logs					x								x					
IM/IT Stage - Gating Process and Project Lifecycle Methodology	x																	
In Person Transfer of PHI Procedure							x											
Incident Management Framework	x									x							x	
Information Security Code of Conduct and Acceptable Use	x	x	x		x	x			x	x	x			x				
Information Security Framework	x	x													x	x		
Information Security Incident and Breach Response Standard	x																x	x
Information Security Policy	x	x	x		x	x	x	x	x	x	x	x	x	x	x		x	
Internal Data Access Procedure			x															
KeyScan System Log				x														
Log of Security Audits															x	x		
Log of Security Incidents							x											x
Log of Third Party Service Providers with Access to PHI					x													
Logging, Monitoring, and Auditing Procedure	x						x		x	x				x	x			

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Logging, Monitoring, and Auditing Standard	x	x					x		x	x				x	x			
Logical Access Control Standard	x		x			x	x		x									
Mobile Device and Pager Policy						x												
Mobile Device and Pager Procedure						x												
New Employee Facilities & Information Technology Services Form			x	x														
Non-Disclosure/Confidentiality Agreement					x													
Open Media Logs					x								x					
Operational Security Procedure: Patching											x							
Operational Security Standard			x								x		x		x	x		
Personal Action Form			x															
PHI Handling Procedure					x	x	x											
PHI Handling Standard					x	x	x											
Photo ID Request Form			x															
Physical Security Access Card Log				x														
Physical Security Policy			x					x										
Policy on Retention of Records Containing PHI					x								x					
Principles and Policies for the Protection of PHI at Cancer Care Ontario, (CCO's Privacy Policy)					x										x			
Privacy Audit and Review Standard			x	x	x		x											

CCO Security Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18
Privacy Breach Management Procedure			**x**		**x**													
Procurement Policy			**x**															
Secure Transfer of PHI Policy					**x**		**x**						**x**					
Secure Transfer of PHI Standard					**x**		**x**						**x**					
Security Audit, Testing, and Compliance Standard										**x**				**x**	**x**			
Security Risk Management Standard															**x**	**x**		
Security Risk Register																**x**		
Services Agreement - Template Schedule for Third Party Agreements					**x**			**x**					**x**					
Statement of Confidentiality			**x**				**x**											
Threat Risk Assessment Template															**x**			
Transfer of PHI by Regular Mail Procedure							**x**											
Video Monitoring Standard			**x**															
Visitor Access Procedure			**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 program is risk based and includes a credible audit and assurance element. The program supports the identification, implementation, and effective operation of a robust information security infrastructure through the Technology Services department.

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

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

	**All requirements for this section have been met.**

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

CCO has implemented an annual review process for the entire body of the security policy framework. Updates are done according to CCO corporate practices, with policy documents kept in a controlled document library on eCCO. The implementation of the security 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 and ensure effective operation.

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

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

All requirements for this section have been met.

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

In 2013, CCO drafted a new comprehensive Physical Security Policy. This policy is supported by certain other Facilities, Human Resources' and Information Technology Services' policies that are designed to protect PHI from theft, loss, or unauthorized use or access. 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. *Physical Security Policy,* Facilities
2. *Information Security Policy*, EISO
3. *Information Security Code of Conduct,* EISO
4. *Operational Security,* EISO/Technology Services
5. *Statement of Confidentiality,* Legal Department and Human Resources
6. *Privacy Breach Management,* PAO
7. *Logical Access Control,* EISO
8. *Internal Data Access Procedure,* PAO and CIO
9. *New Employee Facilities & Information Technology Services Form,* Facilities
10. *Photo ID Request Form,* Human Resources
11. *Authorization to Access Data Centre Employee Form*, Technology Services
12. *Authorization to Access Data Centre Contractor Form*, Technology Services
13. *Data Center Access and Usage Policy,* Technology Services
14. *Procurement Policy*, Procurement Office

15. *Employee Exit Checklist,* Human Resources
16. *Employee Exit Process ,* Human Resources
17. *Personnel Action Form (**PAF**) ,* Human Resources
18. *Visitor Access Procedure*, Facilities
19. *Video Monitoring Standard,* Facilities
20. *Privacy Audit and Review Standard*, PAO
21. *Access Card Procedure,* Facilities
22. *Physical Security Access Card Log,* Facilities
23. *EasyLobby Visitor Grid Log,* Facilities
24. *KeyScan System Log,* Facilities

All requirements for this section have been met.

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

CCO maintains a comprehensive log of all access 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 Technology Services.
2. *Physical Security Access Card Log,* Facilities
3. *Access Card Procedure,* Facilities
4. *EasyLobby Visitor Grid Log,* Facilities
5. *KeyScan System Log,* Facilities
6. *Privacy Audit and Review Standard,* PAO

All requirements for this section 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 Policy on Retention of Records Containing Personal Health Information, the Information Security Policy, the Information Security Code of Conduct, the PHI Handling Standard and Procedure, and appropriate agreements. Where records of PHI will be accessible, retained, or disposed of by a third party, CCO's Services Agreement, which contains robust privacy provisions in its Schedule for Third Party Agreements, ensures that all third parties secure and dispose of PHI in accordance with CCO's applicable retention periods.

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

1. *Policy on Retention of Records Containing Personal Health Information*, PAO
2. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)*, PAO
3. *Information Security Policy*, EISO
4. *Information Security Code of Conduct*, EISO
5. *Secure Transfer of Personal Health Information Policy,* PAO
6. *Secure Transfer of Personal Health Information Standard*, PAO
7. *Non-Disclosure/Confidentiality Agreement,* Legal and CIO
8. *Application for Disclosure of Information from CCO for Research Purposes,* CIO
9. *Data Sharing Agreement Template,* PAO
10. *Data Sharing Agreement Procedure,* PAO
11. *Data Sharing Agreement Standard,* PAO
12. *Data Use and Disclosure Standard,* PAO and CIO
13. *Privacy Audit and Review Standard,* PAO
14. *Privacy Breach Management Procedure,* PAO
15. *Data Back-up Policy*, Technology Services
16. *Data Back-up Procedure,* Technology Services
17. *PHI Handling Standard,* EISO
18. *PHI Handling Procedure*, EISO
19. *Open Media Logs*, Technology Services

20. *HP Data Protectors Session Logs*, Technology Services
21. *Services Agreement -Template Schedule for Third Party Agreements,* Legal Department
22. *Log of Third Party Service Providers with Access to PHI,* PAO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

23. *CSP Privacy Breach Management Standard Operating Procedure,* PAO

All requirements for this section have been met.

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

CCO has implemented a PHI Handling Standard and Procedure that specifically includes the policy requirements, as defined in the Manual, for ensuring the protection of PHI records retained on mobile devices. The Standard and Procedure also address the retention of PHI on external storage media and use of PHI in non-production environments, ensuring consistency in application of the Manual's decision criteria regarding PHI use.

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

1. *Information Security Policy,* EISO
2. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
3. *Logical Access Control Standard,* EISO
4. *Cryptography Standard,* EISO
5. *Mobile Device And Pager Policy,* Technology Services
6. *Mobile Device And Pager Procedure,* Technology Services
7. *PHI Handling Standard,* EISO
8. *PHI Handling Procedure*, EISO
9. *De-identification Guidelines* (Under Revision), PAO

All requirements for this section have been met.

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

The security requirements for the secure transfer of PHI are set out in CCO's Secure Transfer of Personal Health Information Standard. CCO has documented standards for the use of

cryptographic technologies and logical access controls. External parties' secure transfer obligations are managed through Data Sharing Agreements and other third party service provider agreements, all in accordance with CCO's Secure Transfer of Personal Health Information Standard. 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. *Secure Transfer of Personal Health Information Policy,* PAO
2. *Secure Transfer of Personal Health Information Standard*, PAO
3. *Courier Transfer of Personal Health Information Procedure*, PAO
4. *Exchanging Personal Health Information via Application Services Procedure,* PAO / Technology Services
5. *Exchanging Encrypted Personal Health Information on Digital Media,* PAO / Technology Services
6. *Exchanging Personal Health Information via Secure Managed File Transfer Procedure,* PAO / Technology Services
7. *Fax Transmission of Personal Health Information Procedure*, PAO / Technology Services
8. *In Person Transfer of Personal Health Information Procedure*, PAO / Technology Services
9. *Transfer of Personal Health Information by Regular Mail Procedure*, PAO
10. *Statement of Confidentiality,* Legal Department and Human Resources
11. *Privacy Audit and Review Standard,* PAO
12. *Information Security Policy*, EISO
13. *Cryptography Standard,* EISO
14. *Logical Access Control Standard,* EISO
15. *Logging, Monitoring and Auditing Standard,* EISO
16. *Logging, Monitoring and Auditing Procedure, EISO*
17. *PHI Handling Standard,* EISO
18. *PHI Handling* Procedure, EISO

All requirements for this section have been met.

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

CCO has in place policies and practices to ensure the secure disposal of paper and electronic copies of records containing PHI. Where records of PHI will be disposed of by a third party service provider, CCO's Services Agreement, which contains robust privacy provisions in its Schedule for Third Party Agreements, ensures that all third parties secure and dispose of PHI in accordance with CCO's security standards. A comprehensive contract management procedure is currently in development; CCO estimates that this procedure will be in place by early 2015. However, CCO's policies and procedures are compliant with the requirements of the Manual without this procedure in place.

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

1. *Physical Security Policy,* Facilities
2. *Hard Copy Personal Health Information Disposal Procedure*, Facilities
3. *Information Security Policy*, EISO
4. *Digital Media Destruction Standard,* EISO
5. *Digital Media Destruction Procedure,* EISO
6. *Services Agreement - Template Schedule for Third Party Agreements,* Legal Department

All requirements for this section have been met.

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

CCO has implemented policies and procedures with respect to supporting passwords for authentication to information systems, equipment, resources, applications and programs. These policies and procedures represent a foundation from which technical controls are implemented, including controls to identify, authenticate, and authorize users and systems accessing CCO information resources. The policies also include the requirement to include risk based decisions regarding the context of any given authentication approach.

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
5. *Logging, Monitoring and Auditing Procedure, EISO*

✓	**All requirements for this section have been met.**

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

CCO has implemented a system for the creation, maintenance and ongoing review of system control and audit logs that are consistent with evolving industry standards and that are commensurate with the amount and sensitivity of the personal health information maintained, with the number and nature of agents with access to personal health information and with the threats and risks associated with the personal health information.

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

1. *Information Security Policy*, EISO
2. *Information Security Code of Conduct,* EISO
3. *Logging, Monitoring and Auditing Standard,* EISO
4. *Logging, Monitoring and Auditing Procedure,* EISO
5. *Information Security Incident & Breach Response Standard*, EISO
6. *Incident Management Framework*, EISO
7. *Security Audit, Testing, and Compliance Standard*, EISO

✓	**All requirements for this section have been met.**

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

CCO's Operational Security Standard and Operational Security Procedure: Patching set out CCO's standard operating practices for patch management. These practices provide baseline patching of operating systems and applications designed to support the security accessibility and reliability of CCO data holdings. Technology and process enhancements to patching are implemented on a regular basis.

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

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

All requirements for this section 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. Since the last review, CCO has revised and supplemented its change management practices to clarify roles and improve testing requirements, among other improvements.

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

1. *Information Security Policy*, EISO
2. *IT Change Management Policy*, Technology Services
3. *IT Change Management Process Flow,* Technology Services
4. *Change Advisory Board Terms of Reference,* Technology Services
5. *IT Change Management Standard: Request for Change Lead Time,* Technology Services
6. *IT Change Management Standard: Change Category and Type,* Technology Services
7. *IT Change Management Standard: RFC ,* Technology Services
8. *Change Request Control Form,* Technology Services

All requirements for this section 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 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 Procedure,* Technology Services
4. *Disaster Recovery Plan,* Technology Services

5. *Services Agreement - Template Schedule for Third Party Agreements,* Legal Department
6. *Secure Transfer of Personal Health Information Policy,* PAO
7. *Secure Transfer of Personal Health Information Standard*, PAO
8. *Policy on Retention of Records Containing Personal Health Information*, PAO
9. *Operational Security Standard,* Technology Services
10. *HP Data Protector Session Logs,* Technology Services
11. *Open Media Logs*, Technology Services and Third Party Service Provider

	**All requirements for this section 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 acceptable use of technology in their job role.

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

1. *Information Security Policy*, EISO
2. *Information Security Code of Conduct and Acceptable Use Policy,* EISO
3. *Acceptable Use of Social Media Policy*, EISO
4. *Logging, Monitoring and Auditing Standard,* EISO
5. *Logging, Monitoring and Auditing Procedure,* EISO
6. *Security Audit, Testing, and Compliance Standard*, EISO

	**All requirements for this section 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 risk assessments (**TRAs**); security reviews or assessments; and technical vulnerability assessments (**VAs**); penetration testing and ethical hacks (when required) and reviews of system control and audit logs.

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*, Technology Services
5. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)*, PAO
6. *Logging, Monitoring, and Auditing Standard,* EISO
7. *Logging, Monitoring, and Auditing Procedure,* EISO
8. *Threat Risk Assessment Template,* EISO
9. *Security Audit, Testing, and Compliance Standard,* EISO
10. *Log of Security Audits*, EISO

All requirements for this section have been met.

Security: IPC Requirement 16: Log of Security Audits.

CCO maintains a log of security audits that have been completed. This log is inclusive of the nature and type of the security audit conducted; the date that the security audit was completed; the agent(s) responsible for completing the security audit; the recommendations arising from the security audit; the agent(s) responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed

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

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

All requirements for this section 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. This work has synergy with the privacy breach management processes and leverages the security and privacy auditing and logging technologies.

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

1. *Information Security Policy*, EISO
2. *Information Security Incident & Breach Response Standard*, EISO
3. *Incident Management Framework*, EISO
4. *Log of Security Incidents,* EISO

	**All requirements for this section 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.

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

1. *Log of Security Incidents,* EISO
2. *Information Security Incident & Breach Response Standard*, EISO

	**All requirements for this section 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
Consulting Agreement					x	x					
Code of Conduct											x
Confidentiality Policy					x						
Contract Management System							x				
Core Privacy and Security Training eLearning Curriculum	x		x			x	x				
CSP Privacy Breach Management Standard Operating Procedure											x
Employee Exit Checklist										x	
Employee Exit Process										x	
Exiting Employee Data Management										x	
Information Security Code of Conduct and Acceptable Use			x	x						x	x
Information Security Policy			x	x							
Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy 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
Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program									**x**		
Log of Privacy and Security Training Completion	**x**	**x**	**x**	**x**							
Personnel Action Form					**x**					**x**	
Principles and Policies for the Protection of PHI at CCO (CCO's Privacy Policy)	**x**	**x**	**x**								
Privacy & Security Acknowledgment Form											**x**
Privacy and Security Training and Awareness Procedure	**x**	**x**	**x**	**x**	**x**						
Privacy Audit and Review Standard	**x**		**x**								
Privacy Breach Management Procedure	**x**										**x**
Privacy Governance Framework	**x**										
Procurement of Goods and Services Policy					**x**						
Progressive Discipline Policy											**x**
Secondment Policy					**x**						
Services Agreement - Template Schedule for Third Party Agreements					**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
Statement of Confidentiality	**x**					**x**				**x**	**x**
Termination Monthly Reports										**x**	
Termination of Employment Policy										**x**	
Unpaid Student Intern Policy					**x**						
VIP Payroll System							**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 its individual agents (*e.g.*, employees) are aware of CCO privacy policies, procedures and best practices, as described herein. The mandatory new employee privacy and security training program and the mandatory annual privacy and security refresher training program, ensure that all CCO employees and all other agents of CCO that will have access to CCO's systems or PHI are informed of their privacy and security responsibilities, in addition to CCO's legislative compliance obligations. All of these individuals, upon completion of the training, must electronically accept a Privacy and Security Acknowledgment form that confirms their understanding of the training and acceptance of their obligations and responsibilities. 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 (CCO's Privacy Policy)*, PAO
2. *Privacy and Security Training and Awareness Procedure*, PAO
3. *Core Privacy & Security Training eLearning Curriculum*, PAO
4. *Privacy Audit and Review Standard*, PAO
5. *Privacy Breach Management Procedure*, PAO
6. *Statement of Confidentiality*, Legal Department and Human Resources
7. *Log of Privacy and Security Training Completion*, PAO
8. *Privacy Governance Framework*, PAO

	**All requirements for this section 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. CCO's information technology solution for privacy & security training ensures that an individual cannot electronically accept this form without first reviewing the applicable privacy & security training.

The following documents outline compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)*, PAO
2. *Privacy and Security Training and Awareness Procedure*, PAO
3. *Log of Privacy and Security Training Completion*, PAO

✓	**All requirements for this section 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 its individual agents are aware of CCO security policies, procedures and best practices as described herein. Through the employee privacy and security training program and the annual privacy and security refresher training program, all CCO employees and all other agents of CCO that will have access to CCO's systems or PHI 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 (CCO's Privacy Policy)*, PAO
2. *Information Security Policy*, EISO
3. *Information Security Code of Conduct,* EISO
4. *Privacy and Security Training and Awareness Procedure,* PAO
5. *Core Privacy & Security Training eLearning Curriculum*, PAO
6. *Privacy Audit and Review Standard*, PAO
7. *Log of Privacy and Security Training Completion*, PAO

✓	**All requirements for this section 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. CCO's information technology solution for privacy & security training ensures that an individual cannot electronically accept this form without first reviewing the applicable privacy & security training.

The following documents outline compliance with this requirement:

1. *CCO's Information Security Policy,* EISO
2. *CCO's Information Security Code of Conduct and Acceptable Use Policy,* EISO
3. *Privacy and Security Training and Awareness Procedure,* PAO
4. *Log of Privacy and Security Training Completion,* PAO

All requirements for this section 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 individual agents 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*, PAO and Human Resources
2. *Privacy and Security Training and Awareness Procedure,* PAO
3. *Personnel Action Form*, Human Resources
4. *Procurement of Goods and Services Policy*, Procurement Office
5. *Secondment Policy,* Human Resources
6. *Unpaid Student Intern Policy,* Human Resources
7. *Consulting Agreement – Template*, Legal Department

8. *Services Agreement - Template Schedule for Third Party Agreements,* Legal Department
9. *Contract Management System*, Procurement Office
10. *VIP Payroll System*, Human Resources

All requirements for this section have been met.

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

CCO has put in place administrative safeguards to ensure that CCO employees and all other agents of CCO that will have access to CCO's systems or PHI 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*, Legal Department and Human Resources
2. *Confidentiality Agreement, Board and Board Committees,* Legal Department
3. *Services Agreement - Template Schedule for Third Party Agreements,* Legal Department
4. *Consulting Agreement – Template*, Legal Department
5. *Core Privacy & Security Training eLearning Curriculum,* PAO

All requirements for this section 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. CCO's Legal Department maintains a log of confidentiality agreements executed by CCO Board and Board Committee members. Agreements executed by third parties retained by CCO, with access to PHI, include specific terms outlining the third party's confidentiality obligations in respect of the PHI. A log of such agreements is maintained by CCO's Procurement Office through its Contract Management System.

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

1. *Contract Management System*, Procurement Office
2. *VIP Payroll System*, Human Resources
3. *Core Privacy & Security Training eLearning Curriculum,* PAO

All requirements for this section 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)*, PAO
2. *Privacy and Access Analyst Job Description,* PAO
3. *Senior Privacy Specialist Job Description*, PAO
4. *Manager, Privacy Job Description,* PAO

All requirements for this section 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 Manager, Job Description* (Draft)*,* EISO
2. *Technical Architect, Information Security, Job Description*, EISO
3. *Sr. Information Security Specialist, Job Description*, EISO
4. *Technical Specialist, Information Security, Job Description, EISO*

✓	**All requirements for this section 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 individual agent (*e.g.*, employment or under contract) relationship, is primarily outlined in the Employee Exit Process. In addition, the policies and procedures listed below ensure that when an individual agent 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.

The following documents outline compliance with this requirement:

1. *Employee Exit Process*, Human Resources
2. *Employee Exit Checklist*, Human Resources
3. *Statement of Confidentiality*, Legal Department and Human Resources
4. *Personnel Action Form*, Human Resources
5. *Termination of Employment Policy,* Human Resources
6. *Termination Monthly Reports,* Human Resources
7. *Information Security Code of Conduct,* EISO
8. *Exiting Employee Data Management,* Technology Services

✓	**All requirements for this section have been met.**

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

CCO has a formal progressive discipline policy that is invoked as appropriate whenever an employee fails to comply with any of CCO's privacy and security and related policies. The *Progressive Discipline Policy* includes requirements relating to the investigation, documentation, and follow-up in respect of any reported non-compliance. The privacy and security-related policy owners are responsible for the enforcement of their policies, and are supported by Human Resources and the PAO.

The following documents outline compliance with this requirement:

1. *Code of Conduct*, Human Resources

2. *Statement of Confidentiality*, Legal Department and Human Resources
3. *Privacy & Security Acknowledgment Form,* PAO
4. *Progressive Discipline Policy*, Human Resources
5. *Privacy Breach Management Procedure*, PAO
6. *Information Security Code of Conduct & Acceptable Use Policy*, EISO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

7. *CSP Privacy Breach Management Standard Operating Procedure*, PAO

	**All requirements for this section 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
Annual Privacy Report	x							
Architecture Review Board Terms of Reference			x					
Business Continuity Plan								x
Business Continuity Framework								x
Business Continuity Worksheet								x
CCO Board of Directors Orientation Handbook		x						
Charter, IM/IT Committee of the Board of Directors	x	x	x					
Core Privacy Committee Terms of Reference			x					
CSP Privacy Breach Management Standard Operating Procedure						x		
Data Access Committee Terms of Reference			x					
Data Governance Council Terms of Reference (Draft)			x					
Disaster Recovery Plan								x
Enterprise Risk Management Framework				x				

CCO Organizational and Other Documentation Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8
Enterprise Risk Management Register			**X**	**X**				
Information Partners Committee Terms of Reference			**X**					
Information Security Framework		**X**						
Information Security Incident and Breach Response Standard						**X**		
Job Descriptions for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program		**X**						
Log of IPC Recommendations							**X**	
Log of Privacy Breaches							**X**	
Log of Privacy Impact Assessments							**X**	
Log of Privacy Inquiries and Complaints							**X**	
Log of Security Audits							**X**	
Log of Security Incidents							**X**	
Principles and Policies for the Protection of PHI at CCO (CCO's Privacy Policy)	**X**					**X**	**X**	
Privacy Audit and Review Standard						**X**		
Privacy Breach Management Procedure						**X**		
Privacy Governance Framework	**X**							

CCO Organizational and Other Documentation Matrix	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8
Privacy Impact Assessment Standard						**X**		
Privacy and Information Security Risk Management Framework				**X**		**X**		
Privacy Risk Register				**X**	**X**		**X**	
Security Audit, Testing, and Compliance Standard						**X**		
Security Operations Working Group Terms of Reference			**X**					
Security Risk Management Standard				**X**		**X**		
Security Risk Register				**X**	**X**		**X**	
Statement of Information Practices	**X**							

IPC Requirements

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

CCO's Privacy Governance 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 CPO has been delegated authority to manage the Privacy Program and is supported by the PAO in carrying out the day-to-day duties. Significant Privacy Program initiatives and changes to the Privacy Program are presented to the CCO Board of Directors. The Strategic Planning, Performance & Risk Management Committee (**SPPRMC**) of the Board of Directors currently oversees the CCO Privacy Program; these duties transitioned to the newly formed IM/IT Board Committee effective September 2013.

CCO's privacy governance structure informs its overall privacy management practices, including leadership, strategy, priorities and risk management. The privacy governance structure provides assurance that the strategies, policies, standards, processes and resources to manage privacy risk are aligned with CCO's objectives and are consistent with applicable laws, standards and best practices.

The following documents outline compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)*, PAO
2. *Privacy Governance Framework,* PAO
3. *Statement of Information Practices*, PAO
4. *Annual Privacy Report,* PAO
5. *Charter - IM/IT Committee of the Board of Directors,* Legal Department
6. *Charter – CCO Board of Directors,* Legal Department

✓	**All requirements for this section 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 ET and Board are apprised of the security program updates through the Chief Technology Officer and CPO briefing updates. The SSPRMC of the Board of Directors oversees the CCO security program. This reporting function transitioned to the IM/IT Committee in September 2013.

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

1. *Information Security Policy*, EISO
2. *Information Security Framework,* EISO
3. *CCO Board of Directors Orientation Handbook,* Legal Department
4. *Charter - IM/IT Committee of the Board of Directors*, Legal Department
5. *Charter – CCO Board of Directors,* Legal Department

	**All requirements for this section have been met.**

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

CCO has terms of reference for every committee that has a role in the Privacy and Security Programs, including the Information Partners Committee, the Data Governance Council, Security Operations Working Group, and the Architecture Review Board. In addition, the PAO, EISO, CPO, and Chief Technology Officer are supported by the ET when addressing significant privacy and security issues.

The following documents outline compliance with this requirement:

1. *Information Partners Committee Terms of Reference,* PAO
2. *Data Governance Council Terms of Reference* (Draft), PAO
3. *Architecture Review Board Terms of Reference,* PAO
4. *Security Operations Working Group Terms of Reference,* EISO
5. *Charter - IM/IT Committee of the Board of Directors*, Legal Department
6. *Data Access Committee – Terms of Reference*, PAO

	**All requirements for this section have been met.**

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

CCO has an ERM Framework (which establishes CCO's Risk Tolerance Levels) which is designed to ensure compliance with CCO's ERM requirements under Management Board of Cabinet's Agency Establishment & Accountability Directive (**AEAD**) and CCO's Memorandum of Understanding with the MOHLTC. This enterprise-wide document is complemented by CCO's Security Risk Management standard and the *Privacy and Information Security Risk Management Framework*, currently being implemented. Together, these documents comprehensively address all roles and responsibilities associated with the identification, assessment, management and monitoring of privacy and security risks throughout CCO. CCO estimates that the *Privacy and Information Security Risk Management Framework* will be

implemented by the end of November 2014. Once this has taken place, CCO will be in compliance with this section of the Manual.

The following documents outline compliance with this requirement:

1. *Privacy and Information Security Risk Management Framework,* PAO & EISO
2. *Privacy Risk Register,* PAO
3. *Security Risk Management Standard,* EISO
4. *Security Risk Register,* EISO
5. *Enterprise Risk Management Framework*, Legal Department
6. *Enterprise Risk Management Register, Summary and Action Plan*, Legal Department
7. *Enterprise Risk Register,* Legal Department

All requirements for this section have been met.

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

CCO has implemented an enterprise wide risk inventory process, and, more specifically, has developed a Security Risk Register, and is implementing a comprehensive Privacy Risk Register which reflects all privacy and security risks respectively throughout CCO. Currently, CCO consolidates recommendations through the use of several logs (i.e. breach log, PIA log, Inquiries and complaints log, Procurement PIA log, IPC recommendations log). CCO is working toward a central Privacy Risk Register which logs both privacy risk as well as recommendations to mitigate and manage those risks for any risk identified during the course of a privacy review. CCO estimates that the *Privacy Risk Register* will be implemented by the end of July 2014. Once this has taken place, CCO will be in compliance with this section of the Manual.

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

1. *Privacy Risk Register*, PAO
2. *Security Risk Register,* EISO
3. *Enterprise Risk Register,* Legal Department

All requirements for this section have been met.

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

CCO's Privacy and Information Security Risk Management Framework requires the maintenance of a Privacy Risk Register which logs both privacy risk as well as recommendations to mitigate and manage those risks. The log includes risks or

recommendations identified through PIAs, privacy audits, privacy reviews, complaint investigations, breach reports and IPC reviews.

Likewise, CCO's Privacy and Information Security Risk Management Framework and Security Risk Management Standard require the maintenance of the Security Risk Register which logs security risks and the corresponding asset, vulnerability, and impact information. The log aggregates risks identified through TRAs, security audits, security reviews, incidents and operational security activities.

The following documents outline compliance with this requirement:

1. *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)*, PAO
2. *Privacy Breach Management Procedure*, PAO
3. *Privacy Impact Assessment Standard,* PAO
4. *Privacy Audit and Review Standard*, PAO
5. *Privacy and Information Security Risk Management Framework,* PAO
6. *Security Risk Management Standard,* EISO
7. *Security Audit, Testing, and Compliance Standard,* EISO
8. *Information Security Incident & Breach Response Standard,* EISO Privacy Risk Register, PAO
9. *Log of Privacy Impact Assessments*, PAO
10. *Log of Privacy Breaches*, PAO
11. *Log of Privacy Inquiries and Complaints*, PAO
12. *Log of IPC Recommendations*, PAO
13. *Log of Security Audits*, EISO
14. *Security Risk Register*, EISO
15. *Log of Security Incidents*, EISO

In addition, the following document addresses additional compliance measures specific to CCO's role as a Prescribed Person:

16. *CSP Privacy Breach Management Standard Operating Procedure,* PAO

	**All requirements for this section have been met.**

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

Currently, CCO consolidates recommendations through the use of several logs (i.e. breach log, PIA log, Inquiries and complaints log, Procurement PIA log, IPC recommendations log). CCO is working toward a central Privacy Risk Register which logs both privacy risks as well as recommendations to mitigate and manage those risks for any risk identified during the course of a privacy review. The log will include risks or recommendations identified through PIAs, privacy audits, privacy reviews, complaint investigations, breach reports and IPC reviews.

CCO also maintains a Security Risk Register which is a consolidated log of risks and recommendations identified through TRAs, security audits, security reviews, incidents and operational security activities.

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 (CCO's Privacy Policy)*, PAO
2. *Privacy Risk Register,* PAO
3. *Log of Privacy Impact Assessments, PAO*
4. *Log of Privacy Breaches, PAO*
5. *Log of Privacy Inquiries and Complaints, PAO*
6. *Log of IPC Recommendations, PAO*
7. *Log of Security Audits,* EISO
8. *Security Risk Register,* EISO
9. *Log of Security Incidents,* EISO

All requirements for this section have been met.

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

In 2013, CCO improved its Business Continuity and Disaster Recovery strategies with the re-drafting and implementation of a robust Business Continuity Plan and separate Disaster Recovery Plan. The Business Continuity Plan is also supported by the Business Continuity Framework. These documents comprehensively address identification, notification, documentation, and assessment of an interruption or threat. They further address the activation of the Disaster Recovery Plan and/or Business Continuity Plan, as applicable, including roles and responsibilities, decision-making, documentation, and resumption activities.

1. *Business Continuity Plan,* Technology Services
2. *Business Continuity Framework*, Technology Services
3. *Business Continuity Worksheet,* Technology Services
4. *Disaster Recovery Plan*, Technology Services

	**All requirements for this section have been met.**

PRIVACY, SECURITY AND OTHER INDICATORS

Part 1 – Privacy Indicators

All Indicators are for the period of November 1, 2011 - October 31, 2013.

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.	Policies and Procedures reviewed in December 2011: • Access and Correction Procedure Policies and Procedures reviewed as a result of last IPC review in 2011, in particular the requirements relating to HO-011: • *Privacy Breach Management Procedure* • CCO's *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)* • Health Information Network Provider (**HINP**) Privacy Policy • Integrated Cancer Screening (**ICS**) Privacy Inquiries and Complaints Procedure (ICS is the former name of CSP) • *Privacy and Security Training Awareness Procedure* • *Privacy Audit and Compliance Procedure* • *Privacy Inquiries and Complaints Procedure* Policies and Procedures reviewed in September 2011: • *Business Process for Data Access Requests* • *Data Linkage Procedure* • *Data Linkage Standard* • *Data Use and Disclosure Standard* • *Decision Criteria for Data Requests* • *De-Identification Guidelines* • *Direct Data Access Procedure* • *ICS Data Request Procedure* • *ICS Access Control Procedure* Policies and Procedures reviewed in January 2012: • *Confidentiality Statement* • *Privacy Impact Assessment Standard* Policies and Procedures reviewed in February 2012: • *Non-Disclosure Confidentiality Agreement* Policies and Procedures reviewed in June 2012: • *Statement of Information Practices* For Policies and Procedures reviewed in August 2013, Please refer to Appendix C – Summary of August 2013 Policy Revisions & New Documents
2	Log of amendments, date of amendment and description of amendment, as a result of the prior review of the IPC.	Minor and substantial changes were made to all Policies and Procedures reviewed in December 2011: • *Access and Correction Procedure* • *CCO's Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)* • *HINP Privacy Policy*

		• *ICS Privacy Inquiries and Complaints Procedure* • *Privacy and Security Training Awareness Procedure* • *Privacy Audit and Compliance Procedure* • *Privacy Breach Management Procedure* • *Privacy Inquiries and Complaints Procedure* Minor and substantial changes were made to all Policies and Procedures reviewed in September 2011: • *Business Process for Data Access Requests* • *Data Linkage Procedure* • *Data Linkage Standard* • *Data Use and Disclosure Standard* • *Decision Criteria for Data Requests* • *De-Identification Guidelines* • *Direct Data Access Procedure* • *ICS Data Request Procedure* • *ICS Access Control Procedure* Minor and substantial changes were made to all Policies and Procedures reviewed in January 2012: • *Confidentiality Statement* • *Privacy Impact Assessment Standard* Minor and substantial changes were made to all Policies and Procedures reviewed in February 2012: • *Non-Disclosure Confidentiality Agreement* Minor and substantial changes were made to all Policies and Procedures reviewed in June 2012: • *Statement of Information Practices* All amendments made as a result of the prior IPC review include all updates per Order HO-011. Amendments also include updates per new programs. Please refer to Appendix C – Summary of August 2013 Policy Revisions & New Documents, for a log and brief description of amendments made to Policies and Procedures in 2013.
3	Record of new policies and procedures developed as a result of the prior review of the IPC.	A new Policy, Standard and set of procedures were created as a result of the last IPC review in 2011: • *Secure Transfer of Personal Health Information Policy* • *Secure Transfer of Personal Health Information Standard* • *Courier of Personal Health Information Procedure* • *In-Person Transfer of Personal Health Information Procedure* • *Transfer of Personal Health Information via Fax Procedure* • *Exchange of Personal Health Information via Secure Managed File Transfer* • *Exchange of Personal Health Information via Application Services Procedure* • *Exchange of Personal Health Information on Encrypted Digital Media Procedure* The policy and procedure for the secure retention of records of personal health information on mobile devices is currently in the process of being drafted.
4	Record of dates and nature of communication regarding amendments.	All 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 posted: • *Access and Correction Procedure* • *CCO's Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario(CCO's Privacy Policy)* • *HINP Privacy Policy* • *ICS Privacy Inquiries and Complaints Procedure* • *Privacy and Security Training Awareness Procedure* • *Privacy Audit and Compliance Procedure*

		• *Privacy Breach Management Procedure* • *Privacy Inquiries and Complaints Procedure* • *Business Process for Data Access Requests* • *Data Linkage Procedure* • *Data Linkage Standard* • *Data Use and Disclosure Standard* • *Decision Criteria for Data Requests* • *De-Identification Guidelines* • *Direct Data Access Procedure* • *ICS Data Request Procedure* • *ICS Access Control Procedure* • *Confidentiality Statement* • *Privacy Impact Assessment Standard* • *Non-Disclosure Confidentiality Agreement* • *Statement of Information Practices* The policy, standard and procedures relating to secure transfer have been communicated through CCO's intranet and have also had their own formal communications sent enterprise wide, per CCO's dissemination procedure. These policies and procedures include: • *Secure Transfer of Personal Health Information Policy* • *Secure Transfer of Personal Health Information Standard* • *Courier of Personal Health Information Procedure* • *In-Person Transfer of Personal Health Information Procedure* • *Transfer of Personal Health Information via Fax Procedure* • *Exchange of Personal Health Information via Secure Managed File Transfer* • *Exchange of Personal Health Information via Application Services Procedure* • *Exchange of Personal Health Information on Encrypted Digital Media Procedure* CCO is currently drafting the retention of PHI Policy.
5	Record of changes to public communication materials, as a result of the prior review of the IPC.	There were no changes related to public communication materials as a result of the prior IPC review. Any changes were as a result of regular updates to policies and procedures.

Collection

IPC Key Indicator Required		CCO's Response
1	The number of data holdings containing personal health information.	CCO has 27 data holdings which are operating under the PHIPA authority of a Prescribed Person. CCO has 116 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.	CCO has 20 statements of purpose have been developed for CCO's data holdings for programs operating under the PHIPA authority of a Prescribed Entity. CCO has 17 statements of purpose have been developed for CCO's data holdings for programs operating under the PHIPA authority of a Prescribed Person. The Log of Statements of Purpose is currently under review.
3	The number and list of the statements of purpose for data holdings containing PHI	CCO has 20 statements of purpose have been developed for CCO's data holdings for programs operating under the PHIPA authority of a Prescribed Entity.

	that were reviewed since the prior review of the IPC.	CCO has 17 statements of purpose have been developed for CCO's data holdings for programs operating under the PHIPA authority of a Prescribed Person. The Log of Statements of Purpose is currently under review. Note: CCO has reviewed its list of statements of purpose for data holdings as of June 30, 2014. Please see Appendix J for the updated list.
4	Log of amendments, date of amendment and description of amendment made to statements of purpose as a result of the prior review of the IPC.	7 amendments to CCO's statements of purpose were made as of June 30, 2014 to add new data holdings, and to amend statements of purpose for existing data holdings. The following data holdings were added to the list: -Evidence-Based Program (EBP) -Case-by-Case Review Program (CBCRP) -Ontario Laboratory Reporting System (OLIS) -e-Outcomes – Head and Neck -Multidisciplinary Case Conference (MCC) Pilot Program The following data holdings were amended: -Ontario Breast Screening Program (OBSP) – to reflect the operation of the OBSP as a prescribed person (previously operated as a prescribed entity) -Mortality data – to reflect the use of this data for prescribed person, in addition to prescribed entity, purposes Please see details in Appendix J.

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.	Through the IDAR process, CCO has granted approval to 369 agents since the prior review of the IPC.
2	The number of requests received for the use of personal health information for research, since the prior review of the IPC.	No requests were received for the use of personal health information for research, since the prior review of the IPC.
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.	No requests were received for the use of personal health information for research, since the prior review of the IPC.

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 in respect of the Prescribed Person received 4 requests for PHI for purposes other than research. 92 requests for PHI were received in respected of the Prescribed Entity for purposes other than research.
2	The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied, since the prior review of the IPC.	All 92 requests received for PHI in respect of the Prescribed Entity for purposes other than research, since the IPC's last review, were approved. The 4 requests received for PHI in respect of the Prescribed Person for purposes other than research, since the IPC's last review, were approved.
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 6 research requests received by CCO in respect of the Prescribed Person for PHI. There were 42 research requests received by CCO in respect of the Prescribed Entity for PHI.
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 6 research requests approved, and none denied, for the disclosure of PHI by CCO in respect of the Prescribed Person. There were 24 research requests approved, and none denied, for the disclosure of PHI by CCO in respect of the Prescribed Entity.
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 6 research agreements executed with researchers in respect of the Prescribed Person. There were 24 research agreements executed with researchers in respect of the Prescribed Entity.
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 119 requests received for de-identified and/or aggregate information for both research and other purposes, in respect of the Prescribed Person. There were 64 requests received for de-identified and/or aggregate information for both research and other purposes, in respect of the Prescribed Entity.
7	The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes, since the prior review of the IPC.	39 agreements were signed for Surveillance, Epidemiology, and End Results Statistical (**SEER*Stat**) data and 3 research agreements were signed by persons to whom de-identified and/or aggregate information was disclosed. Note: At the time of drafting, not all disclosures of de-identified and/or aggregate data require execution of an acknowledgement or agreement. This is being reviewed.

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.	From November 1, 2011 to October 31, 2013, there have been **12** Data Sharing Agreements executed or amended for the collection of PHI by CCO, under PHIPA authority of a Prescribed Entity and a Prescribed Person: • **8** Data Sharing Agreements were executed for the collection of PHI by CCO • **4** were amending agreements Note: There have been **7** amending agreements for the collection **and** disclosure of PHI between Prescribed Entity and Prescribed Person programs within CCO (in addition to the totals above).
2	The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity, since the prior review of the IPC.	From November 1, 2011 to October 31, 2013, there have been **7** Data Sharing Agreements executed or amended for the disclosure of PHI by CCO, under the PHIPA authority of a Prescribed Entity: • **3** Data Sharing Agreements were executed for the disclosure of PHI by CCO • **4** were amending agreements Note: There have been **7** amending agreements for the collection **and** disclosure of PHI between Prescribed Entity and Prescribed Person programs within CCO (in addition to the totals above).

Agreements with Third Party Service Providers

IPC Key Indicator Required		CCO's Response
1	The number of agreements executed with third party service providers with access to personal health information, since the prior review of the IPC.	From November 1, 2011 to October 31, 2013, there have been **three** agreements executed with third party service providers with access to personal health information in the Prescribed Person. CCO has conducted a manual review of the number of agreements executed with third party service providers with access to PHI in the Prescribed Entity. Since the last review of the IPC up until October 31, 2013, **36** 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 IDAR system.

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 16 data linkages approved since the prior review of the IPC. Please refer to Appendix D: Indicators – List of 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 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.	CCO has completed **14** PIAs since the IPC's last review of CCO in October 2011 for programs operating under the PHIPA authority of a Prescribed Entity. These are as follows: 1. CBCRP and EBP: Nov-01-2011 2. WTIS Expansion: Dec-14-2011 3. Computerized Physician Order Entry (**CPOE**) Oncology Patient Information System (**OPIS**) – Addendum to the 2007 PIA Version 5 and 2009 Addendum Version 5 (draft): Feb-03-2012 4. Survivorship Colorectal Cancer Pilot: Feb-27-2012 5. Multidisciplinary Case Conference (**MCC**) Pilot Program: Feb-27-2012 6. OBSP Interval Cancer Review (**ICR**): Mar-01-2012 7. ORN: May-01-2012 8. NDFP eClaims: Jun-10-2012 9. Diagnostic Assessment Program – Electronic Pathway Solution (**DAP-EPS**) Phase II: Jul-19-2012 10. Head and Neck Program - eOutcomes Project: Aug-01-2012 11. Ontario Cancer Registry Information System (**OCRIS**) Enterprise Data Warehouse (**EDW**) Migration Addendum: Sep-24-2012 12. Survivorship - New Models for Breast Cancer Well Follow up Care (**BCWF**) Project: Addendum #1: Apr-30-2013 13. Ontario Renal Reporting System (**ORRS**) Release 3.0: Jun-24-2013 14. MRI Process Improvement Project, Phase 3 - Interim Solution: Jun-27-2013 CCO has completed **9** PIAs since the IPC's last review of CCO for programs operating under the PHIPA authority of a Prescribed Person. These are as follows: 1. Colonoscopy Interim Reporting Tool (**CIRT**) PIA Addendum #1 – Out of Hospital Premises (OHP) - Phase 1: Jan-01-2012 2. ColonCancerCheck Fecal Occult Blood Test (**FOBT**) Reminder Research Study: Jan-01-2012 3. Integrated Cancer Screening (**ICS**) Program – Release 3.0: Mar-20-2012 4. ICS Secure Messaging Solution: May-31-2012 5. OCSP Privacy notice and Result Correspondence: Jun-19-2012 6. Pilot Evaluation of Fecal Immunologic Test in Ontario – Phase 2: Sep-27-2012

		7. CIRT PIA Addendum # 2 – Out of Hospital Premises (**OHP**) - Phase 2: Oct-23-2012 8. CCO PIAs as a Prescribed Person – General Addendum Regarding Section 49(1) of PHIPA: Dec-01-2012 9. Sandy Lake Screening Activity Report (**SAR**) Pilot: May-10-2013 CCO has also completed **1** PIA that is subject to FIPPA: 1. eCCO Sharepoint: Nov-01-2011 Please refer to Appendix E: Indicators – Summary from the Log of Privacy Impact Assessments, for a list of Privacy Impact Assessments completed by CCO from November 1st 2011 to June 30th, 2013.
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 2 PIAs since the IPC's last review of CCO in October 2011 for programs operating under the PHIPA authority of a Prescribed Entity. These are as follows: 1. DAP-EPS Phase II, Privacy Impact Assessment (PIA) Addendum #2, (completed in November 2013) 2. Ontario Positron Emission Tomography Scan Evidence-Based Program: Pediatric PET Registry, Privacy Impact Assessment Addendum #1, (completed in November 2013) CCO has undertaken but not completed 1 PIA since the IPC's last review of CCO in October 2011 for programs operating under the PHIPA authority of a Prescribed Person. These are as follows: 1. OCSP Invitation, Reminder and Recall Correspondence PIA Addendum (completed in March 2014)
3	The number and list of privacy impact assessments that were not undertaken but will be completed and the proposed date of completion.	**33** Planned PIAs are scheduled to be completed for programs operating under the PHIPA authority of a Prescribed Entity and Prescribed Person: Cancer Staging: Oct-15-2013 Updates to the Brachytherapy application and process review: Nov-30-2013 Specialized Services Oversight: Dec-30-2013 "Out of Country" Reimbursement Program: Q4 2013/14 HHRPP: Dec-31-2013 Initial Assessment of Funding Unit Operations: Nov-30-2013 Non-Primary Care Physician (**PCP**) Ordered Screening Tests: Q4 2013/14 Screening Electronic Medical Records Optimization Implementation: Q4 2013/14 Human Papilloma Virus Research Project: Q3 2014/15 FNIM Identifier Pilots and Plan: Q4 2013/14 High Risk Lung Cancer Screening Planning Project: Q4 2013/14 Under/Never Screened Initiative (Phase 2): Q4 2013/14

		On Boarding of Non-OBSP Sites to OBSP: 2015/16 Colposcopy Quality Based Procedures Project: Q4 2013/14 Breast Data Collection: Q4 2013/14 Reporting & Analytics PIA: Oct-01-2013 Ontario Association of Community Care Access Centres PIA: Oct-01-2013 Institute for Clinical Evaluative Sciences PIA: Sep-01-2013 ORN – Ontario Laboratories Information System: Dec-01-2013 Implement an Online Cancer Risk Assessment Toot for use by individual Ontarians and PCPs: Sept-30-2014 DAC: Barisic study: Nov-30-2013 Regional Systemic Treatment Program: Dec-31-2013 Stem Cell Transplant Program Nov-30-2013 DAP EPS Phase II Nov-30- 2013 Pediatric PET Registry Nov-30- 2013 MRI Process Improvement Project (PIP) Phase III Jan-31-2013 OCSP Correspondence Phase II PIA Addendum no. 1 Mar-31-2014 eReports (Secure Messaging Solution) PC SAR Release 1 Mar-31-2014 OBSP Correspondence Phase I and Primary Care Screening Activity Report Mar-31-2014 Ontario Renal Network Acquisition of OLIS Data Phase I May-31-2014 ORRS Release 4.0 Sept-30-2014 EPIC Prostate Cancer Pilot Project Oct-31-2014 ISAAC ADT Integration Nov-30-2014 5 Planned PIAs are currently still in progress: • Integrated Care (in progress)

		• Out of Country (in progress) • ORN CCACs and LTCH Data (in progress) • OBSP correspondence Phase II (in progress) • OBSP Program (in progress)
4	The number of determinations made, since the prior review of the IPC, that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.	CCO uses a Preliminary Privacy Assessment Form (**PPAF**), completed in the initiating phase of a project, to determine whether a PIA or Addendum to a PIA is required for a project based on the collection, use or disclosure of PI/PHI which is in scope for that project. In 2011 there was 1 PPAF that determined a PIA was not required In 2012 there were 21 PPAFs that determined a PIA was not required. In 2013 there were 15 PPAFs that determined a PIA was not required. Please refer to Appendix F: Indicators – Summary from the Log of PPAFs, for the data holding, program at issue, and a brief description of the reasons for the determination. **Note:** In July 2013, new intake and assessment and forms were introduced to the organization – the Privacy Services Engagement Request (PSER) and the Privacy Needs Assessment and Workplan. A Note to File is completed when no privacy services are required in order to document the reasons for such determination. As of July 1st, 2013, CCO uses a PSER form, completed in the definition 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 PHI which is in scope for that project. From July 1, 2013 to October 31, 2013, there were 9 PSERs that determined a PIA was not required. Please refer to the updated version of Appendix F: Indicators – Summary from the Log of PPAFs/PSERs, for the data holding, information system/technology/program at issue, and a brief description of the reasons for the determination.
5	The number, list and a brief description of privacy impact assessments reviewed, since the prior review of the IPC.	There have been 2 PIAs for programs operating under the PHIPA authority of a Prescribed Entity since the IPC's last review of CCO in October 2011: 1. Wait Time Information System Expansion Project PIA Addendum #2 - December 2011 2. DAP-EPS PIA Addendum - Phase II - July 2012 There have been 5 PIAs for programs operating under the PHIPA authority of a Prescribed Person since the IPC's last review of CCO in October 2011: 1. CIRT PIA Addendum #1 – OHP - Phase 1 - January 2012 2. OCRIS EDW Migration PIA Addendum - September 2012 3. ICS PIA Addendum #1 - InScreen 3.0 - March 2012 4. CIRT PIA Addendum #2 – OHP - Phase 2 – November 2012 5. CCO as Prescribed Person PIA General Addendum – s.49 (1) - December 2012

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 IDAR system, to access and use PHI, were conducted since the IPC's last review of CCO in November 2011: • December 2012 – Audit of all data holdings in IDAR system Please refer to Appendix G to Indicators – IDAR Audit Report and Recommendations
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 November 2011: • **Policy review** 2012 – 1 review completed. o The purpose of the review was to identify policies that were "related" to CCO's *Privacy Breach Management Procedure* and amend them to add definitions of the terms "privacy breach", "suspected privacy breach", and "privacy risk" in accordance with the revisions to CCO's *Privacy Breach Management Procedure* that were mandated by HO-011. o A total of six policies were identified as "related" policies and the single "recommendation" was that the policies be revised in accordance with the purpose of the review – these six policies (along with the *Privacy Breach Management Procedure* are listed above as part of IPC Indicator 1 for "General Privacy Policies, Procedures and Practices" under the heading "Policies and Procedures reviewed as a result of last IPC review in 2011, in particular the requirements relating to HO-011:" o This audit was initiated in November 2011 and was completed in January 2012, at which time the "recommendation" was carried out and the required revisions to these policies were approved. 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.	For the PE programs there was a total of 110 privacy incidents from November 1, 2011 - October 31, 2013 (this includes OBSP): • In 2012, 12 of these were externally originated and count as an unauthorized collection (PHI accidentally sent to us) • In 2013, 72 of these were externally originated and count as an unauthorized collection (PHI accidentally sent to us) • In 2011, 0 privacy risks occurred • In 2012, 2 privacy risks occurred • In 2013, 2 privacy risk occurred • In 2011, 3 internal privacy breaches occurred • In 2012, 5 internal privacy breaches occurred • In 2013, 14 internal privacy breaches occurred For the PP programs there was a total of 51 privacy incidents from November 1, 2011 - October 31, 2013: • In 2012, 5 of these were externally originated and count as an unauthorized collection (PHI accidentally sent to us) • In 2013, 20 of these were externally originated and count as an unauthorized collection (PHI accidentally sent to us) • In 2011, 2 privacy risks occurred • In 2012, 2 privacy risks occurred • In 2013, 1 privacy risk occurred • In 2011, 3 internal privacy breaches occurred • In 2012, 11 internal privacy breaches occurred • In 2013, 8 internal privacy breaches occurred
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,	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: **2011:** PE - 3 policy infractions PP - 3 policy infractions **2012:** PE - 5 policy infractions, 12 unauthorized collections PP - 11 policy infractions, 5 unauthorized collections **2013**: PE - 16 policy infractions, 71 unauthorized collections PP - 8 policy infractions, 20 unauthorized collections Please refer to Appendix H to Indicators - Summary from the Log of Privacy Breaches for a list of privacy breaches.

	• The date(s) that notification was provided to the health information custodians or any other organizations, • The date that the investigation was commenced, • The date that the investigation was completed, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	

Privacy Complaints

IPC Key Indicator Required		CCO's Response
1	The number of privacy complaints received, since the prior review of the IPC.	No privacy complaints received for the Prescribed Entity. 508 complaints received for the Prescribed Person. CCO's cancer screening programs, operating under a Prescribed Person authority, involve direct contact with the public through several different types of correspondence. This correspondence includes invitation letters, result letters and reminder letters to remind participants to get screened. In addition, the OCSP program also sends out a privacy notice to program participants prior to sending out result letters. The public facing nature of these programs and direct contact with the public tend to promote more awareness among members of the public of CCO's collection of PI and PHI. In contrast, CCO's Prescribed Entity programs are not public facing and do not involve direct contact with the public using PI and PHI.
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	Of the 508 complaints received for the Prescribed Person, all have been investigated and closed as per CCO's *Privacy Inquiries and Complaints Procedure*. As part of an ongoing effort to address complaints and inquiries, the PAO develops FAQs that respond to common questions and complaints. Most complaints that are received by telephone are resolved using FAQs. All relevant details of each resolution are logged. Complaints that cannot be addressed using FAQs are investigated further by the Privacy Specialist assigned to the cancer screening programs in accordance with CCO's *Privacy Inquiries and Complaints Procedure.* The current method of capturing information related to complaints for the Prescribed Person is through InScreen. The log maintained in InScreen includes detailed notes, including investigation information, internal escalation procedures, resolutions, the date investigations were complete and the date recommendations were addressed. .A separate complaint log

	investigation was commenced, • The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation, • The date that the investigation was completed, • A brief description of each recommendation made, • The date each recommendation was addressed or is proposed to be addressed, • The manner in which each recommendation was addressed or is proposed to be addressed, and • The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.	is not currently created as detailed records of each complaint are attached to the complainant's record in InScreen. This approach enables complaint investigations involving PHI to be securely stored in one location. Data stored in InScreen for each complaint is consistent with the requirements set out on page 73 of the Manual. Prior to March 2014, InScreen did not have an automated feature that allowed for complaint data to be extracted into a log. Extracting the data was a manual process and PHI had to be redacted from each complaint record. In March 2014, the first series of technical changes were made to InScreen to allow data to be more easily extracted for all new complaints. Further technical changes will follow in July and August 2014. When fully implemented, these changes will allow for complaint data to be segregated from the parts of each InScreen record that contain PHI. This new functionality will allow us to maintain and extract a complaint log that is compliant with the Manual but that does not contain PHI. In summary, CCO currently complies with the Manual requirements for tracking privacy complaints, however, the complaints are not easily aggregated without including PHI. Technical changes are currently being implemented to allow for CCO's continued compliance and to allow us to produce a complaint log that does not contain PHI.
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.	All privacy complaints are investigated.

Part 2 – Security Indicators

All Indicators are for the period of November 1, 2011 - October 31, 2013.

General Security Policies and Procedures

	IPC Key Indicator Required	CCO's Response
1	The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.	There have been three reviews of security policies and procedures since the IPC's last review of CCO in October 2011: 1. March - 2012 2. February – March 2013 3. April, 2013 **Note:** the 2013 reviews included a full update to 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 2013 review of CCO's security policy suite resulted in amendments to the following documents: • *Security Risk Management Standard* • *Logging, Monitoring, and Auditing Standard* • *Logical Access Control Standard* • *Operational Security Standard* • *Information Security Code of Conduct & Acceptable Use* • *Physical Security Policy* • *Paper Destruction Policy* • *Data Centre Access Policy* • *Visitor Access Policy* All amendments made were to ensure technical currency and to achieve further alignment of language with that of the review Manual. For a description of amendments made as a result of the August 2013 review, please see Appendix C - Security.
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 standards and/or procedures were developed as a result of the IPC's last review of CCO in October 2011. The new documents are as follows: • *Logging, Monitoring, and Auditing Procedure -Provides procedural implementation for the corresponding standard* • *Operation Security: Patching Procedure - Provides procedural implementation for security patching* • *Digital Media Disposal Procedure - Provides procedural implementation for the corresponding standard* • *Security Audit, Testing, and Compliance Standard - Clarifies the types of security testing performed and to align with industry practices* • *Information Security Incident & Breach Response Standard - Supports effective security incident / breach response and tracking in accordance with CCO's compliance requirements* • *Digital Media Disposal Standard- Consolidates previous guidelines and formalizes practices* • *PHI Handling Standard- Consolidates previous guidelines and formalizes practices* • *PHI Handling Procedure - Provides procedural implementation for the corresponding standard*
4	The dates that each amended and newly developed security policy and procedure was communicated to agents	All of the new security policies, standards and/or procedures which were developed and approved have been communicated through CCO's intranet. The new and updated policies, standards, and procedures will go through the approval work flow and be in effect for in 2014.

	and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.	
5	Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	No externally available communication materials were amended as a result of the IPC's last review of CCO in October 2011.

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 conduct audits when an incident or suspected physical security incident has occurred or is notified by an employee. There have been no physical security breaches since the previous IPC review in 2011. 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 Physical Security, Paper Destruction, Data Centre Access, and Visitor Access policies were reviewed in 2013-14 and revisions to those policies were approved on March 19, 2014. Video monitoring includes a live system.. All access cards provided to agents are registered with Facilities upon receipt of the NESF form. 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.

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.	Cancer Care Ontario continually monitors our system control and audit logs using a number of automated systems. These systems monitor for errors in applications, availability of system components, and security events. These logs are reviewed both through automated means, as well as by CCO operations staff. For example: • Security events at both an infrastructure level and application level are logged to CCO's Logging, Monitoring, and Auditing System (**LMAS**). This system uses a collection of rules to generate alerts based on certain detected patterns. An example of this would be excessive file system activity on our PHI file shares. • Operational events from our Windows servers are centrally logged and monitored through the Microsoft System Centre Suite. This monitoring detects failed applications and other error states, allowing operations staff to ensure normal operation of systems • Network devices use Syslog and Simple Network Management Protocol (**SNMP**) to generate logging and event data for both real time and ad-hoc analysis. These typically discover excessive network patterns or configuration errors, allowing for operational staff to investigate. Events that require action trigger some combination of CCO's ITIL based incident process, security response process, and privacy breach process. Examples of typical responses include: • Reviewing and analyzing unusual log entries that are indicative of a misconfiguration or software flaw. These are then escalated to a product team to isolate the cause. In some cases vendors are notified and a software patch is applied. • Excessive security events trigger follow up from CCO's EISO. For example, failed login attempts are analyzed to determine whether as system is being attacked or whether a user simply forgot their password. • Alerts from operational systems result in a more immediate responses from both operational teams and the EISO when the source of the alert is deemed to be security related. For example, a server that goes offline is investigated immediately based on alerts triggered within the monitoring systems.
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	**95** security audits have been completed since the IPC's last review of CCO in November 2011, as noted in CCO's log of security assessments. CCO's security audits include: • Threat risk assessments; and • Vulnerability and Other assessments. Please refer to Appendix I: Summary from the Log of Security Audits & Information Security Breaches, for a list of security audits completed since the IPC's last review of CCO.

	each recommendation made, – The date that each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is expected to be addressed.	

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 October 31, 2013 there have been **16** security incidents and breaches at CCO since the IPC's last review of CCO in October 2011. CCO does not distinguish between PE and PP incidents hence the number below includes incidents and breaches for both PE and PP Nov – Dec 2011: 3 Incidents Jan – Dec 2012: 10 Incidents, 2 of which were determined to be breaches. Jan – Oct 2013 : 3 Incidents **Note:** CCO's EISO has updated its definitions of information security incident and security breach as follows: **Information Security Incident:** An information security incident is a security event that may compromise business operations or threaten CCO security. Incidents require action on the part of CCO resources to contain and prevent further harm to CCO infrastructure and/or information assets. A ***Near Miss*** is an incident that did not result in a breach – but had the potential to do so. **Information Security Breach:** A security breach occurs when there is a loss of confidentiality, integrity, or availability of sensitive information and information assets, resulting from a breach of CCO's security safeguards or from failure to establish reasonable safeguards. Security breaches include contravention of policies, procedures, or practices that result in material security risk to CCO.
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	Descriptions of all suspected information security breaches are captured in Appendix I: Summary from the Log of Security Audits & Information Security Breaches.

	or suspected information security breach, – 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 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

All Indicators are for the period of November 1, 2011 - October 31, 2013.

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 October 31, 2013, all CCO employees (includes PE and PP) have received initial privacy orientation since the IPC's last review of CCO in November 2011. • **2012:** 296 employees received initial privacy orientation at the start of their employment • **2013:** 250 employees received initial privacy orientation at the start of their employment 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.	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 system access for employees who do not complete their initial privacy orientation within 30 days of their start date will be disabled.
3	Record of agents who have attended and who have not attended ongoing privacy training each year, since the prior review of the IPC.	As of October 31, 2013, the number of CCO employees who completed ongoing privacy training each year since the IPC's last review of CCO in October 2011 are as follows: • **2011**: 973 completed the Annual Privacy Refresher Training • **2012**: 842 completed the Annual Privacy Refresher Training • **2013**: The Annual Privacy Refresher is scheduled for November 2013 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 Refresher 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 2011, as described in CCO's PAO Communication Plan. These are as follows: **2011**: • Revised and published Statement of Information Practices (internal and external) • Revised and published Privacy FAQs (internal and external) • Developed and published Privacy posters to raise visibility and awareness on compliance services provided by CCO's PAO (internal) • Developed and published Privacy Calendars (internal) **2012**: • Developed and published Privacy Calendars (internal) **2013**: • Developed and published new privacy lifecycle process with communications strategy

		• Presented Privacy 101 Presentations offered enterprise-wide • Presented Privacy Lunch and Learn offered enterprise wide

Security Training and Awareness

IPC Key Indicator Required		CCO's Response
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 October 31, 2013, all CCO employees (includes both PE and PP) have received initial security orientation since the IPC's last review of CCO in November 2011. • **2012:** 296 employees received initial security orientation at the start of their employment • **2013:** 250 employees received initial security orientation at the start of their employment 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.	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 system access for employees who do not complete their initial privacy orientation within 30 days of their start date will be disabled.
3	Record of agents who have attended and who have not attended ongoing security training each year, since the prior review of the IPC.	As of October 31, 2013, the number of CCO employees who completed ongoing security training each year since the IPC's last review of CCO in October 2011 are as follows: • **2011**: 973 completed the Annual Privacy Refresher Training • **2012**: 842 completed the Annual Privacy Refresher Training • **2013**: The Annual Privacy Refresher is scheduled for November 2013 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 Refresher 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 November 2011. These are as follows: **2011:** • Monthly Security Bulletins (once a month) • Privacy and Security Annual Refresher Training 2011 (Nov- Dec, 2011) **2012:** • Monthly Security Bulletins (once a month) • Healthcare Information Security Seminar 2012 – (Mar, 2012) • Privacy and Security Annual Refresher Training 2012. (Nov – Dec, 2012) • October is Cyber Security Awareness Month – (Oct, 2012)

		2013: • Monthly Security Bulletins (once a month) • A prescription for digital health : Empowering you to protect your online privacy (Jan, 2013) • Information Security Knowledge Sharing (TASK – May, 2013)

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.	For the period between November 1st, 2011 and October 31st, 2013, the number of Confidentiality Agreements executed are as follows: • Nov 1, 2011 to Dec 31 2011 – 33 Confidentiality Agreements executed • Jan 1, 2012 to Dec 31, 2012 - 266 Confidentiality Agreements executed • Jan 1, 2013 to October 31, 2013 – 273 Confidentiality Agreements executed Note: The confidentiality agreement is a part of the package that every agent receives upon commencement of work at CCO. Agents are blocked from being entered into the HR system if their confidentiality agreement is not signed. The numbers noted above include CCO employees associated with both the roles of CCO i.e. as a Prescribed Entity and as a Prescribed Person. These numbers do not include the number of third party service providers who have accepted confidentiality terms under contract.
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. An employee will not be set up in the Human Resources Information System (**HRIS**) until all of the mandatory paperwork has been received, which includes the confidentiality agreements. Employees not set up in HRIS are not paid. All agreements with third party service providers contain confidentiality terms.

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	From November 1st, 2011 to October 31st , 2013, there have been **466** terminations and cessations. The number of Terminations/Cessations (by year) are as follows:

	related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.	By Year: • Nov 1, 2011 to Dec 31 2011: **35** • Jan 1, 2012 to Dec 31, 2012: **239** • Jan 1, 2013 to Oct 31, 2013: **192** Due to the confidential nature of some of the information provided in response to this indicator, CCO has excluded some of details from the public version of this report, however this information has been provided to the IPC.

Part 4 – Organizational Indicators

All Indicators are for the period of November 1, 2011 - October 31, 2013.

Risk Management

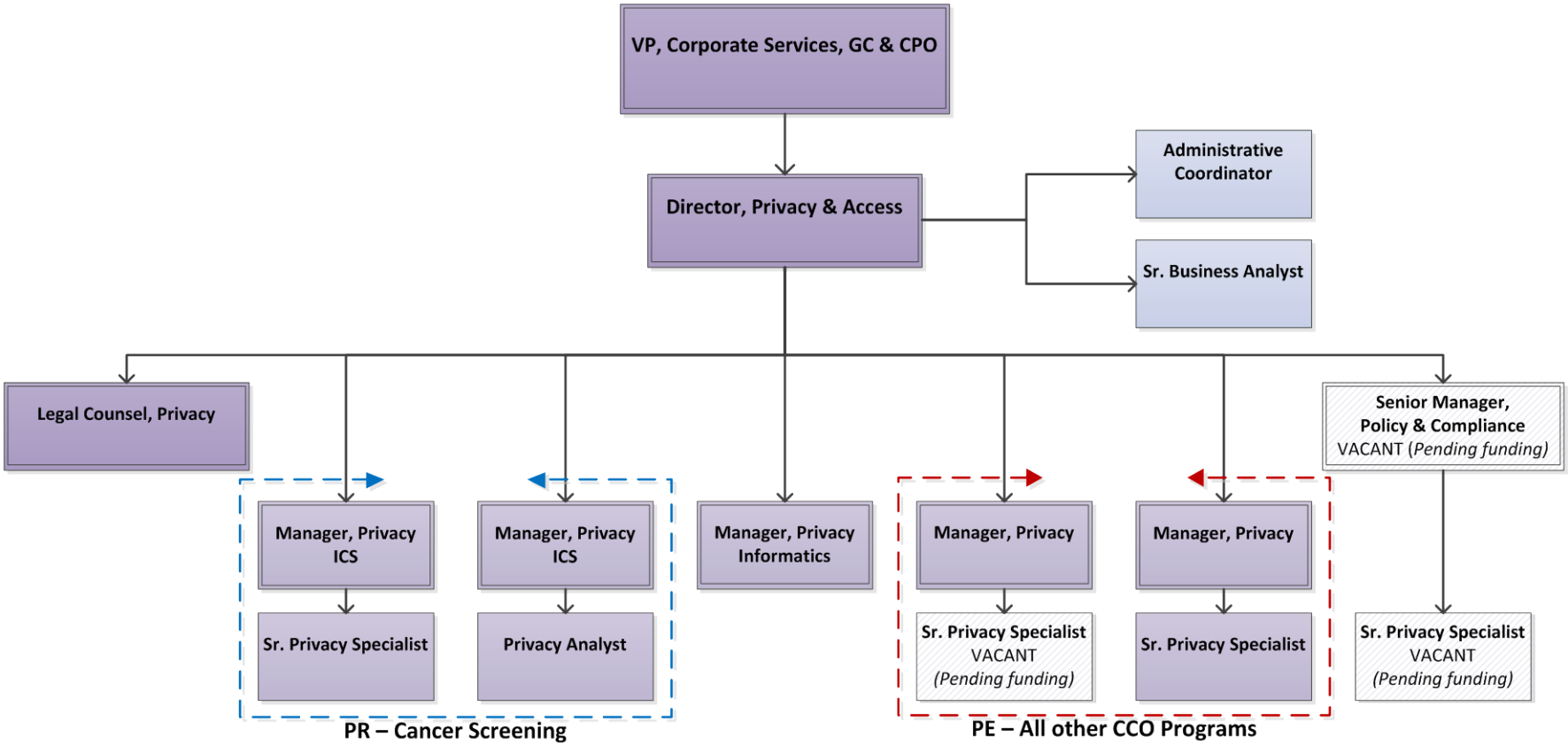
	IPC Key Indicator Required	CCO's Response
1	The dates that the corporate risk register was reviewed by the prescribed person or prescribed.	Since the prior review by the IPC, the corporate risk register has been reviewed by the Board in October 2012 and 2013.
2	Whether amendments were made to the corporate risk register as a result of the last IPC review, and if so, a brief description of the amendments made.	Amendments were made to the corporate risk register as a result of the review in September 2012. Based on this review, the number of High risks (as defined in the CCO' Risk Assessment Matrix) dropped from 8 to 2. In November 2012, CCO's Legal Department developed (and CCO's Board approved) a comprehensive *Enterprise Risk Management Policy* (Policy) and *Enterprise Risk Management Framework: A Step-by-Step Guide to Risk Management* (Framework). CCO's Policy and Framework are based on the Ministry of Government Services' *Guide to the Risk-Based Approach for the Agency Establishment and Accountability Directive dated February, 2011.* The objectives of the Policy and Framework are to: • Ensure that all Material Risks (defined as those risks calculated as Low, Medium or High in accordance with CCO's Risk Assessment Matrix) are properly assessed, mitigated (to the extent possible), and monitored; • Establish risk management processes that comply with CCO's obligations under the AEAD; • Integrate and align existing risk management processes across CCO; and • Develop a culture of risk awareness. The Policy and Framework do not try to duplicate formalized risk assessment processes existing at CCO. Rather, the aim of the Policy and Framework is to ensure that all risk assessments performed at CCO use consistent risk language and permit CCO to establish an aligned picture of risk across the enterprise. The Framework also includes a Risk Tolerance Statement, which outlines the degree to which CCO is willing to accept residual risk (defined as the remaining level of risk after mitigating action is taken) across CCO's major risk categories. CCO's Risk Tolerance Statement permits CCO to monitor whether CCO's risks identified in the Tool are within acceptable levels.

Business Continuity and Disaster Recovery

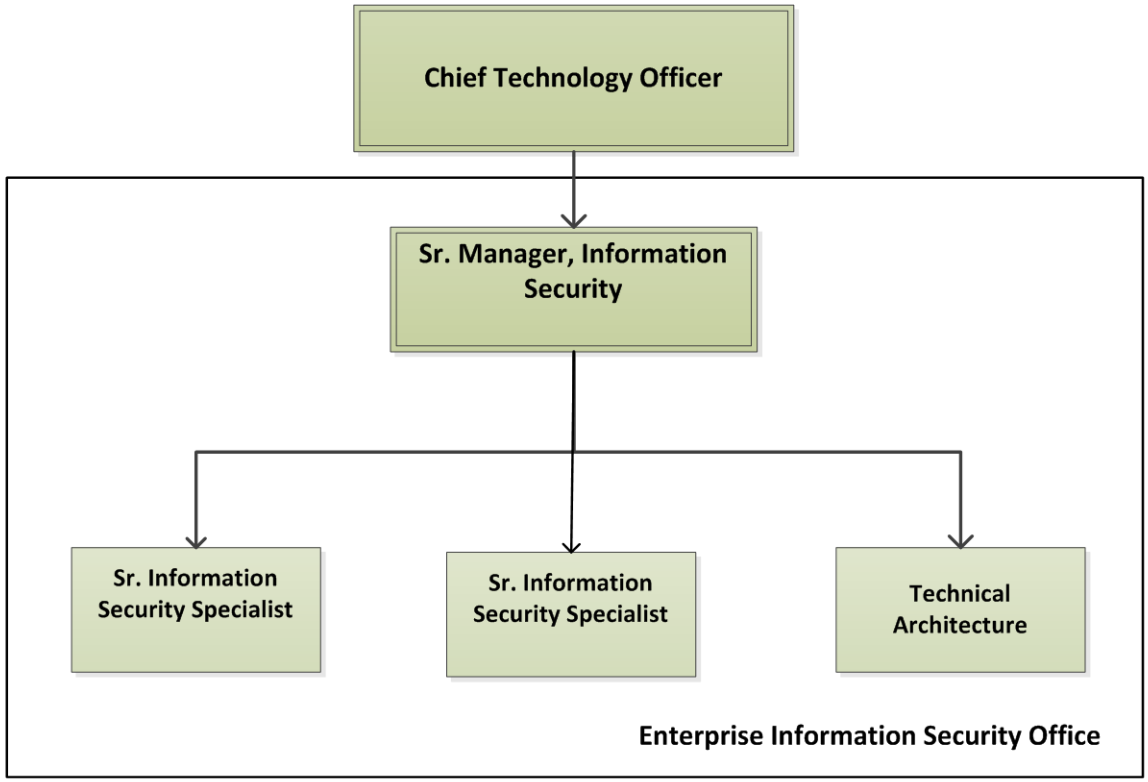
	IPC Key Indicator Required	CCO's Response
1	The dates that the business continuity and disaster recovery plan was tested since the prior review by the Information and Privacy Commissioner of Ontario.	From November 1, 2011 to June 30, 2013, the following tests were performed: Disaster Recovery Plan Testing dates: General Tabletop walk-through 4/23/2013 14:00 Network Infrastructure Tabletop Exercise 5/22/2013 10:00 Technology Component testing dates: File Level Recovery 3/12/2013 10:30 Hypervisor Server Recovery 3/12/2013 10:40 DB Recovery 3/12/2013 11:00 Hypervisor Server Recovery 3/20/2013 12:00 Hypervisor -V Server Recovery 4/12/2013 11:55 File Level Recovery 4/12/2013 12:15 DB Recovery 4/12/2013 12:30 Hypervisor Server Recovery 5/14/2013 11:15 Hypervisor Server Recovery 5/14/2013 11:35 File Level Recovery 5/14/2013 11:45 DB Recovery 5/14/2013 14:30 File Level Recovery 6/20/2013 11:55 Hypervisor Server Recovery 6/20/2013 12:15 DB Recovery 6/20/2013 12:25 File Level Recovery 7/2/2013 11:20 DB Recovery 7/2/2013 11:25 Hypervisor Server Recovery 7/9/2013 10:25 Hypervisor Server Recovery 7/10/2013 14:05 From July 1, 2013 to October 31, 2013, the following tests were performed: Table top tests: Lync 7/26/2013 15:00 Lync 8/21/2013 13:00 Exchange & Active Directory 9/24/2013 10:00 Internet Access 9/24/2013 15:00 Internal and External DNS 10/24/2013 10:00 Direct Access & Legacy VPN 10/24/2013 11:00 Technology Component testing dates: M:\ drive 7/2/2013 11:20 SQL DB File Recovery - atcprd4sqdb1 7/2/2013 11:25 Hyper-V server CORPRD1EPWEB2 7/9/2013 10:25 Cogeco backup power supply 7/9/2013 12:00 VM Ware-P server recovery 7/10/2013 14:05 Hyper-V Server - CCOPRD1UMA01 8/16/2013 17:40 P: Drive 8/16/2013 17:55 BSD Database (Prod) 8/21/2013 15:00 power load test 8/21/2013 20:00 Cogeco generator monthly testing 8/24/2013 23:00 CCOPRD1LYD01 9/17/2013 11:25 H: Drive 9/17/2013 16:40

		SQLSERVER4STG 9/17/2013 16:45 EPO1 9/17/2013 16:50 CCOQAS1UAGGW3 10/10/2013 13:05 M: Drive 10/15/2013 10:25 BSD database (dev) on obspdbdq server 10/15/2013 10:35
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.	No changes or amendments were made as a result of testing. Revisions were approved for the business continuity and disaster recovery plans in March 2013. Subsequent minor revisions were approved in early June 2013. None of the revisions were as a result of testing. The updated documents include: • Business Continuity Framework – CIO • Business Continuity Plan – CIO • Disaster Recovery Plan

APPENDIX A: Current Organizational Structure for the Privacy & Access Office



APPENDIX B: Current Organizational Structure for the Enterprise Information Security Office



APPENDIX C: Summary of August 2013 Policy Revisions & New Documents

Documents listed below are still in draft form and have not yet received formal approval.

PRIVACY

Item	Description of Amendments
Application for Disclosure of Information for Research Purposes	Minor amendments to align with other related procedures and make certain requirements more express
Business Process for Data Requests	Re-drafted to reflect current practices while still ensuring that IPC manual requirements are met.
Data Linkage Policy	Re-drafted entirely to reflect current practice and continue to meet all IPC requirements.
Data Linkage Procedure	Re-drafted entirely to reflect current practice and continue to meet all IPC requirements.
Data Sharing Agreement Initiation Procedure	Minor changes to expressly set out documentation requirements.
Data Sharing Agreement Standard	Minor changes to more expressly set out certain requirements.
Data Sharing Agreement Initiation Form	Moderate changes to expressly (i) require Data Steward to assess whether Data Exchange meets quality and privacy standards and safeguards in place, and (ii) require PAO to confirm reasons for approval and assess whether DSA required.
Data Sharing Agreement Template	Re-drafted to provide comprehensive agreement template with robust privacy terms rather than sample template provisions.
Data Use and Disclosure Standard	Substantial changes to expressly expand application to registry activities, expand third party service provider requirements, and more expressly set out responsibilities associated with the disclosure process.
Decision Criteria for Data Requests	Minor revision to clarify one aspect of the process.
Disaster Recovery Plan	Re-drafted to form *Business Continuity Plan*
Employee Exit Checklist	Minor revisions to update names and process.
Employee Exit Process	Moderate changes to expressly expand application to all contractors and consultants, and to expressly contemplate return of PHI.
Internal Data Access Policy	Substantially revised to replace the *Direct Data Access Procedure* to reflect current practices and continue to meet IPC manual requirements.
Internal Data Access Procedure	Substantially revised to replace the *Direct Data Access Procedure* to reflect current practices and continue to meet IPC manual requirements.
Non-Disclosure Agreement	Minor revision to clarify breach notification requirements.
Physical Security Policy	New policy drafted to consolidate various physical security principles and controls.
Principles and Policies for the Protection of PHI at Cancer Care Ontario (CCO's Privacy Policy)	Minor updates to policy references and responsible individuals.
Privacy Audit and Review Standard	Substantial changes to enhance requirements around reviews and audits, including scheduling thereof.
Privacy Breach Management Procedure	Minor amendments were made regarding the review and storage of breach reports.
Privacy Governance Framework	Newly drafted to clearly set out operational governance structure and core program controls.
Privacy Impact Assessment Standard	Minor amendments to clarify requirements.
Privacy Inquiries and Complaints Procedure	Minor to moderate amendments to enhance investigation plan and process.
Privacy Risk Management Framework	Newly drafted to set out comprehensive process to evaluate privacy risks.
Privacy Risk Management Policy	Newly drafted to define the approach by which CCO identifies, assesses, responds to and monitors privacy risks.

Services Agreement – Template Schedule for Third Party Agreements	*Revised Template Schedule for Third Party Agreements* to house it within a template services agreement in order to ensure more robust protection for PHI, and in particular on transfer, retention, disposal and inventory requirements.

SECURITY

Item	Description of Amendments
Access Card Procedure	Minor to moderate amendments to enhance the procedure and reflect current practices
Change Management Policy	Minor revisions to include greater process detail
Data Backup Procedure	Minor revisions to include greater process details and cross-reference new secure retention of PHI policy.
Data Centre Access and Usage Policy	Minor revisions to more expressly require that access be limited only to individuals who routinely require access.
Hard Copy PHI Disposal Procedure	New procedure to document current process and ensure compliance with IPC manual requirements.
Information Security Code of Conduct & Acceptable Use	Minor revisions to better reflect the specific requirements set out in the review manual
Information Security Program Framework	New document to consolidate various documents describing the overall security program structure and operation
Logging, Monitoring, and Auditing Standard	Minor wording changes to better reflect the specific requirements set out in the review manual
Logical Access Control Standard	Minor revisions to stay current with technology
Operational Security Procedure – Patching	Moderate changes to enhance clarity around responsibilities and risk-based decision-making.
Operational Security Standard	Minor revisions based on improved operational security practices
Physical Security Policy	New policy drafted to consolidate various physical security principles and controls.
Policy on Retention of Records Containing PHI	New policy drafted to describe the purposes for retention of PHI.
Secure Transfer of PHI Policy	Minor amendments to expand application.
Secure Transfer of PHI Standard	Minor amendments to expand application.
Security Risk Management Standard	Minor revisions to better align with CCO's Enterprise Risk Management Policy and other compliance requirements (e.g. Canada Health Infoway product certification)

HUMAN RESOURCES

Item	Description of Amendments
Employee Exit Checklist	Minor revisions to update names and process.
Employee Exit Process	Moderate changes to expressly expand application to all contractors and consultants, and to expressly contemplate return of PHI.
Principles and Policies for the Protection of PHI at Cancer Care Ontario	Minor updates to policy references and responsible individuals.
Privacy and Security Acknowledgement	Minor revisions to enhance acknowledgment language.
Privacy and Security Training and Awareness Procedure	Amended in response to PHIPA Order HO-011 to clarify that privacy training will include information concerning the manner in which CCO staff are expected to respond to privacy breaches, suspected privacy breaches, and privacy risks as those terms are defined in CCO's Privacy Breach Management Procedure.

Privacy Audit and Review Standard	Substantial changes to enhance requirements around reviews and audits, including scheduling thereof.
Privacy Breach Management Procedure	Amended in response to PHIPA Order HO-011 (HO-011) to clarify definitions and further minor amendments were made regarding the review and storage of breach reports.
Privacy Governance Framework	Newly drafted to clearly set out operational governance structure and core program controls.
Progressive Discipline	Minor amendments to enhance detail on investigation process and clarify parties responsible for determining disciplinary action.
Services Agreement – Template Schedule for Third Party Agreements	Revised Template Schedule for Third Party Agreements to house it within a template services agreement in order to ensure more robust protection for PHI, and in particular on transfer, retention, disposal and inventory requirements.

ORGANIZATIONAL

Item	Description of Amendments
Business Continuity Plan	Re-drafted to separate *Business Continuity Plan* from *Disaster Recovery Plan*.
Disaster Recovery Plan	Re-drafted to form *Business Continuity Plan*.
Enterprise Risk Management Framework	Newly drafted to provide a comprehensive process to evaluate material risks to integrate and align existing risk management processes across CCO.
Enterprise Risk Management Policy	Newly drafted to set out applicable risk management processes and document the roles and responsibilities of CCO Staff and CCO's board in identifying, assessing, mitigating and monitoring material risks and outlines key aspects of CCO's risk management and reporting processes.
Principles and Policies for the Protection of PHI at Cancer Care Ontario (CCO's Privacy Policy)	Minor updates to policy references and responsible individuals.
Privacy Audit and Review Standard	Substantial changes to enhance requirements around reviews and audits, including scheduling thereof.
Privacy Breach Management Procedure	Minor amendments were made regarding the review and storage of breach reports.
Privacy Governance Framework	Newly drafted to clearly set out operational governance structure and core program controls.
Privacy Risk Management Framework	Newly drafted to set out comprehensive process to evaluate privacy risks.
Privacy Risk Management Policy	Newly drafted to define the approach by which CCO identifies, assesses, responds to and monitors privacy risks.

APPENDIX D: Indicators – List of Data Linkages

Request No.	Data Holdings Linked	Description	Requestor	Request Acknowledgement Date	DAC Approval Date
13-052	Ontario Cancer Registry (**OCR**);#Pathology Information Management System (**PIMS**)	Testicular cancer study	Requester	Mar-11-2013	Jun-06-2013
12-138	Activity Level Reporting (**ALR**);#OCR;#NDFP	Hodgkin's lymphoma study	Requester	Dec-21-2012	Jan-23-2013
12-125	ALR;#OCR;#NDFP	Breast cancer study	Requester	Dec-19-2012	Jan-23-2013
12-124	ALR;#Other	Diagnostic assessment programs study	Requester	Dec-19-2012	
12-117	OCR;#ALR;#OBSP	Breast cancer study	Requester	Nov-29-2012	Dec-11-2012
12-115	ALR;#OCR;#OBSP	Breast cancer study	Requester	Nov-28-2012	Dec-11-2012
12-112	OCR;#ALR	Cancer incidence study	Requester	Nov-22-2012	Nov-28-2012
12-101	OCR;#PIMS;#ALR	Gynecologic cancer study	Requester	Oct-24-2012	Dec-11-2012
12-079	ALR;#OCR	Cancer study	Requester	Sep-05-2012	Jan-23-2013
12-077	Other	Colorectal cancer study	Requester	Aug-15-2012	
12-076	NDFP;#ALR	Childhood cancer study	Requester	Aug-08-2012	Dec-11-2012
12-061	OBSP	Cancer Screening study	Requester	Jun-21-2012	Dec-14-2012
12-032	OCR;#Colorectal Screening Data - CIRT	Colonoscopy study	Requester	Mar-16-2012	Apr-11-2012
12-031	Other	Cancer risks study	Requester	Apr-27-2012	Aug-17-2012
11-160	OCR;#ALR	Carcinoma study	Requester	Nov-24-2011	May-11-2012
11-133	PIMS	Testicular cancer study	Requester	Apr-30-2012	

APPENDIX E: Indicators –Log of Privacy Impact Assessments

From November 1st, 2011 to October 31, 2013

The data holding, information system, technology or program involving Personal Health Information that is at issue	Date of completion of PIA (or date expected to be completed)	Person responsible for completing PIA	Risk No.	The Privacy Risks arising from the Privacy Impact Assessment	The Recommendations, Mitigation Strategies, and/or Privacy Controls arising from the Privacy Impact Assessment	Responsible party for addressing each recommendation	Date that each recommendation was addressed (or is expected to be addressed)	The manner in which each recommendation was or is expected to be addressed
MRI Process Improvement Project (PIP) Phase III - Interim Solution	Jun-27-2013	Legal Counsel, Privacy	**1**	Contractual authority for Collection #1 may not be in place because the Template Agreements have not yet been executed.	ATC must ensure that the Template Agreement for a Participating Hospital has been fully executed (i.e., signed by the Participating Hospital and CCO) before the date that CCO begins to collect MRI Data from that Participating Hospital.	Legal Counsel, Privacy & Access Office	6/24/2013	Template Agreement approved by Chief Privacy Officer on June 24, 2013. Template Agreements then circulated by Business Unit to Participating Hospitals. No PHI was collected by CCO from a Participating Hospital prior to complete execution of the Template Agreement.
			2	The public has not been provided with notice of CCO's creation of a permanent data holding for the MRI Data.	The PAO must amend CCO's Privacy Policy so as to appropriately reference the MRI Data as part of its next update to these policies. These amendments must be completed by July 31, 2013.	Legal Counsel, Privacy & Access Office	N/A	Recommendation was not carried out, as decision was made by CCO to collect MRI PIP Data on a permanent basis via its Wait Times Information System , which is already listed as a data holding in CCO's Privacy Policy.
Ontario Renal Reporting System Release 3.0 (ORRS R.3.0)	Jun-24-2013	Consultant	**1**	CKD Service Providers need to know the PHI they are required to submit to CCO for the purposes of the ORN in order that a privacy breach not occur because of the provision of unnecessary data for which ORN has no purpose.	The draft Schedule "C" to the CKD Management Agreement 2013/14 include the data elements included in the VA&IA Assessment Tool that are required to be submitted to the ORN by the CKD Service Providers.	Privacy Specialists (PAO)	Jul-05-2013	Followed up with Legal

			2	If CCO is required to comply with all of the obligations of an institution as set out in FIPPA, policies, processes and procedures will need to be put in place that address CCO's collection, use, disclosure, retention and destruction of personal information related to the operation of ORRS R.3.0.	CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or the PHIPA Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a HINP; a Service Provider; an agent under PHIPA; a s. 39(1)(c) prescribed person; and a s. 45 prescribed entity **[outstanding Recommendation #1 from the ORN PIA]**.	Privacy & Access Office (PAO)	Oct-01-2014	Follow up with IPC and/or MOHLTC
			3	In the event that the CKD Management Agreements are not executed prior to the deployment of ORRS R.3.0, a risk exists that CCO will not receive the necessary Patient PHI for the continuing operation of ORN and/or that the CKD Service Providers will not adhere to its privacy obligations as set out in the agreement.	CCO complete and execute the amended CKD Management Agreements with all CKD Service Providers prior to the deployment of ORRS R.3.0.	Program	Oct-01-2013	All CKD providers have accepted the terms of an agreement.
			4	CCO will not be in compliance with ss. 6(3)(7) of the Regulation as well as s.7 of its *HINP Privacy Policy* if the License and HINP Agreement is not executed before CCO begins providing its services as a HINP to the CKD Service Providers.	CCO to manage the distribution and execution of the License and HINP Agreement to ensure that it has been signed by all CKD Services Providers for which CCO is providing HINP services prior to Go-Live and keep the CCO Privacy & Access Office apprised of its progress on a monthly basis.	Privacy and Access Office and Program	Sep-01-2013	All CKD providers have accepted the terms of an agreement.
			5	Generally ORN employees do not function in the role to which they are assigned at the current time before Tier 1 Services will be assumed by the CCO HelpDesk, as is generally the case. These employees need to understand how to appropriately manage PHI in this role, as do the Service Desk employees managing issues related to ORN PHI.	CCO to ensure that all ORN and CCO Service Desk employees providing services in support of R.3.0 receive/received privacy training specific to the operation of ORRS R.3.0.	Privacy and Access Office and Program	Aug-01-2013	Delivery of very specialized training related to new/unique features of ORRS R.3.0 provided.

			6	The provisions of the applicable policies, procedures and agreements that will come into play in the event of a privacy breach of PHI in ORRS R.3.0, include inconsistent and sometimes conflicting responsibilities of the roles and responsibilities of CCO and the CKD Service Providers . They also do not address certain matters that must be dealt with in the event of a breach. Together these create the risk that a breach will not be managed efficiently and effectively exposing both CCO and the CKD Service Providers to adverse publicity and comment by the IPC and potential concerns of Patients whose PHI is included in ORRS R.3.0.	1) CCO to review the HINP Privacy Policy, the Privacy Breach Management Procedures and the applicable provisions in the License and HINP Agreement and clarify the Procedures to be followed by CCO staff in the event of a Privacy Breach of PHI to which CCO has access in its dual role under PHIPA as a prescribed entity and a HINP. 2) CCO must develop a list of those individuals and their contact information at each of the CKD Service Providers who are to notify their Privacy Officers in the event of a data Breach, as well as the names and contact information of their Privacy Officers. 3) CCO to ensure that the list of the contact information for the CKD Service Providers' Privacy Officers be available to the CCO Privacy & access Office for their use should notification of these individuals be required in the event of a Privacy Breach relating to the PHI provided to CCO via ORRS R.3.0 by the CKD Service Providers.'	1) Privacy and Access Office 2) Program 3)Program & Privacy and Access Office	Dec-01-2013	1) Policy review and amendments for consistency 2) Contact lists in the Insight Database 3) See #2 above. PAO can have access to the contact information in the Insight database if and when required
			7	CCO will be receiving PHI from Transferring-In Sites	CCO develop operational processes for the collection, use, disclosure and retention of Patient PHI received by the Service Desk from Transferring-In sites who have received a "multiple patients" notice in response to a search for a Patient in ORRS; such processes to be reviewed by the CCO Privacy & Access Office.	Content: Program Review: Privacy and Access Office	Oct-01-2013	Process developed and include requirement for review by P&A Office
			8	In circumstances in which there are currently no controls over how this information will be recorded, used, retained etc. such that there is a risk that it will not be managed according to the requirements in PHIPA.	ORN Program to advise the Privacy & Access Office if and when new linkages are occurring between the ORN PHI and existing CCO data holdings and whether a permanent data holding will be created after any such new linkages, so that a PIA or PIA Addendum can be completed for such new linkages **[outstanding as Recommendation #4 from the ORN PIA]**.	Privacy and Access Office and Program	Feb-14-2014	Project confirmed their understanding that linkages to ORRS requires notification to PAO. New linkages to CORRS data confirmed.

			9	CCO policies require that a PIA be conducted on any data linkages that will result in the creation of a new data holding. In the absence of the Privacy & Access Office being aware that such linkages are taking place, there is a risk that any privacy issues that would be identified through the conduct of a PIA will not be identified.	Before linking ORN PHI with PHI in other CCO prescribed entity or prescribed registry data holdings or external data holdings, CCO's Privacy & Access Office will review any DSAs or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO **[outstanding as Recommendation #5 from the ORN PIA]**.	Privacy and Access Office and Program	Feb-14-2014	Project confirmed their understanding that linkages to ORRS requires notification to PAO. New linkages to CORRS data confirmed.
			10	CCO may be using PHI in contravention of the terms of the data sharing agreement pursuant to which it was received from an external entity.	Program to establish a retention period for the ORN data holding and ensure that the retention period is necessary for the fulfillment of the Program purpose. Program/data steward to advise the Privacy & Access Office when all or part of the ORN data holding is no longer required for the purposes of the Program **[outstanding from Recommendation #6 of the ORN PIA]**.	Program	N/A	Program to advise PAO when all or part of the ORN data holding is no longer required.
			11	CCO is not complying with its own policies setting out the requirements to be established by the data stewards of each of CCO's data holdings.	The Program/data steward responsible for the ORN data holding to establish an inventory of data retained by the Program, in line with CCO's Privacy Policy **[outstanding from Recommendation #7 of the ORN PIA]**.	Program and Data Steward	6/1/2013	Complete.
			12	A retention and archiving policy applicable to PHI may be developed that does not comply with CCO's privacy policies and/or the requirements of PHIPA.	EISO work with the CCO Privacy & Access Office, the ORN Data Steward and the Program to develop a retention (and archiving policy) with associated procedures for ORRS data, including the ORRS logging tables.	Enterprise Information Security Office (EISO) & Privacy and Access Office (PAO)	Oct-15-2013	Policy & procedure development

			13	In the absence of data quality standards the PHI provided to CCO may not be accurate for the purposes for which CCO uses it for planning etc. This risk is exacerbated with the deployment of ORRS R.3.0 because a risk now exists that the accuracy will not be sufficient to support the data usage by the CKD Service Providers for direct Patient management purposes.	Program to prepare CCO data specifications for data collectors to adhere to when submitting data to CCO and ORN data steward to be responsible for implementing data quality practices. Program to advise the Privacy & Access Office when this has been implemented **[outstanding from Recommendation #8 of the ORN PIA]**.	Program	Oct-15-2013	Data specifications and QA for ORN data to be submitted
			14	A risk exists that, without input from the CCO Privacy & Access Office the development of and changes to enterprise security policies, procedures and standards that relate to PHI will not be in compliance with *CCO's Privacy Policy* and/or PHIPA.	- The CCO Privacy & Access Office to work with EISO and Technology Services to identify the security policies, standards and procedures, including those related to identity management; authentication; access controls; assignment of data use groups; data encryption and or other forms of data de-identification; data storage segregation; separation of data testing and production environments; auditing and reporting; security incident management; and session management that impact the manner in which PHI is collected, used, disclosed, retained, transferred and destroyed by CCO. - The CCO Privacy & Access Office to be consulted on any changes and updates made to CCO's current security policies, standards and procedures that impact on the manner in which PHI is collected, used, disclosed, retained, transferred and destroyed by CCO, as well as on the development of any new such policies, standards and procedures.	Enterprise Information Security Office (EISO) & Privacy and Access Office (PAO)	Oct-15-2013	Identification of policies/ procedures/ standards

			15	There is a risk that the CKD Service Providers will not understand their obligations related to safeguarding the Patient PHI to be inputted into ORRS, as well as the security requirements related to the operation of the Application itself.	The Program work with the CCO Privacy & Access Office to develop the Registration Guide to include the provisions in Recommendation #1 of the Remediation Plan developed in response to the recommendations in the TRA. The Privacy & Access Office should ensure that the Registration Guide includes those CCO privacy policies and procedures with which the CKD Service Providers are required to comply pursuant to the terms of the License and HINP Agreement and the CKD Management Agreement, as well as security best practices such as a prohibition on the use of shared workstations, networks and ORRS accounts, requirements for strong passwords and maintenance of the currency of ORRS accounts to manage privacy risks that may result from inadequate security when CKD Service Providers access the ORRS system and ORN PHI.	Program, Enterprise Information Security Office (EISO), & Privacy & Access Office (PAO)	Sep-01-2013	Content of Registration Guide completed and is available on the CKD site. Information session on the Guide had been provided.
			16	A risk exists that appropriate safeguards as required by PHIPA and CCO's privacy and security policies the system holding ORN Patient PHI have not been implemented thus exposing CCO to regulatory non-compliance as well as privacy breaches.	CCO to implement all of the remediation action items in the Remediation Plan, as well as Recommendation ID 15 in the June 2013 TRA prior to the deployment of ORRS R.3.0.	Enterprise Information Security Office (EISO)	Oct-15-2013	Risk Register for TRA completed and signed off
			17	CCO risks being in non-compliance with its statutory obligations as a HINP as well as contractual obligations in its License and HINP Agreement with the CKD Service Providers if the results of the PIA and the TRA are not provided to the CKD Service Providers.	As part of its project management of the ORRS R.3.0 deployment, CCO ensure that an individual is responsible for providing the CKD Service Providers with a copy of the results of this PIA Addendum and the TRA conducted on the Application.	Content: Privacy & Access Office (for PIA) and EISO (for TRA) Communications: Program	Sep-01-2013	Results of the PIA and TRA provided to users and still available on the CKD site.

			18	If CCO does not communicate more specific information to the CKD Service Providers on the CCO policies and practices to which they must comply per their contractual agreements, as well as more detailed security best practices, Permitted Users may not understand their security responsibilities as set out in the License and HINP and CKD Management Agreements.	- CCO to develop a vehicle to communicate to the CKD Service Providers their specific obligations, including those of their Permitted Users, as set out in CCO policies and procedures with respect to maintaining the privacy of the individuals to whom the ORN PIA relates and the security and confidentiality of their PHI. - The vehicle developed for the communication to the CKD Service Providers of their specific obligations as set out in CCO policies and procedures with respect to maintaining the privacy of the individuals to whom the ORN PIA relates and the security and confidentiality of their PHI and security to include their responsibility for implementation of security best practices related to the matters outlined in Recommendation # 1 in the Remediation Plan. - The CCO Access & Privacy Office to work jointly with the ORN Program to develop the content for the communication vehicle developed in response to Recommendation #22.	Content: Privacy and Access Office (for PIA) and EISO (for TRA) Communications: Program	Sep-01-2013	PIA Q and As provided on CKD Site.
			19	A risk exists that any exceptions developed to the implementation of the roles, responsibilities and processes established by the RA/LRA Agreement do not meet the same privacy, security and confidentiality standards as those included in the Agreement signed by the CKD Service Providers.	- In the event that a CKD Service Provider seeks an exception process, such an exception process must be fully documented by CCO and approved by CCO EISO and the CCO Privacy & Access Office. - Once the ORRS Registration Guide has been developed for ORRS R.3.0 it should be reviewed by the CCO Privacy & Access Office and the Legal Department to ensure that it is consistent with the relevant privacy and security provisions of the License and HINP Agreement and reflects the LRA registration process contemplated for the Application.	Program and Privacy and Access Office (PAO)	Aug-01-2013	Exception process developed and approved by EISO and the P&A Office.

			20	A risk exists that the LRAs are not aware of their responsibilities for ensuring that the list of the Permitted Users at their facility is kept current and that revocation of the access rights of Permitted Users be done in a timely manner to ensure that there is no unauthorized access to ORN PHI.	- The ORRS Registration Guide should include a process setting out the roles of the LRA and the ORN in the event that the access rights of a Permitted User may be revoked, the timing of the sending of the revocation form to the Service Desk and the follow up contact by the LRA with the Service Desk if the LRA does not receive notification of receipt of the request within two business days. - The Registration Guide for ORRS R. 3.0, to mandate the timing of reporting by the LRA to the CCO Help Desk of changes in user credentials and, in particular the revocation of access rights when a Permitted User is suspected of having caused a privacy breach, to be within one (1) business day as is the case with respect to changes in user information. - The ORN Program, in collaboration with the CCO Privacy & Access Office explicitly assign to the LRAs the responsibility for keeping Permitted User accounts and access up to date in their development of the Registration Guide.	Program, Enterprise Information Security Office (EISO) and Privacy and Access Office (PAO)	Sep-01-2013	Content of Registration Guide completed and is available on the CKD site. Information session on the Guide had been provided.
			21	LMAS alerting updates required	- CCO to establish criteria to assess in what circumstances the development of additional use cases and threat scenarios for ORRS may be required. - In the event that CCO determines that additional rules specific to ORRS are warranted, a threat model which identifies the typical use cases with respect to access to PHI and threat scenarios for each use case is to be developed by the ORN Program in collaboration with the Privacy & Access Office and EISO, in accordance with ss.6(3)4 of the Regulation, Policy 7.5 of CCO's Privacy Policy and Requirement 4 of CCO's HINP Privacy Policy.	Enterprise Information Security Office (EISO)	Apr-30-2014	EISO to confirm that they will establish the criteria for detecting threat scenarios as required. To be completed by April 2014.

			22	CCO risks being in non-compliance with its own Privacy Policy if the summary of this PIA is not made publicly available.	The CCO Access & Privacy Office to prepare a summary of this PIA and post it on the CCO corporate website.	Privacy and Access Office	Sep-01-2013	Completed and posted.
			23	There is a risk that CCO will be in non-compliance with subsections 6(3)(2) and (3) of the Regulation if it does not develop a plain language description of the services it provides as a HINP to the CKD Service Providers as HICs which description is made available to the CKD Service Providers to provide to the Patients whose PHI is provided to CCO through ORRS.	CCO prepare a "plain language" statement of the services it provides to the HICs, including a general statement of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information and provide this statement to all CKD Service Providers to make it publicly available to individuals whose PHI will be uploaded into ORRS R.3.0.	Privacy and Access Office	Sep-01-2013	PIA Q and As provided on CKD Site.
			24	CCO risks not being transparent with respect to the information services it provides to CKD Service Providers in its role as a HINP under PHIPA.	- CCO to include a reference to the License and HINP agreement, this PIA and the TRA(s) conducted on ORRS R.3.0 in the list of "References" that inform the HINP Privacy Policy. - CCO draft a description of the ORRS R.3.0 web application and upload tool to be included in Appendix "A" to the HINP Privacy Policy.	Privacy and Access Office	**TBD**	HINP Privacy Policy to be updated and description to be drafted.
Sandy Lake Screening Activity Report (SAR) Pilot	5/10/2013 - Updated 10/12/2013	Legal Counsel, Privacy / Privacy Manager	**1**	The PAO has not reviewed the operational processes by which this Use will be carried out.	1. The ACCU must document the processes by which :a) the Sandy Lake Resident List will be securely transferred from CCO to the CCO Representative on-site at Sandy Lake; b) the CCO Representative will use the Sandy Lake Resident List to confirm the identities of residents who seek to opt-out of inclusion in the Sandy Lake SAR (and thereby generate the Opt-out List) – this process should include checks to ensure the Opt-out List contains accurate data such as: i) requiring government I.D. to verify identity of resident seeking to opt-out of the Sandy lake SAR; and ii) resolving data quality issues when an apparent error or gap is identified in the Sandy Lake Resident List, as explained above. c) the Sandy Lake Resident List and the Opt-out List will be securely stored on-site at Sandy Lake; d) the Opt-out List will be securely transferred from the CCO Representative to CCO; e) the	1. ACCU 2. PAO/EISO 3. ACCU	1. a) November 18, 2013 b) i. November 18, 2013 ii. N/A c) November 18, 2013 d) N/A e) December 17, 2013 f) November 18, 2013 2. The PAO and the Enterprise Information Security Office (EISO) must review and approve these processes. 3. The CCO Representative must sign CCO's standard Statement of Confidentiality,	1. a) The Sandy Lake Resident List was transferred to the CCO Representative in person in accordance with CCO's In-Person Transfer of Personal Health Information Procedure. b) i. The CCO Representatives received privacy and security training regarding the process for confirming opt-outs to the Sandy Lake SAR. This training advised that valid government-issued identification must be presented in order to complete the opt-out. ii. There were not any errors or gaps identified in the Sandy Lake Resident List. c) The CCO Representatives received privacy and

					Sandy Lake Resident List and the Opt-out List will be securely destroyed by the CCO Representative once the Use is complete; and f) the CCO Representative will be trained to follow the above processes. 2. The PAO and the Enterprise Information Security Office (EISO) must review and approve these processes. 3. The CCO Representative must sign CCO's standard Statement of Confidentiality, revised by legal counsel in the PAO to explicitly state that the CCO representative agrees (a) to use the Sandy Lake Resident List and the Opt-out List only for CCO's purposes and (b) to comply with the operational processes in respect of this Use listed above.		revised by legal counsel in the PAO to explicitly state that the CCO representative agrees (a) to use the Sandy Lake Resident List and the Opt-out List only for CCO's purposes and (b) to comply with the operational processes in respect of this Use listed above.	security training regarding best practices for secure storage of PI/PHI. The CCO Representatives also signed a Statement Confidentiality which confirm the Representatives' agreement to store the Resident List in a physically secure location (see attached – Appendix C)d. A plan to securely transfer the Opt-out List from the CCO Representatives to CCO via secure managed file transfer (Tumbleweed) was in place. However, as the CCO Representatives confirmed that no opt-outs were requested , this transfer did not take place. e) CCO has received a Certificate of Destruction (see attached – Appendix D) confirming that the Resident List has been destroyed in accordance with IPC fact sheets. f) The CCO Representatives received privacy and security training. 2. The PAO and EISO reviewed and approved these processes. 3. The CCO Representatives signed the Statement of Confidentiality as revised by legal counsel to address this recommendation (see Appendix C

			2	The Sandy Lake SAR Dashboard may constitute a "Report" for the purposes of the MOHLTC PR DSA	1. Each Sandy Lake Nurse with access to the Sandy Lake SAR Dashboard should enter a confidentiality agreement with CCO in which the Sandy Lake Nurse agrees not to disclose the Sandy Lake SAR Dashboard or any of its contents to any person without CCO's written approval – this contractual obligation may be combined with the agreement between CCO and each Sandy Lake Nurse proposed in respect of Disclosure #2. 2. The ACCU should provide training to the Sandy Lake Nurses in respect of this obligation – this training may be combined with other training provided to the Sandy Lake Nurses in respect of the Pilot (e.g., instructions on how to use the Filtered Sandy Lake SAR).	1. ACCU 2. ACCU/PAO	1. December 6, 2013 2. December 6 and December 17, 2013	1. Upon receipt of feedback from Health Canada on November 15, 2013, the ACCU decided to disclose the SAR to physicians, rather than nurses, at the Sandy Lake Nursing Station only. Due to the confidential nature of the discussions between CCO and its stakeholders, CCO has excluded some of the details of these discussions from the public version of this report, however these details have been provided to the IPC The PAO is comfortable that the privacy and PHIPA authority analysis set out in respect of Disclosure # 2 above applies to the physicians at the Sandy Lake Nursing Station as HICs under PHIPA. The two physician recipients of the SAR have signed a SAR Disclosure Agreement (see attached – Appendix E) drafted by CCO legal counsel setting out their obligations in respect of this recommendation, and in alignment with Health Canada's advice. 2. Privacy and security training in respect of this obligation was provided to the two physician recipients of the SAR.
			3	The draft Privacy Notice for Disclosure #2 has not been finalized, nor has the process	1. The PAO and the ACCU must finalize the wording of the Privacy Notice for	1. PAO & ACCU 2. ACCU	1. November 15, 2013 2. a)	1. The Privacy Notice was finalized and approved by

				for disseminating the Privacy Notice to the residents of Sandy Lake.	Draft #2; 2. The ACCU must document the processes by which the Privacy Notice will be disseminated to the residents of Sandy Lake, including: a. the means by which the Privacy Notice will be disseminated to Sandy Lake residents (e.g., letters, radio advertisements); b. the duration of the dissemination period (e.g., one month); 3. The PAO must review and approve these processes. 4. The ACCU must represent to the PAO that the Privacy Notice has been disseminated in accordance with its documented processes.	3. PAO 4. ACCU	November 18, 2013 b) November 18, 2013 3. November 14, 2013 4. December 10, 2013	Health Canada on November 15, 2013 – see attached – Appendix A. 2. a) ACCU confirmed that the Privacy Notice was disseminated via radio advertisement and posted in a public space at the Sandy Lake Nursing station. 2. b) ACCU confirmed that the Privacy Notice would be posted for a period of 2 weeks, from November 18, 2013 until December 2, 2013. 3. The PAO reviewed and approved these processes. 4. The ACCU represented to the PAO that the Privacy Notice was disseminated in accordance with the approved processes.
			4	CCO has not yet prepared a template agreement for disclosure of the Filtered Sandy Lake SAR to individual Sandy Lake Nurses.	1. Legal counsel in the PAO must draft template agreements for Disclosure #2 with based on the "terms of use" agreed to by PEM Physicians in respect of access to the PEM SAR via CCO's Secure Messaging Solution. In particular, the draft template agreements must address: a. The legislative capacity and authority of the parties for the disclosure of the Filtered Sandy Lake SAR; b. The manner in which: i. the Filtered Sandy Lake SAR will be transferred to the Sandy Lake Nurse; and ii. the Sandy Lake Nurse will access the Filtered Sandy Lake SAR; c. The Sandy Lake Nurse's obligations to collect, use and disclose the Filtered Sandy Lake SAR in accordance with his or her obligations as a HIC under	1. PAO 2. ACCU 3. ACCU & PAO	1. November 15, 2013 2. December 6, 2013 3. December 6 and 17, 2013	1. Legal Counsel in the PAO drafted a SAR Disclosure Agreement addressing each of the recommendations set out in response to risk # 4. However, following the ACCU's consultations with Health Canada as noted above, it was decided that the SAR would be disclosed to physicians at the Sandy Lake Nursing Station only. 2. The 2 physicians to whom the SAR is being disclosed signed the agreement. 3. Privacy & Security training was provided to the physicians.

					PHIPA; d. The Sandy Lake Nurse's acknowledgement that once he or she has "custody and control" of a copy of the Filtered Sandy Lake SAR, the Sandy Lake Nurse is responsible as a HIC in the event that that copy is stolen, lost or subject to (a) unauthorized use or disclosure or (b) unauthorized copying, modification or disposal (i.e., a privacy breach); e. The Sandy Lake Nurse's obligation to contact CCO immediately in the event of any such privacy breach or suspected privacy breach and cooperate with CCO in respect of the investigation of the breach or suspected breach. 2. Each of the Sandy Lake Nurses who will have access to the Filtered Sandy Lake SAR must sign a copy of the agreement. 3. The ACCU should provide training to the Sandy Lake Nurses in respect of the key privacy obligations contained in the agreement – this training may be combined with other training provided to the Sandy Lake Nurses in respect of the Pilot (e.g., instructions on how to use the Filtered Sandy Lake SAR).			

			5	The process by which the Filtered Sandy Lake SAR will be transferred from CCO to the Sandy Lake Nurses have not yet been confirmed by the ACCU.	1. The ACCU must document the process by which the Filtered Sandy Lake SAR will be transferred from CCO to the Sandy Lake Nurses. This process must set out: a. The CCO staff members responsible for the transfer; b. The method of transfer (e.g., encrypted drive); and c. The manner in which the Sandy Lake Nurses will access the Filtered Sandy Lake SAR. 2. The PAO and EISO must approve this method of transfer as compliant with CCO's Secure Transfer of PHI Policy, Standard and Procedures, as applicable; and 3. CCO Staff and the Sandy Lake Nurses must receive training on this transfer process, as needed.	1. ACCU 2. PAO & EISO 3. EISO	1. November 14, 2013 2. November 14, 2013 3. December 6 and 17, 2013	1. The ACCU documented the process whereby the SAR is sent and accessed electronically at the Sandy Lake Nursing Station using secure managed file transfer (Tumbleweed). 2. The PAO and EISO approved this method of transfer. 3. Training was provided.
Survivorship - New Models for Breast Cancer Well Follow up Care (BCWF) Project	Apr-30-2013	Privacy Specialist / Legal Counsel, Privacy	**1**	Members of the public currently have no way of knowing what information is being collected by CCO without their express consent because the BCWF Project is not described on CCO's website or in the Statement of Information Practices. It should be noted that the Survivorship Program has advised that data collected for the BCWF Project will not be a permanent data holding.		N/A	N/A	A decision was made not to update the list due to the data holding being from a pilot program and thus not a permanent data holding.
			2	The Privacy & Access Office must conduct a review to ensure that any linking of collected BCWF data with other CCO data is permitted. This review will also extend to SCRCP, since it is unclear whether that review took place.		Program Manager & Manager, Privacy	N/A	Recommendation was not carried out, as the program chose not to proceed with the data linkage. But they have been advised that should they choose to proceed with any data linkage activities, they must contact the PAO.
			3	The Survivorship Program must ensure that all BCWF Aggregate Reports being disclosed to the MOHLTC and the facilities are prepared according to CCO's De-Identification Guidelines.		Program Manager & Manager, Privacy	Ongoing	This recommendation requires on-going support from the PAO at times of reporting.

CCO PIAs as a Prescribed Registry – General Addendum Regarding Section 49(1) of PHIPA	Dec-20-2012	Legal Counsel, Privacy		N/A		N/A	N/A	N/A
Colonoscopy Interim Reporting Tool Project (CIRT) Out of Hospital Premises (OHP) Phase II	Oct-26-2012	Privacy Specialist	**1**	The OHPs are not explicitly named in PHIPA as a category of "HICs" in the same manner as hospitals.	1. The OHP Project must identify the nature of the legal entity representing each participating OHP (e.g., a corporation, or a partnership of physicians). 2. Each OHP Agreement (including both funded and unfunded OHPs) must contain the following representations and warranties by the OHP: (a) the legal entity representing the OHP in the OHP Agreement is a HIC under PHIPA, (b) such legal entity is in compliance with its obligations as a HIC, (c) such legal entity has the authority to collect and use the colonoscopy data that will be disclosed to CCO under the funding agreement, and (d) such legal entity has the authority to disclose such data to CCO as a prescribed registry under PHIPA.	OHP Project Team/Legal	1 & 2. October 22, 2012	1 & 2. Nature of legal entity was identified, and the final OHP Agreements included the representations and warranties set out in the recommendation.
			2	The OHP Project will send monthly reports to the OHPs setting out the OHP Data Set in aggregate form, and may send additional comparative reports between hospitals and OHPs. Aggregate data that has not been properly de-identified may potentially contain PHI.	3. Should there be any change to the data elements included in the monthly reports to OHPs during Phase 2, the OHP Project must consult with the Privacy & Access Office to ensure that these reports, as well as any additional comparative reports between hospitals and clinics setting out the OHP Data Set in aggregate form, have been de-identified in accordance with the CCO Deidentification Guidelines.	OHP Project Team / Privacy	N/A	3. No additional data elements included.

			3	The new funding model for Phase 2 may require a disclosure of PHI.	4. Should the funding model for Phase 2 require the disclosure of PHI to OHPs or any other parties, the OHP Project must consult with the Privacy & Access Office to ensure that the disclosure is in accordance with PHIPA and CCO's Secure Transfer of Personal Health Information Policy, Standard, and Procedures.	OHP Project Team / Privacy	N/A	4. No disclosure of PHI required.
			4	The CIRT VA identified a number of possible security weaknesses in the CIRT and proposed that certain recommendations be implemented.	5. The IT component of the OHP Project should continue to coordinate with EISO to implement the security recommendations contained in the CIRT, as well as any relevant security recommendations respecting the current CCC infrastructure upgrade.	OHP Project Team / EISO	October - December 2012	5. Project Team worked with EISO to implement recommendations.
Pilot Evaluation of Fecal Immunologic Test (FIT) in Ontario (OCSP-CCC) Phase II	Sep-27-2012	Consultant	**1**	No information is currently available as to who will have access to the PHI of FPPs that is to be reintegrated into InScreen, or the processes by which this will be done. In addition, it is important that any decisions related to the use of addresses of FPPs used for the Pilot, be made by individuals at CCO responsible for assessing address accuracy issues at the Agency level.		Project Team	Ongoing	The reintegration process currently being planned, and the Privacy & Access Office is engaged in this process.
			2	Because there is no direct contractual relationship between CCO and the lab, the labs' obligations related to PHI originally sourced from CCO, as set out in the Service agreement between the lab and the institute, are inconsistent in two important respects – breach notification and return/destruction of CCO PHI at the conclusion of the FIT Pilot – with those required of the institute in the current version of the funding agreement between the institute and CCO. There is a risk that this PHI will not be appropriately managed by the lab in these circumstances.		Privacy/Procurement	September 7, 2012.	Privacy is directly involved in the procurement process through the completion of Procurement PIAs addressing the items in this recommendation, as well as in the provision of language for RFPs. The agreement was finalized prior to Pilot Invitations being sent (Sept. 7, 2012).
			3	The manner in which the PHI of FPPs in the FIT Pilot is different from the usual process applied to that of individuals in CCC. Because Contact Centre is the point of contact for FPPs staff must be trained to respond correctly to any questions related to the confidentiality and security of the PHI of FPPs as well as how the privacy of		Privacy	October 11, 2012.	The Privacy & Access Office reviewed the Contact Centre FAQs and training materials, and provided in person training to Contact Centre staff prior to the launch.

				these individuals is protected.			
			4	The manner in which the PHI of FPPs in the FIT Pilot is different from the usual process applied to that of individuals in CCC. PPCPs and PCPs must understand this in order to respond to questions posed by FPPs. They must also understand their contractual and other privacy-related obligations as participants in the FIT Pilot. Communication of this information to the PPCPs and PCPs is necessary to manage the risk related to misunderstandings and/or concerns expressed by FPPs related to the use of their PHI in the FIT Pilot.		Privacy	September 18, 2012	Privacy reviewed the training materials.
			5	Contact Centre staff need to confirm that an individual is a FPP in order to respond accurately to questions related to the FIT Pilot. The PI or PHI necessary to 'authenticate' such individuals is yet to be determined. There is a risk that too much unnecessary information will be collected from these callers unless the requirements are established. The institute's Project Manager has also indicated that caller information will be retrieved at the conclusion of the Pilot and used in some manner. In the absence of clarity re: the nature of the information, who will have access to it, and the purposes for which it will be used, there is a risk that the PI or PHI will not be managed in accordance with CCO's obligations under the Freedom of Information and Protection of Privacy Act or PHIPA.		Project Team	October 1, 2012.	Information to be collected identified in Contact Centre SOPs for the purposes of caller authentication and verification that their physician is enrolled in the FIT Pilot.
			6	CCO will experience a privacy breach if the FIT test results of a FPP Responder are sent to the wrong individual. CCO can, to a degree, manage this risk by analyzing the results of the fulfillment house's initial address verification undertaken prior to the sending out of the Pilot Invitations to identify and resolve any systemic issues		Address Management Project Team	November 2012 - February 2013	This was considered within the address management review project; a risk measurement tool for all screening correspondence was developed and implemented.

				related to the accuracy of the addresses prior to the sending out of the Results to the FPPs.			
			7	The institute is contractually obliged to CCO to ensure that its PHIPA Agent, the lab and any of its subcontractors, such as its courier service, satisfy the institute's obligations to CCO re: the appropriate handling of PHI. CCO's awareness of the institute's failure to comply with this obligation vis a vis the lab's courier may expose it being held 'accountable' should a privacy reach occur as a result of the courier service committing a privacy breach by e.g. losing a sample of a FPP Responder.		Project Team	August 29, 2012	The agreement was completed and signed.
			8	CCO may not be in compliance with its statutory obligations under PHIPA to implement appropriate technical safeguards for the PHI that it will be providing to the institute for the purposes of the FIT Pilot		EISO	October 9, 2012	Final approval from EISO was granted prior to PHI being provided.
			9	No communications materials have been developed and made publicly available to provide FPPs with information on how their PHI is collected, used or disclosed for the purposes of the FIT Pilot.		Privacy/Project Team	October 11, 2012.	Website updates were implemented with additional privacy information, and materials were provided to Contact Centre during in-person training session.
			10	There is no process in place through which FPPs may access their PHI collected, used and disclosed for the purposes of the FIT Pilot.		Business Unit	September 2012	SOP # 06.02.04 sets out the process for access to PHI.
			11	No information is made available to FPPs related to how they may make a complaint to CCO and/or the IPC with respect to how their PHI is collected, used and/or disclosed for the purposes of the FIT Pilot.		Privacy	October 11, 2012.	Information included in materials referenced.

			12	There are no finalized procedures in place setting out how PHI is to be managed for Business Process IV "Participating PCP With No PSC Close By". In their absence, there is a risk that the PHI of FPPs involved in this process will not be collected, used etc.as required by PHIPA, the CSA Privacy Principles, and/or CCO policies.		Privacy	September 26, 2012	Process reviewed and approved by Privacy.
			13	Because the FIT Pilot SOPs for the Contact Centre have yet to be finalized, it is not possible to assesses whether the PHI of the FPPs will be collected, used etc. as required by PHIPA, the CSA Privacy Principles, and/or CCO policies.		Project Team/Privacy	October 11, 2012	SOPs finalized, reviewed by Privacy, and incorporated into Contact Centre training.
Ontario Cancer Registry Information System (OCRIS) Enterprise Data Warehouse (EDW) Migration	Sep-24-2012	Privacy Specialist	**1**	No additional privacy issues were identified within the scope of this PIA Report. Only recommendations 3 and 6 from original PIA are specifically within the scope of the Addendum. Recommendation 3 states: CCO designate a Data Steward for the EDW for requests for access to more than one data mart or for requests for access through the Person Conformed Dimension; and Recommendation 6 states: CCO conduct an assessment of the data elements required for death data set and work with data provider to eliminate or destroy any data elements that are not required. As per the CCO Privacy & Access Office PIA Implementation Plan for the PIA EDW, only recommendation 3 has been completed. Recommendation 6 is still outstanding.	CCO to ensure Recommendation 6 from the original EDW 2007/2008 is implemented. CCO needs to conduct an assessment of the data elements required for the death data set and eliminate or destroy any data elements that are not required. Project to complete this requirement by December 2012.	Project Team/Privacy	In progress.	CCO has identified the data elements that are not required and are currently negotiating with the data provider to update the data set to ensure that CCO only receives data that it requires.
Head and Neck Program - eOutcomes Project	Aug-25-2012	Privacy Analyst	**1**	It appears that FIPPA applies to CCO in its role as a prescribed entity for the eOutcomes - Head and Neck Project.	CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or the PHIPA Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a HINP; a service provider; an agent under PHIPA; a section 39(1)(c) prescribed person; and a section 45 prescribed entity.	Privacy & Access Office	27-Jul-12	On July 27, 2012, CCO's Privacy & Access Office delivered its request to the MOHLTC for a legislative amendment to PHIPA to address this legislative gap.

			2	The data holdings list appended to CCO's Privacy Policy, which is publicly available on CCO's website, will need to be updated to include a description of the Outcomes Database, including the purpose for which the outcomes data is collected, the types of information collected, the data steward assigned and the source of the information collected.	Program to advise the Privacy & Access Office when the Outcomes Database becomes a permanent CCO data holding. Once Outcomes Database becomes a permanent CCO data holding, Privacy and Access Office to update the list of Head and Neck data holdings appended to the CCO Privacy Policy, which is posted publically and maintained by the Privacy and Access Office.	Program and Privacy & Access Office	N/A	eOutcomes is currently in its pilot phase.
			3	It is the responsibility of the data steward to ensure that the list of staff members who have access to the data holdings under their control are still authorized to access that PHI.	The Outcomes Database data steward responsible for the Data Holding to review and audit the list of staff members who require access to the Outcomes PHI retained by the Program, in line with CCO's Privacy Policy.	Program	Nov-12	Data Steward has been assigned. Inventory has been completed.
			4	The Program will perform data linkages between the outcomes data and CCO's ALR database as outlined in Data Set 2a and 2b. CCO has the authority under section 45(6) of PHIPA to use PHI for the purposes for which it was collected. The Linkage of outcomes data with existing CCO data holdings is considered a "use" of the outcomes data if the purpose of the linkage is for prescribed entity health system planning and management purposes.	- Program to advise the Privacy & Access Office if and when new linkages are occurring between the outcomes data and existing CCO data holdings. Program will also advise whether a permanent data holding will be created through any such new linkages, so that a PIA or PIA Addendum can be completed for such new linkages. - Before linking outcomes data with PHI in other CCO prescribed entity data holdings, the Privacy & Access Office will review any Data Sharing Agreements (DSA) or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO.	Privacy & Access Office	Ongoing	This recommendation provides for future actions should circumstances change
			5	An inventory in line with CCO's Privacy Policy outlining the format, physical location, and time span of each data holding retained by the Project domain has not been completed.	- The data steward responsible for the Outcomes Database to establish an inventory of data retained by the Program, in accordance with CCO's Privacy Policy. - Program/data steward to advise Privacy & Access Office when all or part of the data holding is no longer required for the purposes of the	Program and Privacy & Access Office	(1) November 2012 (2) N/A	(1) Inventory complete. (2) Project is currently in its pilot phase.

					Program.			
			6	At the time of writing this PIA, the Terms and Conditions for both the eOutcomes web application and the user-signed registration form had not yet been finalized. Additionally the license agreements had not yet been executed with each RCC nor has the license agreement with the Hospital for use of the FAST sheet been executed.	- Program to execute license agreements with pilot sites prior to pilot launch and to execute license agreements with the additional eight RCCs prior to the permanent roll-out of the eOutcomes - Head and Neck Project. - Program to execute license agreement for the use of the FAST sheet with the Hospital (and any other party with intellectual property interests in the FAST sheet) prior to pilot launch.	Privacy & Access Office	12-Nov-12	Template Agreement completed and provided to program for circulation.
			7	CCO's Privacy Policy, Principle 7.4, requires that PIAs, including, as appropriate, security analyses and threat risk assessments ("TRAs"), be completed on its data holdings as required. All new data-holdings require a PIA.	- Enterprise Information Security Office shall confirm the date that the Threat Risk Assessment is completed and inform the Privacy & Access Office of the results of this Assessment. - Identification of the typical use cases with respect to access to PHI and potential threat scenarios for each use case is to be developed by the Program in collaboration with the Privacy & Access Office and EISO, in accordance with Procedure 7.5 under CCO's Privacy Policy. These threat scenarios will be used in the logging and auditing program at CCO.	EISO/Program	(1) 4/18/2013 (2) 11/23/2013	(1) Threat modeling confirmed to be completed and eOutcomes integrated with LMAS. (2) EISO confirmed completion of TRA and technical vulnerability assessment.
Diagnostic Assessment Program – Electronic Pathway Solution (DAP-EPS) Phase II	Jul-19-2012	Privacy Specialist	**1**	It is unclear whether FIPPA applies to CCO in its role as a prescribed entity for the DAP Program.	CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or the PHIPA Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a HINP; a Service Provider; an agent under PHIPA; a s. 39(1)(c) prescribed person; and a s. 45 prescribed entity.	Privacy & Access Office	27-Jul-12	As of the date of this PIA, CCO's Privacy & Access Office has completed its draft submission to the MOHLTC in support of its request for a legislative amendment to PHIPA to address this legislative gap. It will make formal submissions in July 2012.

			2	The Program has provided the data holding list to Privacy & Access Office. The data holdings list must include a description of the DAP data holding, including the purpose for which the OLIS PHI is collected, the types of information collected, the data steward assigned to the DAP data holding, and the source of the information collected. The list needs to be updated and posted publically on the CCO website.	- Privacy and Access Office to update the list of DAP data holdings appended to the CCO Privacy Policy, which is posted publically and maintained by the Privacy and Access Office. The list will be updated during the annual privacy policies review in the fall of 2012. - The Program/data steward responsible for the DAP Data Holding to review and audit the list of staff members who require access to the DAP PHI retained by the Program, in line with CCO's Privacy Policy.	(1) Privacy & Access Office (2) Program	(1) 03/01/2014 (2) 03/25/2013	(1) Privacy Policy updated. (2) Data Steward assigned and completed review
			3	The Program has noted the linkages that it intends to conduct using the data collected. However, as it completes the process of gathering the requirements for the indicators and reporting, the Program may need to conduct further linkages.	Program to advise the Privacy & Access Office if and when any linkages are occurring between the OLIS PHI and existing CCO data holdings and whether a permanent data holding will be created after any such new linkages, so that a PIA or PIA Addendum can be completed for such new linkages.	Program	N/A	Recommendation provides requirements for future and speculative linkages
			4	CCO may have data sharing agreements (DSAs) or other agreements with the Service Providers of PHI data ("data source") currently in CCO data holdings to which the OLIS PHI will be linked. It is possible that the DSAs with the data sources include limitations on the purposes for which CCO may use the source data, and therefore that CCO will not be in compliance with the DSAs with the data sources.	Before linking OLIS PHI with PHI in other CCO prescribed entity data holdings, CCO's Privacy & Access Office will review any DSAs or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO.	Privacy& Access Office	Ongoing	Recommendation provides requirements for future and speculative linkages
			5	The Program has not determined for how long the OLIS PHI will be retained in the Permanent Directory on the H Drive or in the DAP-EPS database, therefore, the Program is not able to confirm that the retention period is necessary for the fulfillment of the Program purpose.	Program to establish a retention period for the DAP data holding or external data holdings and ensure that the retention period is necessary for the fulfillment of the Program purpose. Program/data steward to advise the Privacy & Access Office when all or part of the DAP data holding is no longer required for the purposes of the Program.	Privacy & Access Office,Program.	Jul-14	PAO currently working with program on development of retention schedule.
			6	An inventory in line with CCO's Privacy Policy outlining the format, physical location, and time span of each data holding retained by the Program domain	The data steward and Program responsible for the DAP Data Holding to establish an inventory of data retained by the Program, in line with	Program	25-Mar-13	Privacy Policy updated

				has not been completed.	CCO's Privacy Policy.			
			7	Procedure 6.1 in CCO's Privacy Policy states that the Chief Information Officer is responsible for establishing data quality practices appropriate to CCO's Programs. Program area supervisors will prepare CCO data specifications for primary data collectors to adhere to when submitting data to CCO and data stewards will be responsible for implementing data quality practices.	- Program to prepare data specifications for data collectors to adhere to when submitting data to CCO and DAP data steward to be responsible for implementing data quality practices. Program to advise the Privacy & Access Office when this has been implemented. - Program in collaboration with CCO Informatics, the Privacy and Access office, eLab and eHO to outline a process for requesting clarification from eHO in situations where there are major discrepancies between the query and the data received from eHO.	(1) Program (2) Program, eHO, eLab Project team	(1) March 25, 2013 (2) N/A	(1) Data quality framework developed. Program to refine data dictionary and data methodology on an ongoing basis. (2) Project Team has not identified any discrepancies to date.
			8	Procedure 7.2 of CCO's Privacy Policy specifies that CCO will ensure that there are appropriate contracts in place with data service providers.	- Before DAP-EPS Phase II goes 'live' it must ensure that any and all Agreements between CCO and the MOHLTC with respect to the OLIS data have been finalized and successfully executed. - Although a HINP is defined as a person who provides services to two or more HICs where the services are provided primarily to HICs to enable HICs to use electronic means to disclose PHI to one another (and so not a disclosure by CCO), before the DAP-EPS Phase II goes 'live' it must ensure that any and all funding agreements which need to be renewed have been finalized and executed.	Privacy & Access Office and Legal	(1) 8/20/2012 (2) March 2013	(1) Agreements executed. (2) all agreements with HICs renewed.
			9	A security profile (TRA) and Third Party Penetration Testing with Attestation has been completed by security. The findings did not identify vulnerabilities that would exceed the target risk of low. Notwithstanding this finding, the security team at CCO is still currently reviewing the architecture for the DAP-EPS system.	The Program in consultation with EISO will inform the Privacy & Access office as to when the Architecture Review of the DAP-EPS has been completed. The Program will also provide an outcome of the review.	EISO	8-Jan-13	Approval provided by ARB.

			10	Logging and audit requirements have been built into the DAP architecture. However, a threat model which identifies the typical use cases when CCO employees can access and use PHI for the DAP-EPS Phase II has not yet been completed.	Although a threat model has been developed for DAP-EPS Phase I, it is still necessary to review the rules list with EISO and the Privacy & Access Office. As per EISO's recommendation, DAP-EPS must identify and review the typical use cases with respect to access to PHI (for Phase II) and potential threat scenarios for each use case. This must be developed by the DAP Program in collaboration with the Privacy & Access Office and EISO, in accordance with Procedure 7.5 under CCO's Privacy Policy. These threat scenarios will be used in the logging and auditing program at CCO. Identification must be completed by September 2012 and/or the DAP-EPS Phase II 'Go-live' date.	EISO	Sep-14	Integration with LMAS to be completed.
Ontario Cervical Screening Program (OCSP) Privacy notice and Result Correspondence Phase I	Jun-19-2012	Consultant	**1**	CCO is responsible for protecting PHI against loss and unauthorized use and disclosure and to advise individuals at the first reasonable opportunity if their PHI if their information is stolen, lost or inappropriately accessed. Because there is a statistical probability that there will be a privacy breach related to the volume of OCSP correspondence, Contact Centre staff must be thoroughly familiar with their responsibilities as required by the CCO Privacy Breach Management Procedure. CCO is also exposed to reputational risk in the event of a privacy breach, particularly because of the previously-experienced breach reported in IPC Oder HO-011.	1) Prior to the sending out of the OCSP Privacy Notices, all CCO Contact Centre staff should undergo refresher privacy training, focusing on breach management. This training should be delivered by the CCO ICS Privacy Specialist and, among other matters: • explicitly describe the circumstances and provide examples of scenarios that would constitute a 'privacy breach', 'suspected privacy breach' and 'privacy risk' • review the steps to be taken in the event that Contact Centre staff become aware of a 'privacy breach', 'suspected privacy breach and/or a 'privacy risk' • include a 'mock' privacy breach exercise to ensure that Contact Centre staff understand how to implement and exercise their responsibilities as required by the CCO Privacy Breach Management Procedure. 2) The CCO Contact Centre policies and procedures related to privacy matters should be finalized before the Privacy Notices are mailed in order that Contact Centre staff be properly	1) Privacy 2) Project Team/Privacy 3) Privacy 4) Contact Centre	1) July 25, 2013 2) July 31, 2013 3) June 2012 4) June 25, 2013	1) Privacy training including all items set out in recommendation delivered 2) Revisions to SOPs were made, Privacy reviewed, and training was completed 3) It was confirmed that changes to SOPs required for 2013 launch will not impact public facing website 4) Privacy Breach Management Procedure and poster as recommended confirmed available at Contact Centre work stations

					trained on the 'privacy-related' policies and procedures before they may be required to implement them in response to an OCSP-related call. 3) The Privacy & Access Office should review the final versions of the Contact Centre policies and procedures related to privacy matters to ensure that they are consistent with related CCO policies and, in particular, any public-facing policies posted on the CCO website or otherwise publicly communicated. Any required changes to these documents should be made as soon as possible in order that Contact Centre staff be trained prior to the 'go live' date of the OCSP Correspondence Program. 4) All CCO Contact Centre staff should have a copy of the CCO Privacy Breach Management Procedure available at their individual workstation, including all of the contact information for the Privacy & Access Office contact as set out in the Procedure. A poster outlining the steps that Contact Centre Staff should follow upon becoming aware of a privacy breach should be posted in a predominant position in the Contact Centre.			
			2	Individuals may contact the Service Ontario INFOline to report privacy breaches or have other privacy-related inquiries concerning OCSP correspondence. There is a risk to CCO if these matters are not addressed in a timely manner because callers may become concerned that CCO is not appropriately managing their PHI	5) FAQs related to the OCSP be prepared and distributed to Service Ontario. These FAQs should clearly identify the nature of the calls to INFOline that should be immediately transferred to the CCO Contact Centre. 6) An individual or individuals at Service Ontario should be identified as the liaison with the CCO Contact Centre contact to ensure that staff at Service Ontario clearly understand the circumstances in which callers should be directed to the CCO Call Centre.	5) Project Team 6) Project Team	5) August 7, 2013 6) August 7, 2013	5) FAQs including items in recommendation were provided to Service Ontario 6) Program briefed contact at Service Ontario 3 weeks prior to launch

			3	CCO is 'accountable' for the actions of the fulfillment house in its management of the OCSP screening correspondence. The fulfillment house's responsibilities must be clearly identified. There is a risk that the fulfillment house staff will mishandle the correspondence because: (i) their responsibilities have yet to be contractually defined; and (ii) they are not aware of or understand how they are to execute their responsibilities for the appropriate management of the cervical screening correspondence.	7) CCO should ensure that the OPF for the OCSP is completed, reviewed by the Privacy & Access Office and the Legal Department and executed prior to any data being provided to the fulfillment house for the purposes of the OCSP mailing of the Privacy Notice. 8) CCO should ensure that the fulfillment house staff are trained according to the provisions of the OPF and the Agreement prior to any data being provided to the fulfillment house for the purposes of the OCSP mailing of the Privacy Notice.	7) Project Team/Privacy 8) Project Team/Privacy	7) June 25, 2013 8) September 25, 2013	7) Privacy language on OPFs does not change - Program agreed to engage Privacy if changes required going forward 8) Annual the fulfillment house training was provided on September 25, 2013 which covered privacy requirements as per agreement, the Privacy Notice and OCSP mailings
			4	"Privacy risk" is a major element in the risk related to cervical screening correspondence. If the CCO Privacy & Access Department does not participate in the development of the cervical risk identification and mitigation framework there is a risk that the privacy risks will not be identified and appropriate risk management strategies implemented to address the privacy risks.	9) A representative of the Privacy & Access Office should be directly involved in the development of the cervical risk identification and mitigation framework to ensure that the framework addresses privacy risks and proposes an accompanying mitigation strategy for them.	9) Privacy/Project Team	9) August 7, 2013	9) Framework development began in 2012. Project documented current state of program governance as part of project activities in August 2013, including Privacy involvement.
			5	The privacy risks, including potential privacy breaches associated with the cervical screening correspondence program represent a reputational risk to CCO. If the Board of Directors is not apprised of these risks, it will be unable to respond appropriately to questions from the MOHLTC, the media and others.	10) The CCO Board of Directors should be apprised of the privacy posture of the cervical screening correspondence project as part of the Enterprise Risk Management Update to be presented to the Board in September 2012.	10) Chief Privacy Officer	10) September 27, 2012	Report of the Strategic Planning, Performance & Risk Management Committee (SPPRMC) meeting of September 12, 2012 made to CCO Board.
			6	There is a risk that more PHI than is necessary will be collected by CCO Contact Centre staff for the particular purpose.	11) The Contact Centre Policies and Procedures should explicitly enumerate the data elements to be collected from individuals wishing to: (i) opt-out of the receipt of future cancer screening correspondence; (ii) request access to or a correction of their PHI; and (iii) file a complaint and should ensure that Contact Centre policies permit the collection of the least amount of information necessary in order for these transactions to be completed.	11) Project Team/Privacy	11) June 2012	11) Contact Centre SOPs were update to address recommendation.
			7	CCO has an obligation to identify the PHI that it collects, the purposes for which it	12 A) The CCO Statement of Information Practices should be	12A) Privacy 12B) Privacy 13)	12A) June 2012 12B) June 2012	12A) Statement of Information Practices was

				uses and discloses it and how it will be retained and safeguarded. Individuals who contact the CCO Contact Centre to opt-out of screening correspondence, make an access or correction request or report a privacy breach or complaint may not understand why staff are collecting their PHI, how it will be used etc. The risk to CCO is that this lack of understanding will lead to a privacy complaint.	revised to explicitly state the type of PHI that the ICS may directly collect and use for the purposes of authenticating individuals who contact the Contact Centre to opt-out of receiving CCO cancer communications as well as individuals who seek access to or correction of their PI/PHI or wish to file a complaint. 12 B) The CCO Index of "Personal Information Banks" published pursuant to s.44 of the Freedom of Information and Protection of Privacy Act should be updated to include the PI that ICS may directly collect and use for the purposes of authenticating individuals who contact the Contact Centre to opt-out of receiving CCO cancer communications as well as individuals who seek access to or correction of their PI or wish to file a complaint. 13) The OCSP FAQs should include a specific question or questions related to this collection of information and indicate what will be done with the information after authentication is confirmed, how the information will be stored and for what length of time and the safeguards to be applied to it	Project Team	13) June 2012	revised to address recommendation 12B) Personal Information Banks were revised 13) OCSP FAQs were revised to address recommendation
			8	CCO is legally required to identify the PHI that it collects, as a prescribed entity and a prescribed registry and the purposes for which it will be used and disclosed.	14) Appendix B to the Privacy Policy should be amended to delete OCSP and move it to Appendix C. Appendix C to the Privacy Policy should be amended to include Cytobase and OBIEE in the Prescribed Registry Data Holdings. OCSP Siebel should also be added as a data holding to Appendix C. Appendix C to the Privacy Policy should be amended to include cervical screening in the Statement of Purpose for the Screening Hub – OCSR and the Screening Hub – RPDB are currently limited to colorectal screening.	14) Privacy	14) June 2012	14) Updates were made to the Privacy Policy appendices as set out in recommendation

			9	CCO needs to ensure that any individual who purports to be the SDM of another has the requisite legal authority to act on behalf of another individual for all of the activities conducted by the Contact Centre.	15) The SDM Registration Policy should be reviewed by the CCO Privacy & Access Office and Legal Services to ensure that its scope is sufficient to include all Contact Centre activities in which SDM registration may be required.	15) Privacy/Legal	15) June 2012	15) The SDM process/form were reviewed and updated by Privacy and Legal
			10	CCO does not appear to have clear legal authority under PHIPA to use and disclose PHI as is necessary for the effective operation of the OCSP cervical correspondence program.	16) The CCO Privacy & Access Office should move forward as soon as possible with its strategy and work plan to pursue its 2012 goal to resolve the potential conflict between the application of PHIPA and FIPPA through a change to the regulation that applies to CCO as a prescribed registry.	16) Privacy	16) December 2012	16) See "CCO Privacy Impact Assessments as a Prescribed Registry - General Addendum: Revised Authorities Analysis - Section 49(1) of PHIPA", December 2012
			11	CCO staff may inappropriately access the new data sets created as a result of the OCSP cervical screening program.	17) The Data Steward for the OCSP should review the CCO Data Steward: Terms of Reference to ensure that they understand their responsibilities related to access to the new OCSP data holdings prior to the OCSP going live.	17) Project Team	17) August 9, 2013	17) Data Steward (Vickie Welsh) acknowledged she was up to date on current terms of reference.

			12	If CCO does not formally manage data quality issues related to the PHI used for the OCSP screening program, there is an increased risk of a privacy breach.	18) As required by the DSA, CCO should assign an individual to be responsible for chairing the Joint Review Committee (JRC) to manage all issues related to the quality of the data received from the laboratories pursuant to this agreement. The individual that chairs the JRC should also be a member of CCO's internal data quality committee established to address data quality issues related to the receipt of Cytology data pursuant to the DSA. 19) The internal CCO committee established to address data quality issues related to Cytology data should have a clearly defined mandate to include, at minimum. such matters as: (i) a process for defining what constitutes a "data quality issue"; (ii) identifying an individual(s) who has the responsibility for identifying, investigating and taking remedial action on such issues; (iii) development of a reporting process to ensure that the individual responsible for managing data quality issues is advised on a timely basis, outside of the scheduled meetings; (iv) ongoing review of CCO's data linkage rules and data validation processes. This committee should have representation from the CCO Informatics, Privacy & Access, PCCIP, Surveillance and the Cervical Screening Program departments. 20) CCO should develop a method to track reported data quality issues so that patterns of poor data quality may be identified and resolved at an early stage before they create systemic issues and increase the risk of privacy breaches.	18) Program 19) Program 20) Program	18) August 7, 2013 19) In progress 20) May 1, 2013	18) Project documented current state of program governance as part of project activities 19) Privacy engaged in data quality committee to provide input into revised terms of reference 20) Tracking mechanism initiated and reported in project reporting
			13	If CCO does not formally manage data linkage issues related to the PHI used for the OCSP screening program, there is an increased risk of a privacy breach	21) Recommendation #9 from the 2011 ICS PIA should be implemented by assigning an individual from the Privacy & Access Office to sit as a permanent member of the internal	21) Privacy	21) July 2013	21) Privacy appointed as permanent member of the Cytobase Data Quality Working Group

					CCO committee established to address data quality issues related to Cytology data (as described in Recommendation #19 of this PIA).			
			14	There is a risk that the factors leading to the Privacy Notices being sent to and/or received by an individual for whom they were not intended will not be assessed and, where possible, resolved, prior to the Results being communicated. This may lead to the Results being sent to individuals who are not the intended recipients, a potentially avoidable breach if a "root cause" assessment had been conducted prior to their mailing.	22) After the Privacy Notices have been mailed and the fulfillment house has reported to CCO on the number returned, those sent to an incorrect address or otherwise undeliverable, the OCSP Program, in conjunction with the Privacy & Access Office, the fulfillment house and the Informatics Department should, prior to the sending out of any Results, conduct an assessment to identify the root causes and/or systemic issues that have led to the Privacy Notices not being delivered to individuals who have been identified as Eligible Participants. The OCSP Program should ensure that any issues identified as a result of this assessment have been appropriately managed prior to the sending of any Results correspondence.	22) Program/Privacy/informatics	22) July 15, 2013	22) Address Management Risk Assessment, monitoring procedures, and privacy breach process established and implemented in Evaluation & Reporting Unit.
			15	The risk of PHI being sent to an individual for whom it was not intended is dependent upon a number of factors which go to making a decision on whether the information may be communicated in electronic or paper format. CCO may implement inconsistent processes for the transmission of PHI in the same or similar situations.	23) The Interim Guidelines for the Secure Transmission of PHI should specifically address the factors to be taken into account when assessing the risk when sending PHI in electronic and paper format as required by the Manual.	23) Privacy	23) June 2012	23) Addressed in CCO's Secure Transfer Policy, Standard and Procedures approved in June 2012
			16	The technical security safeguards of InScreen™ need to be assessed in a complete TRA to avoid the risk of CCO experiencing a privacy breach related to insufficient technical controls on the system.	24) A TRA should be conducted on InScreen™ during the fiscal 2012-2013 in order to ensure that any security risks are identified and managed prior to the system being used to support additional ICS programs. Given the next major planned release for October, 2012, the TRA should be completed after the release prior to the updated system being used.	24) EISO	24) June 6, 2013	24) TRA completed on InScreen
			17	The security documentation prepared by the EISO could provide clearer direction to internal CCO clients with respect to when different types of security assessments will	25) As part of its overall privacy and security policy review, CCO should review the EISO security documentation to	25) EISO	25) Ongoing	25) EISO considers enhancements such as set out in this recommendation as part of its overall security

				need to be conducted on their initiatives.	consider enhancements related to its criteria for undertaking different types of security assessments.			policy reviews
			18	CCO is not being completely transparent with respect to how it collects, uses and discloses PHI for the purposes of OCSP cervical screening.	26) CCO should ensure that prior to the go-live date of the OCSP all of the related documents that support the Openness Principle 8.1 have included specific references to OCSP and are made available to the public on the CCO website or though other mechanisms that are currently used. Specifically, the Privacy FAQs should be updated to: (i) cross reference the ICS FAQs; (ii) include support for the OCSP as a use of PHI (s.7B. at p. 5); (iii) add one new question: 'What is CCO's role in relation to the Ontario Cervical Screening Program?' (at p. 6); (iv) expand the answers to Question #16- "What if I don't want my information to be shared with CCO?" to include an individual's choice not to participate in the OCSP; #18 – "Can I see the information CCO collects on me?" to include a reference to accessing records related to OCSP and the CCO contact information for doing so; #21 – "How does CCO protect my information?" – by referencing the IPC's 2011 review of CCO's information practices.	26) Privacy	26) June 2012	26) Privacy FAQs were updated to address recommendation.
			19	Individuals who seek access to their PHI collected, used or disclosed for the purposes of the OCSP may not be clear on how they may exercise this right.	27) The ICSR Data Request Procedure should include a section on the procedure to be followed when an individual requests access to their OCSP PHI stored in the OCSR. It should incorporate and be consistent with the data access process followed by the CCO Contact Centre when the request is made to the Centre.	27) Privacy	27) June 2012	27) The ICSR Data Request Procedure was updated to address this recommendation.
			20	Individuals who wish to make a complaint related to how their PHI is collected, used or disclosed for the purposes of the OCSP may not be clear on how they may exercise	28) The Privacy-related FAQs being developed for the OCSP should include information on how individuals may make complaints related to how their	28) Privacy	28) June 2012	28) Privacy-related FAQs include this information.

				this right.	PHI is managed for the purposes of this program.			
New Drug Funding Program eClaims	Jun-10-2012	Chief Privacy Officer	**1**	No Risks Identified	The Program, in consultation with CCO's Privacy & Access Office and CCO's Legal Department, build into the Terms of Use for the e-claims application as well as into the License Agreement between CCO and the hospitals for use of the application environment, provisions which clearly specify for all participating hospitals their agreement and direction to CCO to make available a patient's treatment history, to the clinicians(s) subsequently providing care and requesting reimbursement through the NDFP on behalf of the same patient . The e-claims tool must restrict access only to those clinicians within a patient's "circle of care," recognizing that this "circle" may span years of treatment given the chronic nature of cancer care. The Terms of Use and License Agreement shall provide that CCO will act on this direction as the "agent" for the hospitals as part of its provision of the services of the e-claims tool.	Privacy & Access Office, Legal and Program	Dec-12	eClaims Software License Agreement (Section 9(e) - Agent provision). Schedule "D" Website Terms and Conditions of Use (PDRP Privacy Statement).
			2	No Risks Identified	The Program, in consultation with CCO's Privacy & Access Office, should provide notice to the public through its public disclosure channels, for example, CCO's Statement of Information Practices, the NDFP Statement of Purpose (included in CCO's Privacy Policy) as to the intended disclosure of a patient's NDFP treatment history to hospitals requesting reimbursement through the NDFP.	Privacy & Access Office, Program	Nov-12	Privacy Policy updated and FAQs (HINP) drafted.
			3	Given the legislative gaps, there is some uncertainty as to whether FIPPA applies to CCO in its role as a HINP and prescribed entity for the NDFP.	CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or its Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a	Privacy & Access Office	27-Jul-12	On July 27, 2012, CCO's Privacy & Access Office delivered its request to the MOHLTC for a legislative amendment to PHIPA to address this legislative gap.

					HINP; a service provider; an agent under PHIPA; a ss. 39(1)(c) prescribed person; and a ss. 45 prescribed entity.			
			4	The NDFP will disclose de-identified record-level data to the MOHLTC in response to questions about an individual's interaction with the NDFP. The purpose of the disclosure to MOHLTC is to provide PHI about a patient to MOHLTC. While the NDFP removes the patient's identifying information prior to disclosure, it is reasonable to conclude that the recipient is able to link the disclosed data to an identifiable patient. It is unknown under what PHIPA authority the MOHLTC collects an individual's PHI related to the EAP and discloses this information to CCO as part of its consultations. It is recommended that the Program seek clarity from the MOHLTC as to its authority to request this information from CCO. For example, it may be the case that the MOHLTC manages these requests on a consent basis which consent could include direction to the MOHLTC and CCO to provide the patient's PHI as part of the claims adjudication process.	While it is noted that CCO does not disclose PHI to the MOHLTC, it would be prudent for the NDFP to seek clarity from the MOHLTC as to its authority to request this information from CCO.	Privacy & Access Office, Legal	Sep-12	CCO has obtained/reviewed the EAP Physical PIA (October 2011) from the MOHLTC. There were no outstanding concerns.
			5	The NDFP Business Requirements Document makes provision for the secure collection and disclosure of PHI with the MOHLTC – see Data Flow # 4 above. At present, there is no agreement for the exchange of PHI with the Ministry for purposes of the NDFP (assuming that the appropriate PHIPA authorities are in place).	(i) The Program ensure that CCO executes Agreements with the Hospitals related to the operation of the NDFP; (ii) The Program ensure that CCO executes License Agreements with hospitals prior to granting access to the e-claims tool. The License Agreement should provide the direction and agreement regarding access to a patient's prior treatment history as noted in Recommendation #2 above; (iii) CCO complete an agreement with the MOHLTC (or amend the existing funding agreement) for the collection and disclosure of NDFP PHI assuming that PHIPA authorities are in place.	Program, Legal	(1) December 2012 - January 2013 (2) December 2012 - January 2013 (3) N/A	(1) eClaims Software License Agreement - Schedule B (2) eClaims Software License Agreement (3) Program relying on larger CCO/MOHLTC Accountability Agreement

			6	NDFP data is being linked with systemic therapy data as part of an overall initiative from CCO's Informatics. CCO's Privacy and Access Office was not aware of the linkage.	The NDFP to advise the Privacy Office if and when new linkages occur between the PHI in the NDFP Data Holding and existing CCO data holdings and whether a permanent data holding will be created after any such new linkages, so that a PIA or PIA Addendum can be completed for such new linkages, as per CCO's PIA Policy.	Program	N/A	Recommendation provides requirements for future and speculative linkages
			7	NDFP data is being linked with systemic therapy data as part of an overall initiative from CCO's Informatics. CCO's Privacy and Access Office was not aware of the linkage.	Before linking PHI in the NDFP Data Holding with PHI in other CCO prescribed entity data holdings, CCO's Privacy Office will review any data sharing agreements or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO.	Program	N/A	Recommendation provides requirements for future and speculative linkages
			8	A TRA that identifies the threats, vulnerabilities and risks to the security and integrity of PHI has not been completed	CCO's EISO complete a TRA to ensure that the NDFP services provided by CCO to HICs are done so in a secure manner in accordance with CCO's information security policies and procedures.	EISO	May-13	TRA was completed and identified risks were mitigated.

			9	No Risks Identified	Given the recent introduction of new drug and other treatment reimbursement programs at CCO, and the proposed changes to the NDFP as reviewed in this PIA, it is recommended that the CCO Privacy & Access Office, in consultation with the Clinical Programs Office and the MOHLTC, complete a review of the privacy authorities for all CCO reimbursement programs including: the NDFP; the Evidence Building Program (EBP); the Case-by-Case Review Program (CBCRP), the Brachytherapy Reimbursement Program and the Ontario Positron Emission Tomography Scan Evidence-Based Program (EB-PET Program) to: (i) ensure that a consistent authorities approach is applied to all CCO reimbursement programs (which may translate into an omnibus operations agreement with participating hospitals); (ii) address issues related to the secure method of transferring PHI among the participants of the reimbursement programs; and (iii) address issues related to disclosure by CCO of PHI to external decision makers (e.g. MOHLTC). This review should take place prior to the planned transition of the manual components of the EBP and CBCRP into the NDFP e-claims application.	Legal , Privacy & Access Office	Oct-12	GC & CPO confirmed that a review will not be required. All transfers of PHI are in accordance with the Secure Transfer of PHI Policy and approved by EISO. Legal review of one reimbursement conducted to ensure that it is consistent with general administrative law principles. Review concluded a CCO-MOHLTC DSA required concerning all reimbursement programs only.

Integrated Cancer Screening Secure Messaging Solution	May-31-2012	Consultant	**1**	The Secure Messaging Solution will require ongoing strategic and operational governance to ensure that it meets the needs of CCO's ICSP stakeholders, and that its associated privacy controls are adequately protecting the full scope of PHI it delivers.	1) CCO should develop terms of reference for the strategic and operational governance of the Secure Messaging Solution, and include these in relevant program charters. These terms should include ongoing review of Solution privacy controls.	CIO	October 1, 2012.	The governance structure for the build of the Secure Messaging Solution is currently in place, which consists of the Sponsor's Committee, Secure Messaging Working Group, and Secure Messaging IT Working Group where Privacy provides relevant inputs and controls. The governance structure for future use of the Secure Messaging Solution will be determined and implemented by CCO's Chief Information Officer. Terms of reference will include ongoing review of privacy controls.
			2	CCO does not have an agreement in place with eHealth Ontario for ONE ID services	2) CCO should establish its agreement with ONE ID for the registration, authentication and identity management services related to the Secure Messaging Solution; the agreement should include the terms and shared processes through which end user access to the Solution will be revoked by ONE ID.	Legal	June 15, 2012	CCO's Legal department finalized the agreement with eHealth Ontario.
			3	Terms of Service do not fully address privacy and security responsibilities of end users	3) CCO should include provisions in the Terms of Service that obligate PEM physician end users to notify CCO and/or ONE ID when the PEM physician, or her or his delegate, no longer requires access to the Solution. (see sections 5.5.2 and 5.7.3.2 below for related recommendations). 4) CCO should take measures to increase the likelihood that end users will understand and accept the Terms Service, including but not limited to: • The terms of service should be copy-edited for length • Privacy and security provisions should be formatted so that they are easy to identify in the click-through agreement	3) Privacy 4) Privacy	3) June 15, 2012 4) June 15, 2012	3) Revised terms of service drafted and provided to project team 4) Same comment as # 3

					• The Terms of Service in their entirety should be formatted for readability and ease of scanning • End users should be able to print out the Terms of Service using a prominent Print button.			
			4	CCO has no description of the obligations to which it binds Secure Messaging end users in its consolidated statement of information practices for the ICSP. Such a description would provide assurance to members of the public and other stakeholders regarding the extent of CCO's privacy protections related to the CCC and ICSP.	5) CCO should include in its consolidated statement of information practices for the ICSP a description of the obligations to which it binds Secure Messaging end users.	Privacy	Oct-12	Compliance expectations are addressed in the SAR FAQs available of CCO's public website.
			5	CCO has not completed the Training and Education Plan or training materials for end users of the Secure Messaging Solution	6) CCO should complete the Training and Education Plan, and include in the plan milestones for the development, piloting and deployment of training materials. The Plan should also include a consultation strategy to collect feedback on training materials from providers within the group expected least likely to use the Secure Messaging Solution.	CCC	May 2, 2012	The solution User Guide (integrated with the SAR itself) is the primary training tool. The User Guide has been completed and was tested with physicians. Feedback was reviewed by the project team and Privacy.
			6	CCO has not provided statements of purpose for the data elements in the SARs that has been developed and maintained by a CCO data steward as part of CCO's information governance framework.	7) The relevant CCO business unit should develop the statements of purpose for the SAR elements; the responsibility for these statements of purpose should be assigned to a CCO data steward.	CCC	June 15, 2012	Statements of purpose were confirmed with the program.
			7	End users do not explicitly agree to use SARs only for the purposes for which they are provided	8) CCO should include a provision in the Solution Terms of Service requiring end users to agree that any PHI disclosed to them through the Solution will be used only for the purposes for which it was provided.	Privacy	June 15, 2012	Revised terms of service drafted and provided to project team
			8	CCO has not developed controls to support limiting the scope of disclosure to delegates	9) CCO should provide end users with a reminder in the Terms of Service to appropriately limit the access of any delegates to SARs. This reminder should also be provided in the end user training.	Privacy/CCC	June 15, 2012	Revised terms of service drafted and provided to project team. Also added to User Guide.

			9	CCO has not developed controls to support timely revocation of delegate credentials when a delegate leaves or is dismissed from a practice.	10) The Terms of Service should remind end users that delegate credentials must be revoked by a PEM physician as soon as possible after a delegate leaves a practice, and that each PEM physician end user should consider it her or his responsibility to revoke these credentials for any of her or his delegates, regardless of what other physicians the delegate may act for. See sections 5.1.3.2 and 5.7.3.2 for related recommendations.	Privacy	June 15, 2012	Revised terms of service drafted and provided to project team
			10	Unauthorized access. Due to the sensitive nature of the recommendation, CCO has excluded some of the details from the public version of this report, however these have been provided to the IPC.	11) Refer to TRA for recommended technical controls. 12) Finalize implementation of Logging, Monitoring and Auditing processes in respect of Secure Messaging solution.	11) EISO 12) EISO	11) June 2012 12) June 2012	11) Please see TRA Mitigation Plan developed by EISO 12) Logs were integrated with CCO's Logging, Monitoring and Auditing System to ensure ongoing monitoring and event correlation to detect and respond to potential incidents. eHealth Ontario's OneID also has its own logging, monitoring and auditing standards.
			11	Unauthorized access. . Due to the sensitive nature of the recommendation, CCO has excluded some of the details from the public version of this report, however these have been provided to the IPC	13) Training of physicians to address this issue. 14) Provide physicians with relevant information to identify unauthorized access...	13) CCC 14) IT	13) June 1, 2012 14) October 201	13) Included in User Guide 14) Implemented in User Guide in Q2-3 release of SAR
			12	Unauthorized access. Due to the sensitive nature of the recommendation, CCO has excluded some of the details from the public version of this report, however these have been provided to the IPC	15) Provide physicians with relevant information to identify unauthorized access.	IT	N/A	As the identity provider, eHealth to address this recommendation.
			13	Registration exceptions – use of video ONE ID Identity Assurance Standards do not recognize remote video as an acceptable alternate for registration of users at the required level (they call for involvement of a Notary Public).	16) Obtain approval from ONE ID as to the acceptability of proposed registration process when face-to-face registration of physicians is not practicable.	OneID	N/A	98% of registrations will be done face-to-face. Video is required only for 2% of hard-to-reach physicians. Because video is a new approach, it is not in OneID's current policy. Registration process is currently under review with

								eHealth.
			14	The FOBT privacy insert does not indicate to potential CCC participants that: • participants can request access and corrections to their PHI in the OCSR • CCO has developed an Inquiries and Complaints Procedure for the Integrated Cancer Screening Program	17) The FOBT privacy insert should be updated at CCO's first opportunity to note that: a. participants can request access and corrections to their PHI in the OCSR b. there is an Inquiries and Complaints Procedure specific to the CCC (as a part of the CCO ICSP). This information should also be posted on the CCC web site.	CCC/Privacy	June 2012	Updated website listed on current FOBT kit with up to date information on privacy, information practices, contact information, etc. Insert to be updated in 2013/14.
			15	The ICSP Inquiries and Complaints Procedure is not available on the CCC Privacy section of the CCO public web site.	18) CCO should post the ICSP Inquiries and Complaints Procedure in a prominent place in the CCC Privacy section of the CCO public web site.	Privacy	June 2012	Updated procedure posted to website.
Ontario Renal Network (ORN)	May-29-2012	Privacy Specialist	**1**	It is unclear whether FIPPA applies to CCO in its role as a prescribed entity for the ORN Program.	1) CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or the PHIPA Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a HINP; a Service Provider; an agent under PHIPA; a s. 39(1)(c) prescribed person; and a s. 45 prescribed entity.	Privacy & Access Office	27-Jul-12	On July 27, 2012, CCO's Privacy & Access Office delivered its request to the MOHLTC for a legislative amendment to PHIPA to address this legislative gap.
			2	Sufficient notice must be given to all Service Providers to ensure they are fully apprised of the requirement to transfer PHI through Tumbleweed and not fax.	2) Program and Privacy & Access Office to work together to develop a Notice for each Service Provider. The Notice will outline the importance of transferring PHI from the Service Provider to CCO by way of Tumbleweed and include the reasons for doing so. The Program and the Privacy & Access Office should provide the Notice to all Service Providers by July 1, 2012.	Program and Privacy & Access Office	Jul-12	Notice provided prior to data submission to points of contact at the provincial CKD programs.
			3	The Program has provided the data holding list to Privacy & Access Office. The data holdings list must include a description of the ORN data holding, including the purpose for which the ORN PHI is collected, the types of information collected, the data steward assigned to the ORN data holding, and the source of the information collected. The list needs to be updated and posted publically on the CCO website.	3) Privacy and Access Office to update the list of ORN data holdings appended to the CCO Privacy Policy, which is posted publically and maintained by the Privacy and Access Office. The list will be updated during the annual privacy policies review in the fall of 2012.	Privacy & Access Office	Oct-12	Data holding added

			4	The Program has noted the linkages that it intends to conduct using the data collected. However, as it completes the process of gathering the requirements for the indicators and reporting, the Program may need to conduct further linkages.	4) Program to advise the Privacy & Access Office if and when new linkages are occurring between the ORN PHI and existing CCO data holdings and whether a permanent data holding will be created after any such new linkages, so that a PIA or PIA Addendum can be completed for such new linkages.	Program	N/A	Recommendation provides requirements for future and speculative linkages
			5	CCO may have data sharing agreements (DSAs) or other agreements with the Service Providers of PHI data ("data source") currently in CCO data holdings to which the ORN PHI will be linked. It is possible that the DSAs with the data sources include limitations on the purposes for which CCO may use the source data, and therefore that CCO will not be in compliance with the DSAs with the data sources.	5) Before linking ORN PHI with PHI in other CCO prescribed entity data holdings, CCO's Privacy & Access Office will review any DSAs or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO.	Privacy & Access Office	N/A	Recommendation provides requirements for future and speculative linkages
			6	The Program has not determined for how long the ORN PHI will be retained in the Permanent Directory on the H Drive or in the ORN database, therefore, the Program is not able to confirm that the retention period is necessary for the fulfillment of the Program purpose.	6) Program to establish a retention period for the ORN data holding or external data holdings and ensure that the retention period is necessary for the fulfillment of the Program purpose. Program/data steward to advise the Privacy & Access Office when all or part of the ORN data holding is no longer required for the purposes of the Program.	Program	N/A	Program to advise PAO when all or part of the ORN data holding is no longer required.
			7	An inventory in line with CCO's Privacy Policy outlining the format, physical location, and time span of each data holding retained by the Program domain has not been completed.	7) The data steward and Program responsible for the ORN Data Holding to establish an inventory of data retained by the Program, in line with CCO's Privacy Policy.	Program and Data Steward	6/1/2013	Complete.
			8	Procedure 6.1 in CCO's Privacy Policy states that the Chief Information Officer is responsible for establishing data quality practices appropriate to CCO's Programs. Program area supervisors will prepare CCO data specifications for primary data collectors to adhere to when submitting data to CCO and data stewards will be responsible for implementing data quality practices.	8) Program to prepare data specifications for data collectors to adhere to when submitting data to CCO and ORN data steward to be responsible for implementing data quality practices. Program to advise the Privacy & Access Office when this has been implemented.	Program	Jun-12	Data specifications and QA for ORN data to be submitted

			9	Determination to be made as to whether full TRA is required.	9) Program to work with security to ensure that safeguards in this system are in place. At present the system is being designed in accordance with security standards and the proposed transfer approach is on the (draft) list of approved PHI transfer mechanisms. Security will provide the program for a list of safeguards and any identified risks as the project progresses. Program, in consultation with the EISO will also confirm with Privacy whether a TRA is required. If a TRA is not required, Program will provide Privacy with the reasoning behind the decision. Notwithstanding the completion of a Security Profile in 2010, the Program, in consultation with the EISO will also inform Privacy & Access office as to whether a TRA is required. If a TRA is not required, program will provide privacy with the reasoning behind the decision.	Program and EISO	Jun-12	EISO provided security requirements for ORRS Release 3 and manual collection of data.
			10	Logging and audit requirements have been built into the ORN solution architecture. However, a threat model which identifies the typical use cases when CCO employees can access and use PHI, has not yet been developed.	10) Identification of the typical use cases with respect to access to PHI and potential threat scenarios for each use case is to be developed by the ORN Program in collaboration with the Privacy & Access Office and EISO, in accordance with Procedure 7.5 under CCO's Privacy Policy. These threat scenarios will be used in the logging and auditing program at CCO. Identification to be completed by July 2012.	Program and EISO	Jun-12	Complete.
			11	Logs need to be integrated with a monitoring or auditing system. Creating the threat modeling by itself does not change the state of the logs; it needs to be followed by an implementation step in which the application logs are parsed and integrated with LMAS, and rules need to be defined to trigger alerts for scenarios identified in the threat model. Integration with CCO's Logging and Monitoring program has not yet been finalized.	11) Program to become integrated with CCO's Logging and Monitoring program. Implementation will require integration with ArcSight, and rules need to be defined to trigger alerts for scenarios identified in the threat model. These threat scenarios will be used in the logging and auditing program at CCO. Integration requires a team effort involving, the Privacy & Access Office, EISO, Security Operations and the ORN Program.	Program and EISO	Jun-12	Complete.

					Integration to be completed by July 2012.			
Integrated Cancer Screening (ICS) Program – Release 3.0	Mar-20-2012	Privacy Specialist	**1**	It is possible that system vulnerabilities resulting from the implementation of ICS Release 3.0 may be identified during the TRA process. The TRA may not be complete prior to ICS Release 3.0 going live.	1) CCO's EISO must confirm that substantive technical safeguards are in place prior to ICS Release 3.0 going live. 2) The TRA for ICS Release 3.0 must be finalized and all the recommendations set out therein must be implemented.	1) EISO 2) EISO	1) March 19, 2012 2) March 28, 2012	1) EISO confirmed adequate safeguards were in place 2) EISO confirmed that risks were being managed prior to implementation
Ontario Breast Screening Program (OBSP) Interval Cancer Review (ICR)	Mar-12-2012	Privacy Specialist	**1**	It is not clearly documented whether the Hub is acting as an Affiliate Site's agent under PHIPA.	It is recommended that OBSP staff directly request the MMs from the Affiliate Sites, rather than through the Hubs.	Business Unit	March 2012	Communication through the Hubs was halted as of March 2012, and MMs were requested directly from Affiliated Sites.
			2	Transferring a hard copy list of OBSP interval cancer cases via courier is not in accordance with privacy and security best practices as identified by HO-011, recently issued by the IPC.	It is recommended that the methods chosen to transfer PHI to external parties for the ICR process be approved by the EISO and the Privacy & Access Office to ensure the options are in compliance with evolving privacy and security best practices.	Business Unit / EISO / PAO	May 15, 2012	The PAO and EISO worked with the OBSP to identify the approved options for transferring PHI to external parties for the ICR process. Secure Managed File Transfer protocol was initiated, and when electronic transfers were not possible (for non-digitized mammograms), courier transfer with additional controls was advised.
			3	The CDs prepared by the Affiliate Site and transferred to CCO are unencrypted; there are original analogue MMs containing PHI included in the package sent to CCO via courier. The method of transfer and format of the records with the package is not in accordance with privacy and security best practices, as indicated by HO-011.	It is recommended that the OBSP work with the Privacy & Access Office and the EISO to ensure a secure methods of transfer of PHI by external parties to CCO for the ICR process.	Business Unit / EISO / PAO	May 15, 2012	The PAO and EISO worked with the OBSP to identify the approved options for collecting PHI from external parties for the ICR process. Secure Managed File transfer protocol was initiated, and when electronic transfers were not possible (for non-digitized mammograms), courier transfer with additional controls was advised.

			4	Of particular concern is the collection of original analogue MMs which are intended to be used for ongoing clinical care. These records contain unencrypted PHI. Moreover, these records, if lost, pose a risk to CCO as these records are originals, which cannot be replaced, and form part of the medical history of a patient.	It is recommended that the ICR cease to collect original analogue MMs until such time as the Chief Privacy Officer of CCO grants explicit written approval to the continued collection of such records.	Business Unit / CPO	May 15, 2012	CPO granted approval for collection of analogue MMs via new secure transfer procedure. Privacy provided written approval/instructions to business unit.
			5	To date CCO has not entered into an agreement with the ICR radiologists to carry out the quality assurance work on behalf of CCO.	It is recommended that the OBSP work with the Privacy & Access Office and the Legal Department to finalize the agreements before the next review.	Business Unit / PAO / Legal	June 24, 2011	Agreements between CCO and radiologists for purposes of the ICR are now in place.
			6	At the time of drafting this PIA, the method of transferring the electronic records was not finalized.	It is recommended that the methods chosen to transfer PHI to external parties for the ICR process be approved by the EISO and the Privacy & Access Office to ensure the options are in compliance with evolving privacy and security best practices.	Business Unit / EISO / PAO	May 15, 2012	The PAO and EISO worked with the OBSP to identify the approved options for transferring PHI to external parties for the ICR process. Secure Managed File Transfer protocol was initiated, and when electronic transfers were not possible (for non-digitized mammograms), courier transfer with additional controls was advised.
			7	To date the OBSP communicates and collects additional information from sites that have a secure managed file transfer mechanism. The OBSP is waiting until a secure managed file transfer mechanism is in place with the remaining sites to collect additional digital and digitized information.	It is recommended the OBSP confirm to the Privacy & Access Office once all Affiliate Sites are provisioned with secure managed file transfer accounts.	Business Unit	April 19, 2012	To be completed by June 2012.
			8	It is not clearly documented whether the Hub is acting as an Affiliate Site's agent under PHIPA.	It is recommended that CCO send original analogue MMs back to the Affiliate Site that originally provided it, rather than through the Hubs.	Business Unit	March 2012	CCO no longer sends back original mammograms through the Hub. These are sent directly to the Affiliate Site.
			9	The Privacy & Access Office provided briefing notes (see Appendix B and C) to the OBSP regarding (a) CCO's authority under s. 13(2) of PHIPA O.Reg 329/04 to return the original analogue MMs to the Sites in light of HO-011 (b) the options for returning original analogue MMs via courier.	It is recommended that the OBSP implement the recommendations set out in the briefing notes regarding the return of original analogue MMs (See Appendix B and C).	Business Unit	March 12, 2012	OBSP confirmed briefing note recommendations will be implemented.

			10	To date CCO has not entered into an agreement with volunteer radiologists on the review panel team to carry out the quality assurance work on behalf of CCO.	CCO should enter into agreements with all volunteer radiologists on the review panel team. The agreements in place should stipulate that the volunteer radiologists agree to carry out the work on the ICR process on behalf of CCO.	Business Unit	June 24, 2011	Agreements between CCO and radiologists on the review panel team were put in place.
			11	The OBSP has proposed couriering hard copy reports, sending encrypted CDs by courier or using a secure managed file transfer mechanism.	It is recommended that the OBSP work with the Privacy & Access Office and EISO to find the most appropriate method for transferring the report.	Business Unit / EISO / PAO	March 12, 2012	OBSP will send reports by encrypted device or secure managed file transfer protocol.
			12	As a PE, CCO is authorized to collect PHI from HICs, without the consent of the patient, and use such data for health system planning and management purposes. As CCO operates the OBSP, which includes the operation of the ICR view process, as a PE it is not clear why consent is obtained.	It is recommended that, as part of the re-design of the OBSP within the Integrated Cancer Screening Program, the OBSP together with CCO's Privacy & Access Office review whether the current consent model should be changed.	Business Unit / PAO	March 2014	Consent model for OBSP was changed as OBSP transitioned from a PE to PR in March 2014 in order to initiate OBSP correspondence. A PIA was completed on this.
Colonoscopy Interim Reporting Tool (Out-of-Hospital Premises Project Phase I)	Mar-06-2012	Privacy Manager	**1**	The OHPs are not explicitly named in PHIPA as a category of "HICs" in the same manner as hospitals.	1) The OHP Project must identify the nature of the legal entity representing each participating OHP (e.g., a corporation, or a partnership of physicians). 2) Each OHP Agreement must contain the following representations and warranties by the OHP: (a) the legal entity representing the OHP in the OHP Funding Agreement is a HIC under PHIPA, (b) such legal entity is in compliance with its obligations as a HIC, (c) such legal entity has the authority to collect and use the colonoscopy data that will be disclosed to CCO under the funding agreement, and (d) such legal entity has the authority to disclose such data to CCO as a prescribed registry under PHIPA.	Legal Counsel, Privacy & Access Office	1-Feb-12	Legal prepared two versions of the funding agreement: one for incorporated entities and another for unincorporated entities (e.g., partnerships). Funding Agreement had an effective date of February 1, 2012 and contained the representations and warranties in Section 3.1.
			2	The OHP Project may send monthly reports to the OHPs setting out the OHP Data Set in aggregate form. Aggregate data that has not been properly deidentified may potentially contain PHI.	3) If the OHP Project decides to send monthly reports to the OHPs setting out the OHP Data Set in aggregate form, the OHP Project will consult with the Privacy & Access Office to ensure that this aggregate data has been properly deidentified in accordance with the CCO Deidentification Guidelines.	Project Manger for CIRT OHP Project	N/A	Recommendation not carried out because such monthly reports were not sent.

			3	The CIRT VA identified a number of possible security weaknesses in the CIRT and proposed that certain recommendations be implemented.	4) The IT component of the OHP Project should coordinate with EISO to implement the security recommendations contained in the CIRT VA.	Project Manger for CIRT OHP Project	25-Jan-12	On January 25, 2012, EISO confirmed that the project may proceed because "CIRT risks are being appropriately managed."
Survivorship Colorectal Cancer Pilot (SCRCP)	Feb-27-2012	Privacy Analyst	**1**	It is unclear whether FIPPA applies to CCO in its role as a prescribed entity for the SCRCP	CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or the PHIPA Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a HINP; a service provider; an agent under PHIPA; a s. 39(1)(c) prescribed person; and a s. 45 prescribed entity.	Privacy & Access Office	27-Jul-12	On July 27, 2012, CCO's Privacy & Access Office delivered its request to the MOHLTC for a legislative amendment to PHIPA to address this legislative gap.
			2	The Program has not yet assigned a data steward for the SCRCP data holding, which includes the Tumbleweed Directory on H Drive, (where the SCRCP PHI is retained).	The Survivorship Program to assign a data steward prior to the collection of PHI from the facilities and notify the Privacy & Access Office when this has been completed.	Program	Aug-12	Data Steward has been assigned.
			3	CCO does not provide a description of the SCRCP on its website. Therefore there is no means available for the public to be informed about information is being collected without their express consent to CCO.	The data holdings list appended to CCO's Privacy Policy, which is publicly available on CCO's website, be updated to include a description of the SCRCP data holding, including the purpose for which the SCRCP PHI is collected, the types of information collected, the data steward assigned to the SCRCP data holding, and the source of the information collected.	Program and Privacy & Access Office	N/A	A decision was made not to update the list due to the data holding being from a pilot program and thus not a permanent data holding.
			4	The SCRCP data holding on the H drive has not yet been added as a data holding in ODDAR.	Before SCRCP PHI is submitted to the Program, the Program to add the SCRCP data holdings to ODDAR and ensure that all CCO employees accessing the SCRCP PHI receive authorization through ODDAR first.	Program	22-Jun-12	Program confirmed that data holding has been added to ODAAR.
			5	No Risks Identified	Program to advise the Privacy & Access Office if and when new linkages are occurring between the SCRCP PHI and existing CCO data holdings and whether a permanent data holding will be created after any such new linkages, so that a PIA or PIA Addendum can be completed for such new linkages.	Program	N/A	Recommendation provides requirements for future and speculative linkages

			6	No Risks Identified	Before linking SCRCP PHI with PHI in other CCO prescribed entity data holdings, CCO's Privacy & Access Office will review any DSAs or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO.	Privacy & Access Office	N/A	Recommendation provides requirements for future and speculative linkages
			7	The Program has not determined for how long the SCRCP PHI will be retained in the Directory on the H Drive, therefore, the Program is not able to confirm that the retention period is necessary for the fulfillment of the Program purpose. An inventory in line with CCO's Privacy Policy outlining the format, physical location, and time span of each data holding retained by the Program domain has not been completed.	7) Program to establish a retention period for the SCRCP data holding and ensure that the retention period is necessary for the fulfillment of the Program purpose. Program/data steward to advise the Privacy & Access Office when all or part of the SCRCP data holding is no longer required for the purposes of the Program. 8) The data steward responsible for the SCRCP Data Holding to establish an inventory of data retained by the Program, in line with CCO's Privacy Policy.	Program	(1) June 2012 (2) August 2012	(1) Retention period for SCRCP data is 10 years. (2)Informatics complete inventory of data.
			8	The Funding Agreements between CCO and the facilities did not include Schedule B which includes privacy obligations and expectations or any other privacy language.	9) CCO to enter into amended funding agreements with each participating facility which includes Schedule B and comprehensive privacy language including requirements for the secure transmission of PHI from each facility to CCO, a note on what safeguards CCO has in place to protect the PHI that it is receiving from facilities and an outline of the authority for the collection of the SCRCP PHI by CCO and notify the Privacy & Access Office when this has been completed.	Privacy & Access Office, Legal, and Program	Dec-12	Funding agreements re-sent with Schedule B and signed by each facility.

			9	No Risks Identified	Program to work with security to ensure that safeguards in this system are in place. At present the system is being designed in accordance with security standards and the proposed transfer approach is on the (draft) list of approved PHI transfer mechanisms. Security will provide the program for a list of safeguards and any identified risks as the project progresses. Program, in consultation with the EISO will also confirm with privacy whether a TRA is required. If a TRA is not required, program will provide privacy with the reasoning behind the decision.	Program and EISO	Jun-12	EISO confirmed that a VA was conducted on Tumbleweed.
Multidisciplinary Case Conference (MCC) Pilot Program	Feb-27-2012	Privacy Specialist	**1**	It is unclear whether FIPPA applies to CCO in its role as a prescribed entity for the MCC Program.	CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or the PHIPA Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a HINP; a service provider; an agent under PHIPA; a s. 39(1)(c) prescribed person; and a s. 45 prescribed entity	Privacy & Access Office	27-Jul-12	On July 27, 2012, CCO's Privacy & Access Office delivered its request to the MOHLTC for a legislative amendment to PHIPA to address this legislative gap.
			2	The Program has not made available publically on the CCO website, an updated the data holdings list to include a description of the MCC data holding, including the purpose for which the MCC PHI is collected, the types of information collected, the data steward assigned to the MCC data holding, and the source of the information collected.	Program to advise the Privacy & Access Office when the data holding list will be ready for inclusion on the webpage maintained by Privacy. The Program should provide the list to Privacy by March 9, 2012.	Program and Privacy & Access Office	In progress	Privacy Policy to be updated.
			3	The Program has noted the linkages that it intends to conduct using the data collected. However, as it completes the process of gathering the requirements for the indicators and reporting, the Program may need to conduct further linkages.	Program to advise the Privacy & Access Office if and when new linkages are occurring between the MCC PHI and existing CCO data holdings and whether a permanent data holding will be created after any such new linkages, so that a PIA or PIA Addendum can be completed for such new linkages.	Program	N/A	Recommendation provides requirements for future and speculative linkages

			4	CCO may have data sharing agreements (DSAs) or other agreements with the providers of PHI data ("data source") currently in CCO data holdings to which the MCC PHI will be linked. It is possible that the DSAs with the data sources include limitations on the purposes for which CCO may use the source data, and therefore that CCO will not be in compliance with the DSAs with the data sources.	Before linking MCC PHI with PHI in other CCO prescribed entity data holdings, CCO's Privacy & Access Office will review any DSAs or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO.	Privacy & Access Office	N/A	Recommendation provides requirements for future and speculative linkages
			5	The Program has not determined for how long the MCC PHI will be retained in the Permanent Directory on the H Drive or in the MCC database, therefore, the Program is not able to confirm that the retention period is necessary for the fulfillment of the Program purpose.	Program to establish a retention period for the MCC data holding and ensure that the retention period is necessary for the fulfillment of the Program purpose. Program/data steward to advise the Privacy & Access Office when all or part of the MCC data holding is no longer required for the purposes of the Program.	Program	TBD	Program to confirm
			6	An inventory in line with CCO's Privacy Policy outlining the format, physical location, and time span of each data holding retained by the Program domain has not been completed.	The data steward responsible for the MCC Data Holding to establish an inventory of data retained by the Program, in line with CCO's Privacy Policy.	Program	March-April 2012.	An inventory of the data retained by the Program has been established.
			7	The program has not received a completed TRA from EISO on the MCC solution including the MCC Database. As a result, no recommendations stemming from the TRA have been incorporated into the solution.	Program to work with security to ensure that safeguards in this system are in place. At present the system is being designed in accordance with security standards and the proposed transfer approach is on the (draft) list of approved PHI transfer mechanisms. Security will provide the program for a list of safeguards and any identified risks as the project progresses. Program, in consultation with the EISO will also confirm with privacy whether a TRA is required. If a TRA is not required, program will provide privacy with the reasoning behind the decision.	Program and EISO	Mar-12	Security requirements provided/implemented. Program is using an established secure transfer mechanism (Tumbleweed) and storing on the secure H: drive.
			8	Logging and audit requirements have been built into the MCC solution architecture. However, a threat model which identifies the typical use cases when CCO employees can access and use PHI, has not yet been developed.	Identification of the typical use cases with respect to access to PHI and potential threat scenarios for each use case is to be developed by the MCC Program in collaboration with the Privacy & Access Office and EISO, in accordance with Procedure 7.5 under	Program and EISO	Mar-12	Complete.

					CCO's Privacy Policy. These threat scenarios will be used in the logging and auditing program at CCO.			
Computerized Physician Order Entry (CPOE) Oncology Patient Information System (OPIS) – Addendum to the 2007 PIA v5 and 2009 Addendum v5	Feb-03-2012	Privacy Manager	**1**	CCO enters into software license and services agreements with all hospitals using OPIS.	(1) The Program confirm that licensing agreements have been executed with each of the 15 new sites implementing OPIS. (2) The Program share with the licensing hospitals a summary of the PIA recommendations that are the responsibility of the hospitals.	Program	(1) March - September 2012 (2) March - September 2012	(1) Agreements executed. (2) PIA recommendations were shared and support provided on use of the new multi-site functions.
ColonCancerCheck (CCC) FOBT Reminder Research Study	Jan-27-2012	Privacy Manager	**1**	The Study may involve further disclosures of PHI between ICES and CCO, which fall outside of the scope of this PIA.	1) Any future disclosures of PHI between CCO and ICES that relate to the Study must be reviewed and approved by the DAC.	ICES	30-Nov-12	ColonCancerCheck PHI relating to this project for research purposes was requested through the DAC process. This request was approved by the DAC on November 30, 2012.
			2	The DAC does not have a formal process to determine whether a research project requires a PIA in light of CCO's role in the project.	2) The DAC should establish a procedure to determine whether a research project requires a PIA in light of CCO's role in the project.	Privacy Manager, Cancer Screening	17-Jun-14	CCO's *Decision Criteria for Data Requests*, a policy used by DAC to determine whether to grant a research request, revised to explicitly contemplate that a PIA may be required where CCO is participating in the research in its capacity as a "prescribed entity" or as a "prescribed registry". This revision was approved by DAC on June 17, 2014.
			3	The ICSP Statement of Information Practices does not contemplate that CCC will collect PHI for the purpose of pre-populating FOBT kits and lab requisitions that would be sent to Participants along with screening correspondence.	3) If CCC decides to send prepopulated FOBT kits and lab requisitions to Participants as part of its standard approach to Participant correspondence, the ICSP Statement of Information Practices should be revised to explicitly state that ICSP collects PHI for the purpose of pre-populating screening test kits and	Privacy Manager, Cancer Screening	N/A	To date, CCC has not decided to send pre-populated FOBT Kits and Lab Requisitions as part of its standard approach to Participant correspondence.

					related documents that are sent to Participants along with screening correspondence.			
			4	Certain data elements should not be prepopulated on the lab requisitions sent to the test group of Pilot Recalls because such disclosure is not "reasonably necessary" to meet the purpose of reducing the occurrence of FOBT rejections by Labs.	4) The prepopulated lab requisition for used in Phase 1 of the Study should be altered so as not to prepopulate the following data elements: health number, sex, and telephone number. The specialized recall letter sent to the test group of Pilot Recalls should instruct the Participant to add these data elements to the requisition before sending the completed FOBT and requisition to a Lab. 5) The Privacy & Access Office must review and approve sample versions (without PHI) of the prepopulated lab requisition, FOBT kit and the specialized recall letter before the Phase 2 mailing may proceed.	Privacy Manager, Cancer Screening	19-Jan-12	Correspondence materials discussed in these recommendations reviewed and approved by Privacy Manager, Cancer Screening on January 19, 2012.
			5	If, in the future, CCC decides to send prepopulated FOBT kits and lab requisitions to all Participants as part of its standard approach to Participant correspondence, a substantial privacy risk would be created because it would be a statistical certainty that hundreds of mailings containing a Participant's date of birth (among other PHI) would be sent to incorrect addresses and inappropriately opened.	6) If CCC decides to send prepopulated FOBT kits and lab requisitions to Participants as part of its standard approach to Participant correspondence, the Privacy & Access Office must review of the use of such prepopulated FOBT kits and lab requisitions on a province-wide scale.	Privacy Manager, Cancer Screening	N/A	To date, CCC has not decided to send pre-populated FOBT Kits and Lab Requisitions as part of its standard approach to Participant correspondence.
			6	CCO and the fulfillment house have not yet finalized the Phase 2 SOW.	7) The Phase 2 SOW should implement the recommendations contained in this PIA and contain specific terms to address the privacy and security risks associated with the fulfillment house's involvement in Phase 2 of the Study. 8) The Privacy & Access Office must review and approve the Phase 2 SOW before the fulfillment house carries out any services relating to the production, assembly and delivery of the Phase 2	Privacy manager, Cancer Screening	18-Jan-12	The Phase 2 SOW (A.K.A. the PLI Planning Form) was reviewed and approved by the Privacy manager, Cancer Screening On January 18, 2012.

					mailings to the Pilot Recalls.			
Wait Times Information System (WTIS) - WTIS Expansion	Dec-14-2011	Privacy Manager	**1**	It is unclear whether FIPPA applies to CCO when acting under its various PHIPA authorities.	1) CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or its Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a HINP; a service provider; an agent under PHIPA; a ss. 39(1)(c) prescribed person; and a ss. 45 prescribed entity.	Privacy & Access Office	27-Jul-12	On July 27, 2012, CCO's Privacy & Access Office delivered its request to the MOHLTC for a legislative amendment to PHIPA to address this legislative gap.
			2	CCO discloses PHI for patient identification purposes to eHealth Ontario for the EMPI.	2) CCO consider entering into a Data Sharing Agreement (DSA) for the disclosure of PHI for patient identification purposes to eHealth Ontario for the EMPI.	Privacy & Access Office	**TBD**	CPO and Privacy Counsel to review and provide direction on how to proceed.
			3	There may be a data linkage in the future between the WTIS and NACRS data holdings.	3) Program to advise CCO's Privacy & Access Office before linking PHI in the Program Data Holding with existing CCO data holdings and whether a permanent data holding will be created after any such new linkages, so that a PIA or PIA Addendum can be completed for such new linkages. 4) Before linking PHI in the Program Data Holding with PHI in other CCO prescribed entities data holdings, CCO's Privacy & Access Office will review any DSAs or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO.	Privacy & Access Office	N/A	Recommendation provides requirements for future and speculative linkages
			4	Only necessary patient identifying information should be retained	5) ATC review the WTIS patient identifying information that is collected to determine the appropriate retention time.	Program	**TBD**	Program to confirm.
Case-by-Case Review Program	Nov-18-2011	Chief Privacy Officer	**1**	No Risks Identified	The incorporation of the CBCRP and EBP into the proposed NDFP e-claims solution tool to be addressed through an amendment to this PIA.	Privacy & Access Office	15-Nov-12	Risk Mitigation plan developed for the inclusion of EBP in eClaims. Recommendations have

(CBCRP) and Evidence Building Program (EBP)								been implemented. There are no plans for the inclusion of CBCRP.
			2	It is unclear whether FIPPA applies to CCO in its role as a prescribed entity for the CBCRP and EBP.	CCO to seek clarity on FIPPA's applicability to CCO through an amendment to PHIPA and/or its Regulation, clarifying that FIPPA does not apply to CCO's collection, use or disclosure of PHI, when acting under its various PHIPA authorities, such as a HINP; a service provider; an agent under PHIPA; a ss. 39(1)(c) prescribed person; and a ss. 45 prescribed entity.	Privacy & Access Office	27-Jul-12	On July 27, 2012, CCO's Privacy & Access Office delivered its request to the MOHLTC for a legislative amendment to PHIPA to address this legislative gap.
			3	No Risks Identified	Given the time constraints imposed upon this PIA, the analysis in this section has been accepted notwithstanding that the EBP appears to be similar in many respects operationally to the CBCRP. Given the recent introduction of new drug and other treatment reimbursement programs at CCO, it is recommended that the CCO Privacy & Access Office, in consultation with the Clinical Programs Office and the MOHLTC, complete a review of the privacy authorities for all CCO reimbursement programs including: the NDFP, the EBP, the CBCRP, the Brachytherapy Reimbursement Program and the Ontario Positron Emission Tomography Scan Evidence-Based Program (EB-PET Program) to: (i) ensure that a consistent authorities approach is applied to all CCO reimbursement programs (which may translate into an omnibus operations agreement with participating hospitals); (ii) address issues related to the secure method of transferring PHI among the participants of the reimbursement programs; and (iii) address issues related to disclosure by CCO of PHI to external decision makers (e.g. MOHLTC). This review should take place prior to the planned transition of the manual components	Legal , Privacy & Access Office	Oct-12	GC & CPO confirmed that a review will not be required. All transfers of PHI are in accordance with the Secure Transfer of PHI Policy and approved by EISO. Legal review of one reimbursement conducted to ensure that it is consistent with general administrative law principles. Review concluded a CCO-MOHLTC DSA required concerning all reimbursement programs only.

					of the EBP and CBCRP into the NDFP e-claims application.			
			4	As a privacy best practice, a HIC should enter into an agreement with its PHIPA agents in order to implement the provisions of PHIPA, s. 17. Without an agreement, the privacy responsibilities of the agent may not be clear.	CCO acting as an agent for the MOHLTC for the CBCRP have an appropriate agreement in place to reflect the responsibilities contained in s. 17 of PHIPA.	Legal and Privacy & Access Office	**TBD**	CPO and Privacy Counsel to review and provide direction on how to proceed.
			5	There is a lack of an accountability agreement between CCO in its role as a prescribed entity and HICS. Included in the CBCRP and EBP plans for this year are revisions to the existing NDFP agreement to include these two new drug reimbursement programs.	CCO complete an agreement with HICs (or amend an existing agreement) for the collection and disclosure of PHI for the CBCRP and EBP.	Privacy & Access Office, Legal, Program	Dec-12	Currently NDFP, CBC and EBP are described in the eClaims Software License Agreement with individual hospitals in a Schedule.
			6	The EBP and CBCRP are not itemized in CCO's Privacy Policy as required. The Data Holding requires the designation of a Data Steward and a Privacy lead.	The EBP and CBCRP data holdings be itemized in the CCO's Privacy Policy and a data steward and a privacy lead be designated for each data holding.	Program and Privacy & Access Office	Mar-13	A data steward has been assigned to both the EBP and CBCRP data holdings and the Privacy Policy has been updated
			7	Because the EBP and CBCRP have not been itemized in CCO's Privacy Policy, a Statement of Purpose is not available.	The Statement of Purpose for the EBP and CBCRP be included in CCO's Privacy Policy.	Program and Privacy & Access Office	Mar-13	Privacy Policy has been updated
			8	Principle 4 of CCO's Privacy Policy requires that PHI collected by CCO be limited to only that which is necessary to fulfill the identified purposes of the data holding. For the CBCRP there is an Excel spreadsheet that provides the rationale for the collection of each data element. There is no equivalent data available for the EBP.	The EBP documents the rationale for the collection of each data element	Program and Privacy & Access Office	Mar-13	Rational for collection has been updated.
			9	There is no specific proposal to link other CCO prescribed entity data holdings with the EBP or CBCRP at this time. In the future there may be a need to link the EBP and CBCRP data to other data holdings like the Ontario Cancer Registry and ALR/Data Book (treatment data). In the coming months, the project will be working with the CCO Informatics Department on a reporting and evaluation framework which will provide further information on whether the CBCRP and/or EBP will propose data linkages, to which data sources, and how/why the data will be used.	Before linking PHI in the CBCRP and EBP Data Holding(s) with PHI in other CCO prescribed entity data holdings, CCO's Privacy & Access Office review any data sharing agreements or other agreements between CCO and the data source of the PHI, in order to ensure that the linkages planned by the Program fall within the purpose(s) for which the PHI in the other CCO data holding was collected and may be used by CCO.	Privacy & Access Office	N/A	Recommendation provides requirements for future and speculative linkages

			10	CCO the prescribed entity is restricted in the PHI that it can disclose. The disclosure of PHI to the MOHLTC is discussed in the CBCRP Data Flow 3 of this report. O. Reg. 329/04 provides CCO with the authority to disclose PHI collected as if it were a health information custodian to a custodian (MOHLTC) or person from whom the entity collected the information, whether the information has been manipulated or altered, so long as it does not contain any additional identifying information. The disclosure contains additional identifying information related to the EBP drug for the patient.	CCO review the disclosure of EBP PHI to the MOHLTC to determine the PHIPA authority for the disclosure.	Privacy & Access Office	Mar-13	Re: EBP PHI - it is not disclosed to the MOHLTC.
			11	CCO will be collecting and using CBCRP PHI as an agent of MOHLTC and as a prescribed entity. Certain data will be used for both purposes and certain data will be used only as an agent or only as a prescribed entity. Access controls should be put in place to provide the appropriate access privileges.	CCO put in place appropriate access controls to limit access to CBCRP PHI in the roles of MOHLTC agent and CCO prescribed entity	Program and Technology Services	Mar-13	Data Submitted through secure upload tool and saved in H drive. ODDAR process utilized by PDRP for reimbursement operations and by Informatics for analysis purposes. Only Informatics has access to the subfolder in the H drive that includes a cut of the data for the purposes of PE analysis.
eCCO Sharepoint	Nov-15-2011	Privacy Specialist	**1**	It is unclear if the collection of PI by CCO from staff for the purposes of My Site is an authorized collection of PI under FIPPA.	CCO should provide notice to all CCO employees that they do not need to provide their PI for My Site and if they choose to input their PI, they are consenting to its collection for CCO business purposes. Currently there is no such statement on the My Site page.	Privacy to draft consent provision. Web team to update My Site template.	TBD	The Microsoft Sharepoint 2010 platform will be updated to the Microsoft Sharepoint 201 in the next 24 months. It is expected to have the technical capability to implement this recommendation.
			2	The Terms of Use that an external user for an external collaboration space must agree to should state that they are not to input PI or PHI into any external collaboration spaces.	If there are PI fields and / or the ability to upload photographs for external user profiles, they should be disabled and fields relating only to professional capacity should remain.	Web Team	Dec-11	There is no ability to upload information/documents by external users.

APPENDIX F: Indicators – Summary from the Log of PPAFs/Privacy Service Engagement Requests (PSERs)

Date Submitted	Program/Project Name	Initiative Name	Impacted Data Holding(s)	PIA to be Conducted? (Y/N)	Description of the reasons for the determination/Rationale for the decision
Oct-10-2013	Cancer Information Program	eClaims	New Drug Funding Program (NDFP); Evidence-Building Program (EBP)	N	(1) PIA : An eClaims Solution PIA was completed June 2012, establishing the PHIPA authority in respect of the operation of the eClaims by CCO as a Health information Network Provider ('HINP') and PHIPA Agent. This technical enhancement does not have any impact on the above mentioned PHIPA authorities and on the collection, use and disclosure of PHI for the purposes of the Provincial Drug Reimbursement Program. (2) License and Participation Agreement: Additionally, this technical enhancement does not have an impact on the HINP and PHIPA Agent services to be provided by CCO to Hospitals as described in the eClaims License and Participation Agreement. Specifically, Clause 5(a) of the Agreement, System Integration, notes that the hospital will use the transmission standard developed by CCO allowing OPIS and non-OPIS ST CPOE systems to receive data from CCO eClaims. (3) Security Assessment & Support: Lastly, EISO will be reviewing this technical enhancement and solution amending the eClaims TRA as required. EISO has confirmed that they will continue to work with the project team, architects and developers to ensure that all appropriate security safeguards are implemented and security risks are mitigated prior to the launch of the interface.
Sep-27-2013	Ontario Renal Network	EMRALD	N/A	N	Project was re-evaluated and Privacy support not required. Privacy Manager advised the project requires a consulting agreement. Sent to Legal. CLOSED.

Sep-27-2013	Regional Operations	OBSP High Risk Data Reporting	Ontario Breast Screening Program (OBSP)	N	Note to file completed based on Program's suppression of cell counts less than 6 in High Risk Reports. Reporting issue was revisited in November 2013 and privacy analysis and advice provided (no new PSER was completed).
Sep-10-2013	Technology Services	Bring Your Own Computer Device (BYOCD)	N/A	N	Privacy Deliverables not required. Privacy will be supporting project via RFP committee.
Sep-09-2013	Evaluation Reporting Cancer Screening and Aboriginal Cancer Control Unit	FNIM Data Acquisition Plan: Project Charter A	N/A	N	Following an internal review with the Privacy Manager and Director, Privacy, it was determined that the privacy deliverables were critically dependent on data collected by the project to inform (1) the Privacy and Legal framework (2) the Privacy Impact Assessments and (3) Necessary Data Sharing Agreements or MOUs. Project will submit a subsequent Privacy request once the third party consultants have completed the environmental scan of the data sources containing FNIM identifiers.
Aug-28-2013	Regional Operations	Colposcopy QBP	Ontario Cervical Screening Program (OCSP)	N	No new data collections or linkage with screening data required. To be reviewed as part of HSFR PIA.

Aug-23-2013	Policy, Knowledge Translation and Exchange and Primary Care (PKTEPC)	Physician-Linked Correspondence	ColonCancer Check (CCC)	N	A privacy analysis of the disclosure of physician Information appears in the ColonCancerCheck Privacy Impact Assessment Report — Update#1, and in the Briefing Note: Physician-Linked Correspondence Pilot Program, dated October 14, 2011. There is no change to the PHIPA authority identified in the above documents.
Aug-09-2013	Enterprise Services Information Program (ESIP)	SME Connect!	N/A	N	The SME Connect application will not involve the collection of personal information or personal health information, therefore the involvement of the Privacy & Access Office is not required. The project will draw on existing data posted on CCO employee "My Site" pages. These pages are in the public domain.
Jul-22-2013	Evaluation and Reporting	Correspondence Evaluation Approach & Methodology	N/A	N	The activity will be to develop a two-year Evaluation Plan and the associated Analytic Methodology. There are no Personal Health Information (PHI) elements involved during this planning stage (i.e., the Evaluation Plan), which is anticipated to extend into 2013/14.
Jun-26-2013	Ontario Renal Network	CCO-WTIS Data Linkage	N/A	N	The PAO has considered the record-level data elements to be collected set out at Schedule "A" to this PPAF ¡n light of CCO's *De-identification Guidelines* (currently under review), excluding the "patient information" data elements which will not be disclosed to CCO. The PAO has concluded that this data set does not contain any "immediately identifiable" or "potentially identifiable" data elements Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report, however this has been provided to the IPC. The ORN has agreed to implement four privacy controls in respect of this collection of de-identified data, including adding specific privacy-related language to the information package and in the excel files.

Jun-04-2013	Primary Care, Cancer Screening	Provider-Level Reporting	Corporate Provider Database (**CPDB**), Client Agency Program Enrolment (**CAPE**), CIRT, Lab Reporting Tool (**LRT**), Postal code conversion file, eHealth Ontario - ONE ID registration status list	N	The PAO has completed an analysis of this initiative to be undertaken by CCO as a PP. We have reviewed the data sharing agreements , and the relationships between CCC and those to whom this data will be provided. Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report, however this has been provided to the IPC. The PAO has advised that the program may proceed, provided that 3 recommendations related to the provision of privacy and security instructions, ensuring agreements are in place, and secure transfer of the reports are implemented.
May-23-2013	Cancer screening - OBSP	OBSP Pink Mobile	Integrated Client Management System (**ICMS**)	N	The use of the ICMS by OBSP designated staff to book appointments for mammograms has already been considered in the 2006 P1A for OBSP—ICMS. The only difference introduced by this initiative is the location from which OBSP designated staff will access ICMS — a mobile bus. The PAO has reviewed the updated MOU with CCO's partner and, in collaboration with EISO, has confirmed that the appropriate privacy and security controls are included. Further privacy review is not required provided that prior to the commencement of the campaign: . The 2013 MOU with CCO's partner containing the recommended privacy and security controls is finalized; . The privacy requirements set out in the MOU (e.g., privacy training for individuals with access to the mobile bus) have been implemented by CCO's partner and OBSP designated staff; and . The security recommendations set out in the MOU (*e.g.*, encryption of the laptop, etc.) have been implemented by OBSP designated staff. The Business Unit must demonstrate to the satisfaction of the PAO that these conditions have been met prior to the launch date of June 12, 2013 (e.g., provide copies of following documents: (a) finalized MOU, (b) executed privacy training acknowledgement forms, and (c) opinion by EISO that its recommendations have been properly implemented). If these conditions are not met, agents of OBSP Sites must not access ICMS from the mobile bus.

May-13-2013	Informatics	Statistical Analysis System (**SAS**) Data Quality	ALR	N	The purpose of the initiative is to install the software to allow for future planning and automation of data quality management activities to enable CCO to ensure its data is of the highest quality and enables data sharing and re-use where appropriate. Access to the PHI will be through the ODDAR process and limited to this narrow use. EISO has been involved and provided advice with respect to PHI in testing. All access to PHI will be read-only. LMAS - the software will leverage database logging that should already be in place through LMAS. If in the future it is discovered that there are databases which do not have the ability to link up with LMAS, then logging methodology will need to be developed prior to software use and confirmed with the PAO and EISO. This PPAF covers the initial install to allow Informatics to better understand the product for the purpose of future planning. As a result, no PIA is required at this point. However, when Informatics understands how to better use the tool, subsequent initiatives will be brought forward that utilize this product, each of which will go through the check point process. At that point, a PIA may be required.
Apr-25-2013	Surveillance	Partnership with Public Health Ontario (**PHO**)	OCR	N	This initiative concerns the disclosure of certain data elements contained in the OCR to PHO. The data elements in question (the "Data" for the purposes of this log entry) are identical to the Ontario Cancer Incidence data contained in CCO's SEER*Stat CD, which CCO currently discloses certain researchers and health institutions, including PHO and certain Public Health Units. The PAO — in its review of the SEER*Stat CD — concluded that while this Ontario Cancer Incidence data contains a number of "potentially identifiable" data elements, it does not constitute "personal health information" under CCO's De-Identification Guidelines (currently under review). Given that the Data set does not contain PHI, no further privacy review of this initiative is required provided that the following controls are put in place: - CCO and the PHO enter into a DSA in respect of the disclosure of the Data which contains provisions that are essentially equivalent to those contained in CCO's standard SEER*Stat Agreement; and - The manner in which the Data is to be transferred from CCO to PHO complies with CCO's Policy on the Secure Transfer of PHI.
Apr-17-2013	Aboriginal Cancer Control Unit	Aboriginal Tobacco Smoking Cessation Program (**ATSCP**) Pilot Project	N/A	N	Rationale for the decision: The consultant acting on behalf of CCO in respect of this initiative will review medical records containing PHI at the health center to generate reports containing aggregate data in respect of the ATSCP Pilot Project. To this extent, the consultants will be "collecting" and "using" PHI for the purposes of ss. 45(1), (5) and (6) of PHIPA. Nevertheless, in light of the limited access to PHI that will be granted to the consultant ¡n respect of this initiative, a PIA is not required provided that the following privacy controls are in place before the consultants have access to such PHI: 1. The Third Party Service Provider Agreement between CCC and the consultant must: a. contain CCO's standard privacy schedule; and b. explicitly provide that while the consultant may go on-site at the health center to review records containing PHI for the purposes of the initiative, the consultant must not retain, copy or create any records containing such PHI. The consultant may only use such PHI to create records containing aggregate data. 2. CCO must enter an agreement with the health center under which CCO's consultant ¡s granted the right to review records containing PHI on site for the purposes of the initiative, subject to the restrictions set out above.

Apr-10-2013	Aboriginal Cancer Control Unit	Heath centre Patient Referral Volumes Validation	Canadian Institute for Health Information's (**CIHI**) Discharge Abstract Database (**DAD**) and National Ambulatory Care Reporting System (**NACRS**), CCO's EDW	N	This initiative will involve the collection and use of certain personal health information (PHI). The proposed collection of such data is permitted under PHIPA and CCO's data sharing agreements. Due to the confidential nature of the details of the analysis, CCO has excluded a description of the analysis from the public version of this report, however this has been provided to the IPC. In light of the low privacy risk associated with this initiative — a one-time collection of PHI for a very narrow purpose — further privacy review is not required provided the following privacy controls are put in place: 1. Prior to the collection of PHI from the health centre: a. CCC and the health centre must execute an agreement in respect of this initiative setting out the manner in which such PHI will be collected and used (the agreement has been drafted by Senior Legal Counsel in the PAO, and is included at Schedule IB* to this PPAF). b. The ACCU must confirm that: i. the manner in which the PHI is to be transferred from the health centreto CCO complies with CCO's Policy on the Secure Transfer of PHI; ii. The collected PHI will only be stored on the H: drive; and iii. Access to such PHI will be regulated by ODDAR (and thereby tracked via LMAS). 2. Prior to any use of the collected PHI from the health centre: a. Informatics must confirm (i) whether any data contained in EDW apart from DAD and NACRS will be used and (ii), if so, the specific source of such data. b. The PAO must confirm whether the use of such EDW data is permitted under the relevant DSA. c. Informatics must confirm that the PHI collected from the health centre will be securely destroyed once the use ¡s complete and, ¡n any event, within six months of the date of collection (subject to any extension granted by the PAO).
Apr-02-2013	Cancer Screening	Contact Centre Strategy — User Experience Interviews	N/A	N	Pl and/or PHI will not need to be collected by CCO's service provider for this initiative. At the end of each call during the two-day interview period, CCO's Contact Centre staff will request the consent of clients who call ¡n to participate ¡n an interview. Once consent is obtained, the Contact Centre will then "warm transfer" the call to the service provider to conduct the interview onsite, providing the client's first name only (provided the client consents to this). However, it is possible that PI and/or PHI may be provided by the client to the service provider during the course of the interview. The privacy requirements for the initiative are as follows: . CCO's PAO will provide a script to be followed by Contact Centre staff for obtaining consent to participate in the interviews. The script will include the necessary FIPPA notice (in the event that Pl is collected during the course of the interview) . The PAO will provide feedback and approval of the interview guide to be used by the service provider . All interviews will be conducted on CCO premises. the service provider will set up in a room that is separate from the Contact Centre (due to privacy constraints) and calls will be forwarded to the line where the service provider team is located . No paper records of interview responses will be created; Interview responses must be stored electronically on CCO's secure H: drive.
Mar-25-2013	DAP-EPS Phase II	Pilot integration with Electronic Medical Records (**EMRs**) for electronic Referrals	DAP-EPS Database	N	A PIA is not required for this initiative: This is a very minor change to the program; whereas referral information was previously faxed and then manually entered into the DAP-EPS. (1) In summary, the former method of collecting the referral information was a manual process via fax and this will now change to an automated transmission through the DAP-EPS from an EMR system, sent directly from the originating source (the physician's office). The same data elements are being collected. Thus, the only change taking place is to the method of collection of referral information. (2) Additionally, all users of DAP-EPS will now be able to view the reason for referral. However, there are no implications or changes to the manner in which PHI will be accessed in the DAP-EPS onto the identity management and authentication processes in place for all DAP EPS users. The collection of the patient referral information and the purpose for the collection of this information remains the same. The proposed change is only to the method in which it is being collected (automated and through electronic means) and the ability of users to view this information (through electronic means) via the DAP-EPS. As such, a PIA or Addendum to the PIA is not required for this project. The following recommendations should be carried out by the project team:

					(1) The project team has confirmed that EISO has been engaged for this project. EISO should review and advise on whether the required safeguards are in place for this change in method of collection and whether there are any other security considerations. (2) The project team to advise the PAD once it has determined what the impact is to the access controls that are in place for the DAP-EPS.
Mar-20-2013	Research	Mammography study	N/A	N	The research study received REB approval in June 2010, and ongoing privacy advice has been provided since May 2012 when the researchers began to transfer PHI from study sites. At that time, the PAO was consulted to provide advice on secure methods of transfer. A PIA is not required in respect of the collection, use and disclosure of PHI carried out by a CCO researcher. The researcher nevertheless sought advice from the PAO to confirm that the researcher's use of an information technology solution was in compliance with the researcher's obligations under s. 44 of PHIPA. The PAO provided this advice – which technically was not required by CCO's *Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)* – because CCO had an interest in ensuring that PHI relating to the OBSP was properly protected. The PHI is collected with the express consent of the patient. When received by CCO, the PHI is uploaded onto a secure work station and viewed solely on that work station. The work station has previously been reviewed by the EISO and they are comfortable that this work station is secure and that the appropriate access controls are in place. The change proposed here is the installation of software on the work station and the saving of the PHI used for the study onto a local drive on the work station to enable the software to read the PHI. This software will enable the research team to better view the PHI and to also mask the personal identifiers. There are no changes to the collection, use and disclosure of PHI as a result of this initiative. PAO has also reviewed the approved REB protocol for this study, and is comfortable that this change is permissible under that protocol. The PAO approves the installation of the software, provided that the EISO's recommendations are implemented which includes that: . The tool will be used only for the purpose of this study, and only during the time period from April 2013, until December 2013, after which time the software will be deleted from CCO Systems. . The research team follows up with EISO to ensure that all PHI haa been securely removed from the local drive once they have been successfully read by the software. Due to the confidential nature of the details of the study, CCO has excluded some details from the public version of this report, however these have been provided to the IPC.
Mar-18-2013	Cancer Information Program	Ambulatory Oncology EMR Specifications	N/A	N	CCO's role in this project is purely consultative, where it is tasked with advising the relevant stakeholders of the appropriate information interface standards, in addition to functional requirements for an EMR. CCO will not be collecting, using or disclosing PHI in order to fulfill the objectives of this project. As such, a PIA is not required. The project team is advised to engage the PAO for an additional privacy review, should CCO's role change in the next phase of the project where it may facilitate in the exchange of EMR related data amongst the stakeholders, and as such may require access to PHI ¡n order to implement the recommendations it has provided in Phase I.
Mar-07-2012	Regional Programs	Bile Duct Cancer Treatment	N/A	N	MOHLTC has asked, and CCO has agreed to distribute one time volume funding to support bile duct cancer treatment at hospitals for Ontario patients. The hospitals will receive funding to support the bile duct cancer treatment program deliverables for the period between April 1, 2011 and March 31, 2012 & as per the reporting requirement contained in the funding agreement, the hospitals agreed to provide CCO with certain performance data. The PAO carried out an analysis of the performance data in question in light of CCO's De-Identification Guidelines and thereby

					determined that such data did not constitute PHI. Accordingly, no further privacy review is required.
Mar-04-2013	Informatics	Data Governance Sharepoint	N/A	N	A PIA is not required as it will not involve the collection, use or disclosure of PHI. Nonetheless as the processes will change the way that PHI is accessed, used and disclosed, the PAO must be involved in ensuring that all Sharepoint work flows adhere to Privacy requirements as defined by PHIPA and the Manual.
Jan-14-2013	OCSP	OCSP - Quality Assurance Program	InScreen - CPDB	N	The OCSP, in consultation with the Program in Evidence-Based Care (**PEBC**) has developed new quality assurance guidelines for the delivery of colposcopies. As part of the process to develop the guidelines, it is necessary to engage physicians who perform colposcopies and acquire their feedback. OCSP would also like to take this opportunity to invite those physicians to sign-up with PEBC's review board. The PAO is comfortable that the legislative and contractual authorities are in place for this initiative, and that the OCSP may proceed, provided that 8 privacy controls are implemented. Privacy controls prescribed related to ensuring feedback is anonymous, ensuring confidential information is not included in correspondence, identifying third parties, secure storage and destruction, collecting business contact information only and ensuring that the PAO reviews a sample of the correspondence before it is sent. Due to the confidential nature of the details of the analysis, CCO has excluded some details of the analysis and recommendations from the public version of this report, however this has been provided to the IPC.
Jan-07-2013	OBSP	OBSP Biennial Report	PIMS	N	PHI resulting from a linkage between CCO's PÌMS and OCR data holdings, validated through a manual review of pathology reports from PIMS will be used by OBSP ¡n order to complete the OBSP Biennial Report and the OBSP High Risk Progress Report to the MOHLTC. There will not be any new collection or disclosure of PHI. The PAO is satisfied that the appropriate legislative and contractual authorities are ¡n place for this use of PHI. Due to the confidential nature of the details of the analysis, CCO has excluded these details from the public version of this report, however they have been provided to the IPC.

Nov-12-2012	ICS	Physician Stakeholder Consultation	InScreen Data Mart - includes the following data holdings: CPDB, CHDB, LRT, CIRT	N	The PAO has completed an analysis of this initiative to be undertaken by CCC as a Prescribed Person. We have reviewed the relevant DSAs the relationships between CCO and those to whom this data will be provided, and consulted with Legal Counsel, Privacy regarding the required next steps. The PAO has advised ICS that they may proceed with this initiative, provided that two recommendations with respect to recruitment and confidentiality agreements are implemented. Due to the confidential nature of the details of the analysis, CCO has excluded these details from the public version of this report, however they have been provided to the IPC.
Nov-07-2012	Prevention & Cancer Control	OBSP Radiologist Outcomes Report	ICMS	N	This initiative involves the disclosure of a list containing PHI by CCC the Prescribed Entity to OBSP radiologists requesting a detailed list of the screening results for their patients in order that they may better understand their results. The radiologists already have access to this data, however, CCO will be identifying the specific patient cases. A similar disclosure was contemplated in Data Set 8 of the OBSP — ICR PIA completed in February 2012., The ICR PIA determined that this data disclosure was permissible under PHIPA. , Following the analysis contained in that PIA, we conclude that the data disclosure contemplated in respect of the Radiologist Outcome Report is permissible under PHIPA. Due to the confidential nature of the details of the analysis, CCO has excluded these details from the public version of this report, however they have been provided to the IPC.
Sep-17-2012	Shared Services	Project Portfolio Management Mobile App	N/A	N	A PIA is not required for this initiative as there is no PHI or PI involved.
Sep-13-2012	Prevention & Cancer Control	CCC Migration Project	CCC	N	The initiative involves moving the CCC data holding from one location to another in InScreen in order to better manage separate CCC correspondence campaigns. The 2011 ICS PIA considered the privacy controls in place for InScreen and its subsequent addendum for InScreen Release 3.0 addresses all privacy controls for the migration of OCSP, OBSP and CCC to campaign management. No major additional privacy measures specific to the CCC migration are required which are not already addressed in the 2011 ICS PIA and the InScreen Release 3.0 PIA Addendum. No PIA Addendum is needed for this change. Our decision ¡s contingent on PCCIP implementing the following privacy recommendations, which must be implemented in order for the initiative to be approved at checkpoint 9. 1. CCO's EISO must confirm that reasonable technical safeguards are in place prior to the CCC migration to campaign management going live. 2. Further to recommendation 2 that was documented ¡n the InScreen Release 3.0 PIA addendum, PCCIP in coordination with EISO, to develop a plan to perform an InScreen TRA. Note: This TRA may not be possible to conduct before go-live, but a reasonable plan with clear timelines will be documented and agreed to with EISO, and based on the plan, the PAO will provide their approval for Checkpoint 9. 3. PHI in Testing Form be submitted to the PAO for approval before testing with PHI takes place. 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.
May-17-2012	Cancer Information Program	eLab	OLIS	N	As there will be no permanent storage of OLIS data within eLab and eLab will only act as a conduit of data, the PIAs will be completed program specific for each use of eLab. The MOHLTC has confirmed that there is no requirement for an eLab PIA. The first PIA will be specific to the DAP-EPS Phase II initiative.

Apr-30-2012	Informatics	ePath Archiver	Pathology Report Data	N	The ePath System was the subject of a PIA in August 2011. The two risk mitigation recommendations contained in that PIA have been implemented. The PAO concluded that the review provided by EISO of the testing of the initiative in question – the ePath Archiver tool – was adequate. During the earlier review of the original ePath Archiver tool re-design (December 2011), The PAO's approval was based on EISO approving the safeguards in place for PHI. As noted, the purpose of the ePath Archiver re-design initiative was to replace the existing storage application with a new application. The developer neglected to add a print function even though that functionality was intended to be included in the re-design originally. The PAO therefore concluded that adding the print functionality to the ePath Archvier as originally intended was a minor change and that, as a result, no further privacy review was required.
Apr-16-2012	Patient Experience	Patient Reported Outcomes Measures	Symptom Management Database	N	All PIA recommendations have been implemented except one for which the status is unclear. In the Tele-Interactive Symptom Assessment and Collection (**ISAAC**) PIA Addendum there was a recommendation that an amended agreement with the vendor be drafted "to outline the vendor's privacy responsibilities and obligations, which would serve to assure the protection of PHI, commensurate with that provided by CCO and to furthermore, require the vendor to comply with CCO's privacy and security requirements and retention guidelines." This recommendation was not marked as complete by the PAO and the Program, due to turnover, is unable to find an amended agreement. The Program Manager for ISAAC, has provided additional information about this initiative to the PAO. Based on this information, the PAO recommends: 1. Adding the listing of the new data elements and brief explanation of the expansion of the ISAAC tool for the Patent Reported Outcome measures (as fitting within the original collection purpose) in an appendix in addition to the current Data Elements Chart in the original 2007 PIA; and 2. Patient Experience Program will advise the PAO of any new collections, any new or changed data linkages and any newly created data holdings resulting from such linkages, including name given. Due to the confidential nature of the details of the analysis, CCO has excluded these details from the public version of this report, however they have been provided to the IPC.
Apr-12-2012	ICS	Pink Mobile Bus	ICMS	N	The use of ICMS by agents of OBSP Sites to book appointments for mammograms has already been considered in the 2006 PIA for OBSP—ICMS. The only difference introduced by this initiative is the location from which agents of OBSP Sites will access ICMS — a mobile bus. The PAO has reviewed the draft MOU with CCO's partner and, in collaboration with EISO, added appropriate privacy and security controls.. Further privacy review is not required provided that prior to the commencement of the campaign: . The MOU with CBCF containing the recommended privacy and security controls is finalized; . The privacy requirements set out in the MOU (e.g., privacy training for partner staff with access to the mobile bus) have been implemented; and . The security recommendations set out in the MOU (e.g., encryption of the laptop, laptop is locked to mobile bus) have been implemented; and The Business Unit must demonstrate to the satisfaction of the PAO that these conditions have been met prior to the launch date of May 21st 2012 (e.g., provide copies of following documents: (a) finalized MOU, (b) executed privacy training acknowledgement forms completed by relevant partner staff, and (c) opinion by EISO that its recommendations have been properly implemented). If these conditions are not met, agents of OBSP Sites must not access ICMS from the mobile bus.

Apr-10-2012	Technology Services	Project Citadel	Extension of data centre — Most of the programs will have their PHI moved to the new data center. PHI will remain at 620 University for some programs. The new data center will have both old and new data.	N	The transfer of data from 505 University Avenue, 13th floor to the data centre will include PHI. Although the project will not involve a new collection, use or disclosure of PHI and/or PI or a change in the existing collection, use or disclosure of PHI, it is imperative that procedures are in place to ensure that PHI is properly secured. The PAO is satisfied that because the data centre will have no logical access to the systems and all current passwords and access controls will be maintained as is, there will be no impact to existing privacy measures.
Apr-08-2012	CCC	Physician Linked Correspondence	CCC Integration Hub	N	The authority for CCC to disclose PHI to the physicians of participants was considered in the 2008 CCC PIA. This initiative is a minor change to the program, as it involves a one-time transfer of patient lists containing PHI to a small number of physicians. Further privacy review of this initiative is not required provided that: a) Each of the affected physicians signs a copy of the "Terms and Conditions — Request for Physician-Linked Correspondence List" and returns it to CCC before CCC transfers the detailed patient list to that physician; and b) The detailed patient lists are transferred to physicians in a manner that is approved by EISO.
Mar-21-2012	OBSP	OBSP High Risk Screening Programs - recall notifications	Integrated Client Management System (ICMS)	N	OBSP Sites currently send recall correspondence to OBSP Participants. This activity was considered in the 2006 PIA on OBSP. The change introduced by this initiative is that now OBSP Sites will also send recall correspondence to participants in OBSP High Risk. The OBSP High Risk Initiative itself has already been considered in two prior PPAFs. One potentially significant change is that CCO will transfer certain data elements to OBSP Sites in order to "work around" a technical limitation of ICMS. The OBSP Sites will use these data elements to manually generate High Risk correspondence for certain OBSP High Risk participants. The PAO has determined that these data elements, in themselves, do not contain PHI.
Mar-20-2012	Patient Experience	ISAAC Re-Development	Symptom Management Database	N	This is a minor change to an existing program authorized under PHIPA. As the change to the ISAAC tool does not affect what PHI is collected and only affects who is inputting the data into the tool, a PIA is not required. This change is minor in that it does not change the reason for collection of the PHI nor does the authority to collect the PHI change. All data linkages and the method of transfer of PHI remain the same as noted in the 2007 PIA and in the 2010 PIA Addendum. All privacy measures outlined in the previous PIA and PIA Addend urns remain the same. The Program will consult with privacy on all future, additional collections of patient information.
Mar-15-2012	Integrated Cancer Screening Program	ICS Funding Framework	InScreen Hub Integration, NACRS, DAD, Ontario Case Costing Initiative, Management Information Systems in Canadian Health Service Organizations (**MIS**) Data, Vital Statistics (Mortality file)	N	This initiative concerns the use of PHI collected for CCO's PP purpose for CCO's PE Purpose. This project will require the creation of an internal DSA (from CCO as PP to CCC as PE) as the consultants will require PP data for PE analytical purposes. CCO's Legal Department is currently preparing the DSA. The contract with the consultants contains standard CCC terms regarding privacy obligations for third party service providers with access to PHI. The consultants have undergone Privacy & Security training. Provided that the following controls are implemented in respect of this project, further privacy review is not required: . The Consultants may only access PHI on-site at CCO's premises through COO's IT system using CCC computers; . All of the Consultants' work products containing PHI (e.g., temporary data holdings containing linked PE and PP data) must be contained on a secure folder on CCOs H: drive and not stored in any other location (e.g., the hard drive of a consultant's personal laptop). . The consultants will not have access to the requested PE data until the DSA is finalized; . The Business Unit will provide 30 days' prior notice to CCO's data partner in respect of any report prepared in respect of this project in accordance with CCO's DSAs with the data partner (Business Unit to consult with the PAO prior to publication to ensure this notice requirement is met). The folder on the H: drive containing the requested PHI and the Consultants' work products containing PHI will be securely destroyed (in consultation with EISO) once the Consultants' work has been closed out. Further privacy review will be required if CCO seeks to hold these work products for a further period.

Mar-12-2012	Access to Care	WTIS	WTIS, Emergency Room National Ambulatory Reporting System Initiative (**ERNI**)	N	Although PHI will be involved in this initiative, the initiative will not involve a new collection, use or disclosure of PHI. The initiative will also not involve a change in the existing collection, use or disclosure of PHI. The proposal is to link ERNI data (collected by CCO pursuant to a DSA between CCO and CIHI) with the WTIS data (collected by CCO pursuant to the WTIS License Agreement between CCO and submitting facilities). All data will only be disclosed in aggregate form. It is the position of CCO's PAO that a PIA is not required for this initiative due to the following reasons: 1) Linkage is permitted pursuant to the DSA; and 2) Linkage is permitted pursuant to the License Agreement.
Feb-27-2012	Databook Automation Project	Databook Automation	ALR Data Mart	N	The change only relates to the manner in which collected ALR data (which contains PHI) is formatted before it is placed in the ALR/Databook Data Mart. This is a minor change with no substantial effect on the collection, use or disclosure of PHI.
Feb-24-2012	Surveillance, Prevention and Cancer Control	Pancreatic Cancer Survival	Canadian Cancer Registry limited use datafile	N	Although PHI will be involved in this initiative, the initiative will not involve a new collection, use or disclosure of PHI. The initiative will also not involve a change in the existing collection, use or disclosure of PHI. The initiative will be researching death certificates to determine the proportion of cases of pancreatic cancer registered in cancer registries across the provinces. These proportions will be assessed at 3-year periods and classified by sex and age. The following age groups will be reviewed: 15-44, 45-54, 55-64, 65-74, 75-99. In addition, the program has informed the PAO that there will be no data sharing. Any disclosure will only be presented in aggregate results. The disclosure will take place at a one-day workshop with CCO's partner. Partner staff and one analyst from the provinces which choose to send an analyst will be present at the one-day workshop.
Feb-23-2012	Prevention & Screening Information Program	OBSP PACS - Integration with Technology Services Environment	OBSP PACS	N	This initiative concerned the procurement of a vendor to provide services respecting an IT solution which included a data holding of digital mammography files containing PHI. This data holding has not yet been reviewed by the PAO, but it will be considered as part of the overall OBSP privacy review scheduled in the coming months – accordingly, a PIA considering this data holding was carried out for the purposes of this initiative, by itself (as of March 2014, the PAO is conducting a phased review of the OBSP as it transitions from a program that CCO operates as a PE to a program CCO operates as a PP – Phase 1 will consider the OBSP's correspondence program, and Phase 2 will consider other aspects of the OBSP such as its quality assurance initiatives). At the time of procuring a vendor for this initiative, a Third Party Service Provider Privacy Assessment was completed. In that Assessment, the PAO set out the following privacy requirements which the vendor must adhere to in order to provide their services to CCO: • Contract must impose standard CCO terms re: privacy obligations for third party service providers with access to PHI (use restrictions, privacy training, etc.); • The Third Party Service Provider team member who provides the services: o will be a Canadian who carries out all of the work within Ontario; o will never use remote access to access the data holding from a location outside of Ontario. o will receive CCO privacy and security training; and o will complete such training prior to accessing PHI.
Feb-10-2012	ICMS Release 3 for OBSP Height Risk Program	ICMS High Risk Screening Phase 3 Release	ICMS	N	The OBSP ICMS PIA dated May 11, 2006 reviews the exchange of client information that occurs between OBSP Sites through ICMS for the purposes of providing breast screening services. The High Risk Program involves a subset of the OBSP sites considered in the 2006 OBSP PIA. Although the data will be different than that which was assessed in the 2006 OBSP PIA (i.e. data concerning High Risk clients), the exchange of client information between OBSP sites and the user access provisions of ICMS has previously been reviewed and approved in the 2006 OBSP PIA. This briefing note relies on the analysis conducted previously.

Feb-07-2012	ColonCancerCheck	Transfer of bulk accession numbers	Screening Hub Stage – LRT	N	CCC receives FOBT data in respect of CCC participants from the labs that process the FOBTs (the "Labs"). Such FOBT data includes accession numbers. An accession number is a unique identifier generated by a Lab for each FOBT result that the Lab has processed. CCC is planning to send accession numbers in bulk to the Labs in order to facilitate the investigation and resolution of issues identified by CCO in respect of FOBT data quality. The PAO considered whether an accession number, by itself, constitutes PHI. The PAO concluded that no PIA is required because it is unlikely that the data in question (accession numbers, in themselves without other identifying information), constitute "PHI" as that term is defined in PHIPA.
Jan-30-2012	CIO PMO	CRM / PPM	N/A	N	No PHI and/or PI involved with this initiative.
Jan-10-2012	Stem Cell Transplant (**SCT**)	SCT FYI 11/12 Minimum Data Set (**MDS**) enhancement	SCT	N	No PIA Addendum required because this initiative – the addition of 13 new data elements to the MDS for SCT – represented a minor change to the program. Nevertheless, in accordance with privacy best practices, the purpose for the collection of each data element was been documented.
Nov-10-2011	PCCIP	ICS	InScreen Data Integration Hub, InScreen Siebel	N	The Postal Code to LHIN cross reference file does not contain any PHI, and is already included in the relevant DSA the Business Unit has confirmed that this data element will also be included in proposed amendments to the relevant DSA. OCRIS data does not contain PHI, but certain OCRIS data elements are already transferred from CCO as PE to CCO as PP for the specific purpose of determining the eligibility of an individual for cancer screening. This initiative is for the very same purpose, but adds certain data elements in light of the expansion of the program to include screening for breast and cervical cancer. The 2011 ICS PIA already explicitly contemplates that this issue and sets out the authority for this transfer of PHI at pp. 41 and 42. The Business Unit has confirmed that the CCO PE to PP DSA will be amended to include the new data elements. EISO has confirmed that no TRA is required in respect of this initiative. Due to the confidential nature of the details of the analysis, CCO has excluded these details from the public version of this report, however they have been provided to the IPC.

APPENDIX G: Indicators – IDAR Audit Report & Recommendations

December 2012 Audit of IDAR

Review of all users authorized to access PHI

RECOMMENDATIONS	DATE OF IMPLEMENTATION	MANNER OF IMPLEMENTATION
Review all active accounts that currently have ODDAR/IDAR access	December 13th, 2012	List generated of all users with authorized access to PHI
Ensure staff who have access to PHI through IDAR also have Active Directory Accounts.	By January 11, 2013	Comparison of ODDAR/IDAR accounts and Active Directory accounts.
Ensure all staff with access to PHI through IDAR continue to require such access.	By January 11, 2013	Email sent to all staff with access to PHI requesting response re whether they no longer need access to PHI. If they do need access, request made to reapply for such access
Disable all IDAR accounts that have no Active Directory accounts	By January 11, 2013	40 ODDAR/IDAR accounts disabled
Disable all IDAR accounts that no longer require access to PHI	By January 11, 2013	206 ODDAR/IDAR accounts disabled
Disable all expired IDAR accounts	By January 11, 2013	2 expired accounts disabled.
Follow up with active IDAR accounts that are not actively using the accounts	By January 11, 2013	23 accounts followed up on. Those who no longer needed access were disabled.

APPENDIX H: Indicators – Summary from the Log of Privacy Breaches

Summary of PE Breaches

for the period between November 1st, 2011 to October 31st, 2013

Investigating Agent	Date Notification Received	Extent of Breach/ Suspected Breach	Internal/ External	Nature & Extent of PHI at Issue	Date Sr. Mgmt Notified	Containment Measures	Date Investigation Completed	Recommendations	Date Recommendation Addressed
Privacy Analyst	Oct-24-13	PHI - case number and patient name sent to CCO.	External	Email with PHI was sent to CCO Helpdesk	Oct-24-13	Sender contacted and requested to resend request using the Interface Message ID or Waitlist ID to reference the patient.	Oct-24-13	Sender reminded to not send PHI via email.	Oct-24-13
Privacy Analyst	Oct-22-13	PHI - patient name, and chemotherapy drug orders emailed to CCO.	External	Email with PHI was sent to CCO Helpdesk	Oct-22-13	Sender contacted and requested to resend request using the Interface Message ID or Waitlist ID to reference the patient.	Oct-22-13	Sender reminded to not send PHI via email.	Oct-22-13
Privacy Analyst	Oct-24-13	PHI - medical record number, wait list entry, wait time patient ID, discharge dates, and designation dates were sent to CCO and were viewed by 8 - 9 staff.	Internal	PHI - medical record number, wait list entry, wait time patient ID, discharge dates, designation dates	Oct-24-13	Email deleted from inbox and deleted items folder by all recipients.	Oct-24-13	Sender reminded to not send PHI via email.	Oct-24-13
Privacy Analyst	Oct-15-13	Unencrypted medical record numbers and hospital account number submitted to CCO.	External	Unencrypted medical record numbers and hospital account number.	Oct-24-13	CCO Informatics identified that the cancellation file from a Hospital sent to ORBC contained unencrypted medical record numbers and account numbers. Sender informed of the breach and Privacy notified. Breach template completed and sent to Privacy.	Oct-24-13	Sender reminded to not send PHI via email.	Oct-24-13
Privacy Analyst	Oct-21-13	Email with PHI data sent to CCO, STIP in order to find out how to change a disease registration date.	External	PHI – patient surnames appeared throughout the body of the email	Oct-22-13	Senior Support Specialist notified user at site of the breach and Privacy.	Oct-22-13	Sender reminded to not send PHI via email.	Oct-22-13

Privacy Analyst	Oct-25-13	Email with PHI data sent to OPIS Help Desk and CCO Help desk from a Hospital in an effort to find out why drugs were duplicated in an order for one patient.	External	PHI Data, patient name, sex, date of birth and chart number	Oct-25-13	STIP removed the email from all mailboxes, asked the sender to resend request without PHI. OPIS Help Desk and CCO Help Desk to delete email from all folders. STIP notified of the breach and Privacy contacted.	Oct-25-13	Sender reminded to not send PHI via email.	Oct-25-13
Privacy Analyst	Oct-15-13	Email to MRI Efficiency Team with a screenshot indicated in the text that PHI was hidden. The Coordinator then sent the data template back to the MRI Efficiency Team at CCO via email not managed file transfer (MFT) Tumbleweed.	External	Elements in data submission template (3)	Oct-15-13	Sender informed to use Tumbleweed and not send data files via email.	Oct-15-13	The Coordinator was contacted and informed that record level data should not be sent via email as it is not a secure method.	Oct-15-13
Privacy Analyst	Oct-9-13	PHI in email screenshot was hidden by boxes superimposed on the screen shot but PHI could still be viewed.	External	PHI in email screenshot was hidden by boxes superimposed on the screen shot but PHI could still be viewed	Oct-7-13	Sender informed of the breach and advised to delete the email from all folders and recipient also told the same thing.	Oct-8-13	Sender reminded to not send PHI via email.	Oct-8-13
Privacy Analyst	Oct-4-13	PHI was included in a screenshot of a data extract that included 15 - 20 health card numbers and postal codes.	Internal	PHI was included in a screenshot of a data extract that included 15 - 20 health card numbers and postal codes	Oct-9-13	Team leader to delete email from all mail folders and advise the recipients of the email to do same.	Oct-9-13	Sender reminded to not send PHI via email.	Oct-9-13
Privacy Analyst	Oct-2-13	Systems Designer assisting the Quality Assurance (QA) team in assessing an unexpected defect on an application-under-test. The QA team used a standard tool and discovered a database containing PHI.	Internal	Patient chart number, health card number and version, date of birth, last name, Institution master number, treatment dose, start and end date, treatments and clinical stage	Oct-2-13	Team leader checked to see if data was fabricated and found it was not and contacted Privacy. Privacy advised data must be deleted where possible in consultation with Security. System Designer obfuscated data temporarily and worked with the Operations Team to delete backups. System Designed deleted some data from the database. Data was obfuscated until approval for deletion is received from Security. Security to draft a recommendation report to prevent similar breaches and risks in the future.	Oct-10-13	Security to draft a recommendation report to prevent similar breaches and risks in the future.	Oct-10-13

Privacy Analyst	Sep-13-13	Fax in the cover page was addressed to a doctor and patient name and Health Card Number, name was on the second page as was the lab requisition. The patient name was different from the addressee. Second fax sent to the same inbox was identical so it related to one patient record.	External	Name of physician, patient name and Health Card Number.	Sep-13-13	Analyst discovered the faxes in the inbox and notified Privacy and deleted it from all boxes. Analyst contacted the sender of the fax and notified them of the breach.	Sep-13-13	Sender reminded to not send PHI via email.	Sep-13-13
Privacy Analyst	Sep-23-13	Fax with patient record was sent by an ultrasound clinic to CCO's primary fax # without a cover sheet but was copied to Clinical Lead, OCSP.	External	Patient name, date of birth, telephone, physician name and ultrasound record.	Sep-23-13	Receptionist notified Privacy of the breach. Privacy analyst advised the sender of the fax and it not be faxed to CCO's primary number. Advised the clinic to follow up with the clinical lead to get a secure fax number. Privacy analyst shredded the fax.	Sep-23-13	Sender advised to follow up with clinical lead to get a secure fax number.	Sep-23-13
Privacy Analyst	Sep-16-13	Email with PHI attachment for 1 patient sent to Privacy mailbox.	External	Patient name, date of birth, physician name, patient record.	Sep-16-13	Email sent to Privacy mailbox, Coordinator sent the email to the Director and Manager. Director informed Privacy Analyst of the breach.	Sep-16-13	Coordinator reminded to not send PHI via email.	Sep-16-13
Privacy Analyst	Sep-17-13	Cancellation file sent to ORBC, encrypted like a case file, leaving Medical Record Number and Account Number columns of data unencrypted.	External	Medical Record Number and Account Number	Sep-17-13	Sender contacted to inform of breach. Privacy informed of the breach. Breach report completed and submitted to Privacy.	Sep-17-13	Sender reminded all PHI must be encrypted.	Sep-17-13
Privacy Analyst	Sep-12-13	Email with PHI related to 45 patients sent to Cancer Screening. Was sent in an effort to confirm number of endoscopy cases performed at a Hospital.	External	Patients record for endoscopy patients	Sep-12-13	Sender contacted to inform of breach and requested to resend without PHI. Privacy informed of the breach. Email with PHI was deleted from all folders and sender informed of the breach. PHI to be sent only via secure method.	Sep-11-13	Sender reminded to not send PHI via email.	Sep-11-13
Privacy Analyst	Sep-17-13	Email sent to OPIS from a Hospital and to CCO Help Desk in an effort to find label field name on the OPIS medication administration screen.	External	Patient name, sex, date of birth, chart	Sep-17-13	Senior Support Specialist notified users at site of breach and CCO Help Desk and requested they delete the email. Privacy also notified.	Sep-17-13	Sender reminded to not send PHI via email.	Sep-17-13
Privacy Analyst	Aug-8-13	Email inquiry to SETP mailbox included attachment of Data Check Tool (Excel spreadsheet) with SETP record level case file data for July 2013.	External	SETP record level case file data	Aug-8-13	SETP administrator attempted to call the sender to advise her that the privacy policy had been violated and Privacy was informed. Email was deleted. Breach report completed and submitted to Privacy.	Aug-9-13	Sender reminded to not send PHI via email.	Aug-9-13

Privacy Analyst	Aug-2-13	PHI included in an attachment report in an email to OPIS.	External	PHI data - name, date of birth, address, telephone, health card number and drug	Aug-2-13	Email sent with PHI in attachment. Senior Support Specialist contacted CCO Help Desk and asked that they delete email and attachment from all mailboxes and advised sender and Privacy. Help Desk permanently deleted the email and ticket containing PHI.	Aug-2-13	Help desk to contact sender to reiterate that PHI must not be sent via email.	Aug-2-13
Privacy Analyst	Jul-23-13	PHI data was included in an email to CCO Help Desk from a Hospital.	External	PHI data - patient Health Insurance Number	Jul-23-13	Service Desk removed PHI content and advised end user and Privacy Service Desk permanently deleted the email and ticket containing PHI.	Jul-23-13	Service desk to contact sender to reiterate that PHI must not be sent via email.	Jul-23-13
Privacy Analyst	Jul-23-13	PHI data from a Cancer Centre was included in an email attachment to OPIS Help Desk.	External	Patient name, address and chemotherapy information.	Jul-23-13	Help Desk removed PHI content and advised end user and Privacy.	Jul-23-13	Help desk contacted the sender and reiterated that PHI must not be sent via email and cautioned the sender to take appropriate steps in transferring PHI in future according to the terms of the relevant agreement between the hospital and CCO.	Jul-23-13
Privacy Analyst	Jul-25-13	OBSP High Risk form was faxed to CCO general fax line. Misdirected to CCO and should have been sent to OBSP site.	External	Form included patient's name, DOB, HIN, phone # and address and type of tests required	Jul-25-13	Privacy Analyst, once informed, retrieved hard copy from Reception who then deleted the electronic version. Privacy Analyst scanned and saved the fax to secure H: drive for Contact Centre to retrieve and shredded the hard copy.	Jul-25-13	Contact Centre called sender to inform that CCO is not the correct place to send these requests and to send them to the OBSP site.	Jul-25-13
Privacy Analyst	Jul-16-13	A Hospital did not encrypt MRN and Account number prior to submitting to ORBC.	External	Unencrypted MRN and hospital account number.	Jul-16-13	CCO informatics conducted data quality analysis; identified issue with them sending case file to ORBC and contained unencrypted MRN and Account number.	Jul-16-13	The senders were cautioned not to send unencrypted MRN and Account numbers through ORBC	Jul-16-13

Privacy Analyst	Jul-15-13	PHI data - 2 patient's MRNs were included in an email to CCO (4 internal employees) from a Hospital.	External	2 patient MRNs	Jul-15-13	Clinical Program Mgr noticed PHI and notified Privacy. CCO employees all confirmed deletion of email containing PHI.	Jul-15-13	Sender reminded to not send PHI via email	Jul-15-13
Privacy Analyst	Jul-15-13	PHI data -1 patient's medical record number (MRN) was included in an email to Project a Coordinator from physician at a Cancer Program.	External	1 Patient MRN	Jul-15-13	Project coordinator advised physician of the PHI breach and Privacy.	Jul-15-13	Sender reminded to not send PHI via email	Jul-15-13
Privacy Analyst	Jul-5-13	PHI was included in an email from CCO health Records Technician to Product Manager and ORN data lead at CCO.	Internal	Email contained renal patient identify information, name, DOB, Health Insurance # and single treatment change record for a single patient	Jul-5-13	Product manager instructed the recipients and the original sender to delete email and empty the email deleted folder and to notify him when done.	Jul-5-13	Sender reminded to not send PHI via email	Jul-5-13
Privacy Analyst	Jul-2-13	A screenshot including patient MRN, drugs prescribed and test date was included on a service desk ticket opened by CCO Service desk and assigned to STIP.	Internal	A screenshot including patient MRN, drugs prescribed and test date was included on a service desk ticket opened by CCO Service desk and assigned to STIP.	Jul-24-13	STIP removed PHI content and advised end user and Privacy. Service Desk permanently deleted the email and ticket containing PHI.	Jul-24-13	Service desk to contact sender to reiterate that PHI must not be sent via email.	Jul-24-13
Privacy Analyst	Jun-28-2013	PHI data was included in an email to WTIS Development team. The procedure is to extract data and save it on the H drive. The extract was emailed instead of saving to the H drive. The extract was an excel file with 60 records containing Patient demographics and Health Cards Numbers	Internal	The extract was an excel file with 60 records containing Patient demographics and Health Cards Numbers	Jun-28-2013	All recipients permanently deleted the email. Product manager reviewed the procedure to extract data from WTIS with the developers and Quality Assurance (**QA**) resources. Privacy Lead of the incident completed a report	Jun-28-2013	Products Manager to review the correct procedure to extract data from WTIS with the developers and QA resources.	Jun-28-2013
Privacy Analyst	Jun-26-2013	CCO general fax rec'd a fax from a hospital in error.	External	Fax had patient name, Date of Birth (**DOB**), health insurance and diagnosis	Jun-26-2013	Facilities Coord notified PAO and called hospital to inform them of the incident. Facilities Coord. Deleted the fax from all folders	Jun-24-2013	Facilities Coordinator to delete the email from the inbox and deleted items folders.	Jun-26-2013

Privacy Analyst	Jun-24-2013	ATC Analyst who supports iPort was emailed a file of medical records numbers (MRN) and patient chart numbers who then fwd it to his managers to report the issue but the manager did not open the file	Internal	file of medical record numbers (**MRNs**) and patient chart numbers	Jun-24-2013	Manager informed PAO and deleted the email from inbox and deleted folders. ATC Analyst deleted the email from all folders	Jun-24-2013	Sender and recipient to delete email from their inbox, sent items and deleted items folders.	Jun-24-2013
Privacy Analyst	Jun-18-2013	CCO employee found a package containing patient ID number, name, DOB and health info in an envelope in the lobby of 620 University	External	Patient ID number, name, DOB and health info in a envelope in the lobby of 620 University	Jun-18-2013	Privacy analyst called hospital phone number on the package to report lost package and then hand delivered it to hospital employee	Jun-20-2013	No recommendations were provided as CCO was not the intended recipient of the misdirected package.	n/a
Business Unit	Jun-14-2013	Health centre submitted a cancellation file with 5 records to Operating Room Benchmark Collaborative (**ORBC**).	External	Cancellation file not sent via Tumbleweed used for low volume data submissions	Jun-07-2013	Surgical Efficiency Targets Program (**SETP**) administrator contacted SETP analyst at CCO by email and informed that an unencrypted file had been submitted to ORBC. It was then confirmed that this was a privacy breach and PAO would be informed.	Jun-14-2013	File should have been submitted in Tumbleweed and not ORBC	Jun-14-2013
Business Unit	Jun-14-2013	Hospital didn't encrypt their MRN and Account number prior to submitting to ORBC	External	MRN and Account	Jun-14-2013	CCO informatics conducted data quality analysis; identified issues with hospital submitting Cancellation file to ORBC that contained unencrypted Medical Record Number and Account Number. Sender contacted and informed of the breach, PAO informed and a breach report completed and submitted to PAO	Jun-14-2013	Such records have to be encrypted	Jun-14-2013
Business Unit	Jun-14-2013	Hospital didn't encrypt their MRN and Account number prior to submitting to ORBC	External	MRN and Account	Jun-13-2013	CCO informatics conducted data quality analysis; identified issues with hospital submitting Cancellation file to ORBC that contained unencrypted Medical Record Number and Account Number. Sender contacted and informed of the breach, PAO informed and a breach report completed and submitted to PAO	Jun-14-2013	Such records have to be encrypted	Jun-14-2013

Privacy Analyst	Jun-11-2013	Director rec'd an email with a letter to the CEO attached from external person. It contained client name, client health systems and health services provided. Letter was sent to 3 CCO employees	External	PH I - client name, client health systems and health services provided.	Jun-11-2013	Director notified all recipients that the email contained PHI, as well as the Privacy Analyst. The Privacy Analyst instructed all recipients to delete the email from their inboxes and deleted items folder. Privacy Analyst asked the Communications Officer to hand deliver a hard copy to the CEO's office. PAO - Privacy Analyst rec'd confirmation that all recipients of the email had deleted it from all folders.	June 11,2013	. All recipients of the email to delete it from their inbox, deleted items and/or their sent items folders	Jun-11-2013
Business Unit	Jun-03-2013	PHI Data in email to ATC Service Desk from Director Health Records Information at hospital	External	PHI in email	Jun-03-2013	Service Desk noticed PHI in email and removed the PHI content and advised PAO	Jun-03-2013	Sender informed transferring PHI in email is a privacy breach and should take appropriate steps in transferring such data.	Jun-03-2013
Privacy Analyst	May-31-2013	PHI data was included in an email to CCO ATC from hospital. Email contained patient name.	External	Patient name.	May-31-2013	Service Desk noticed PHI and removed PHI content, advised end user and PAO	May-31-2013	Service desk contact the sender and reiterated that PHI must not be sent via email	May-31-2013
Privacy Analyst	May-23-2013	Mgr PDRP rec'd a request for NDRP containing patient initials and Ontario Health Insurance Number (**OHIN**) along with requested drug and patient diagnosis which was then send to Case by CBCRP unintentionally leaving the PHI	External	Patient initials and OHIN along with requested drug and patient diagnosis	May-23-2013	Mgr notified all parties to deleted email from all boxes and informed PAO. Privacy Analyst rec'd confirmation that email had been deleted from all boxes	May-23-2013	No recommendations made.	May-23-2013
Shiva Dookie	May-22-2013	PHI data included in email to ATC Service Desk from wait list user at hospital. Email sent in effort to resolve an issues send was having with patient name correction	External	PHI in email	May-22-2013	Service desk noticed the PHI in the email and removed PHI content and advised PAO and end user. Service Desk to contact sender and inform them of the breach	May-22-2013	Sender informed transferring PHI in email is a privacy breach and should take appropriate steps in transferring such data.	May-22-2013
Privacy Analyst	May-21-2013	PHI data included in an email to Informatics Analyst from hospital	External	Patient info i.e. chart numbers, diagnosis code etc.	Feb-26-2013	sender asked to delete the email from all mailboxes and the Informatics Analyst also deleted it from all mailboxes and informed PAO	Feb-26-2013	Sender reminded to not send PHI via email	May-21-2013
Business Unit	May-21-2013	SETP admin. at health centre Facilities send SETP mailbox an email advising the Cancellation File for April 2013 had not been encrypted prior to uploading into ORBC and asking if resubmission was possible. Was told not further uploads are allowed and advised of privacy breach.	External	Cancellation file for April 2013 was uploaded into ORBC	May-13-2013	SETP informed of privacy breach and informed PAO. Breach report template completed and submitted to PAO	May-21-2013	Sender informed un-encrypted info being uploaded is a privacy breach	May-21-2013

Business Unit	May-21-2013	Hospital had submitted an unencrypted case input file to ORBC. Senior Business Analyst left voicemail advising the Hospital of the breach and followed up with an email.	External	Case input file in unencrypted format	May-21-2013	email sent to send advising of the privacy breach and PAO advised	May-21-2013	Sender informed un-encrypted info being sent to ORBC is a privacy breach	May-21-2013
Privacy Specialist	May-10-2013	SETP at hospital was having problem with data file and sent an email to SETP mailbox with the attached monthly data file extract containing record level personal health information (PHI) request SETP to resolve the issue	External	monthly data file extract containing record level personal health information (PHI)	May-10-2013	Senior Business Analyst emailed SETP Administrator to not attach record level data in emails and any emails submitted should be without record level data. The only secure method of data transfer to CCO is via ORBC or MFT.	May-10-2013	No data file transmission via email	May-10-2013
Privacy Specialist	May-03-2013	PHI data from hospital as sent to the CCO Help desk	External	MRN, patient name, and exam for 2 patients	May-03-2013	Sender deleted mail from all mailboxes and cc'd PAO and Help desk about it. PAO then found out that the MNR from the email thread was not deleted. Sender then deleted the thread.	May-10-2013	Sender reminded to not send PHI via email	May-03-2013
Privacy Specialist	Apr-15-2013	PHI was included in an email from hospital to OPIS Help Desk (**OHD**). The sender deleted the email within a minute but OHD had already read it.	External	Screenshot of MRN, patient name, DOB and gender for 1 patient	Apr-10-2013	OHD removed PHI content and advised end user & PAO	Apr-10-2013	Sender reminded to not send PHI via email	Apr-15-2013
Privacy Specialist	Apr-09-2013	PHI was included in an email to OHD from hospital	External	Screenshot of MRN	Apr-09-2013	OHD removed PHI content and advised end user & PAO	Apr-08-2013	Sender reminded to not send PHI via email	Apr-09-2013
Privacy Specialist	Apr-04-2013	PHI was included in an email to OHD from hospital	External	Screenshot of MRN	Apr-04-2013	OHD removed PHI content and advised end user & PAO	Apr-04-2013	Sender reminded to not send PHI via email	Apr-04-2013
Privacy Specialist	Apr-03-2013	PHI was included in an email to OHD from hospital	External	Screenshot of MRN	Apr-03-2013	OHD removed PHI content and advised end user & PAO	Apr-03-2013	Sender reminded to not send PHI via email	Apr-03-2013
Privacy Specialist	Mar-28-2013	OHI data was included in an email from hospital in an effort to resolve an issue the sender was having with OPIS	External	Screenshot of MRN, order date, and drug info for one patient	Mar-28-2013	OHD deleted the email from inbox and all deleted folders. OHD emailed sender to not send PHI via email and instructed them to delete email from all folders.	Mar-27-2013	No PHI with patient identifiers should be sent via email	Mar-28-2013
Privacy Specialist	Mar-28-2013	PHI data in email to ATC from a User at hospital in an effort to resolve an issue the sender was having with submitting data	External	MRN and patient name of 1 patient	Mar-28-2013	ATC helpdesk removed PHI and advised end user as well as PAO	Mar-28-2013	Sender reminded to not send PHI via email	Mar-28-2013
Privacy Specialist	Mar-21-2013	PHI data in a email to Project Manager and Devl. Lead at hospital. User there also cc'd	External	MRN, Health Card Number and DOB for 1 patient	Mar-21-2013	Project Mgr replied to the group with the information deleted, reminding them not to send patient identifiers via email. Email with PHI was deleted	Mar-21-2013	Sender reminded to not send PHI via email	Mar-21-2013

Privacy Specialist	Mar-20-2013	Hospitals submitted low volume data to ORBC	External	low volume data to ORBC (5 records)	Jan-13-2013	Email sent to each SETP admin. Letting them know of the violation. In June 2013 a bulletin and mandatory response survey was sent out reminding all hospitals of the process to upload low volume data submissions to Tumbleweed only	Jan-16-2013	Reminder bulletin was sent	Mar-20-2013
Privacy Specialist	Mar-18-2013	PHI data was included in an email to OHD from a Clinical Analyst at hospital.	External	Screen shot and patient name	Mar-18-2013	Reporter contacted the sender to re-iterate that PHI not be send via email and permanently delete from all mail boxes and to take appropriate steps in transferring PHI in the future	Mar-18-2013	Sender informed not to send PHI via email	Mar-18-2013
Privacy Specialist	Mar-18-2013	3 hospitals did not encrypt medical record numbers and account numbers prior to submitting data to ORBC.	External	non encrypted medical records and account numbers	Mar-18-2013	Email sent to each SETP admin. Letting them know of the violation. A SETP bulletin was sent to all SETP admin. To provide them a reminder about SETP privacy requirements and need to encrypt monthly data submissions files	Mar-18-2013	SETP sent notification to administrators in each hospital	Mar-18-2013
Privacy Specialist	Mar-18-2013	3 hospitals did not encrypt medical record numbers and account numbers prior to submitting data to ORBC	External	non encrypted medical records and account numbers	Mar-18-2013	Email sent to each SETP admin. Letting them know of the violation. A SETP bulletin was sent to all SETP admin. To provide them a reminder about SETP privacy requirements and need to encrypt monthly data submissions files	Mar-18-2013	SETP sent notification to administrators in each hospital admin	Mar-18-2013
Privacy Specialist	Mar-07-2013	PHI data in email to ATC from a User at a hospital in an effort to resolve an issue the sender was having with submitting data	External	Screenshot.	Mar-07-2013	Reporter of the breach immediately deleted the PHI therefore nature and extend of PHI not known.	Mar-07-2013	No recommendations were made as the circumstances surrounding this email are unknown.	Mar-07-2013
Privacy Specialist	Mar-06-2013	PHI data included in email to OHD from hospital.	External	MRN, Treatment date and drug info	Mar-06-2013	OHD removed PHI content and advised end user & PAO	Mar-06-2013	PAO, in partnership with EISO is assisting the business unit to resolve the ongoing issues surrounding the emailing of MRN along with other patient info	Mar-06-2013
Privacy Specialist	Feb-27-2013	PHI data was included in fax to general fax line at CCO from a physician's receptionist as she was using an old form	External	patient name, OHIN, diagnostic information for one patient	Feb-27-2013	All resolutions are complete as fax was destroyed and sender told not to send PHI via fax to the general fax line at CCO	Feb-27-2013	Sender reminded to not send PHI via fax	Feb-27-2013

Privacy Specialist	Feb-26-2013	PHI Data was included in an email to Analyst at CCO from hospital to resolve an issue sender was having with submitting data for Data Book ALR	External	Chart #s, diagnosis code and MRN	Feb-26-2013	Reporter contacted the sender and asked that the email be deleted from all folders, deleted his email folders and contacted PAO	Feb-26-2013	Sender reminded to not send PHI via email	Feb-26-2013
Privacy Specialist	Feb-22-2013	Under a DSA between data partner and CCO, CCO sends data to data partner once a year thru Tumbleweed. On two occasions, Oct, 2012 and Jan 2013 sent data to data partner. Included in the transfer were 2 tables of data not contained in the DSA. The Mgr sent the tables because, at that time, discussions were taking place about amendments to the DSA to facilitate transfer of the above tables.	Internal	The tables included medical information i.e. size of tumor, #of positive lymph nodes etc. as well as Cancer Checklist templates etc.	Feb-21-2013	The incident is a privacy risk as PHI was not transferred insecurely but in contravention of a Data Sharing Agreement thus creating a risky situation. Data partner is permitted to keep the additional tables, particularly since the current agreement is being negotiated to formalize this.	Feb-21-2013	Program to ensure that PHI is sent in accordance with any Data Sharing Agreements.	Feb-22-2013
Privacy Specialist	Feb-13-2013	PHI data was included in body of email to CCO services desk with issues re: open cases for a doctor in 2 separate emails from 2 user at hospital	External	OHIP # of 20 patients	Feb-13-2013	Service Desk removed PHI and advised end user and PAO	Feb-13-2013	Sender reminded to not send PHI via email	Feb-13-2013
Privacy Specialist	Feb-08-2013	PHI data was included in body of email to CCO services desk with issues being reported for duplicate entries from hospital	External	OHIP #, First and last name, DOB, Service location, Medical record # of 1 patient	Feb-08-2013	Service Desk removed PHI and advised end user and PAO	Feb-08-2013	Sender reminded to not send PHI via email	Feb-08-2013
Privacy Specialist	Feb-06-2013	14 patients names were sent in an email from Sr. QA Analyst to QA team leader and Sr. Programmer Analyst	Internal	First and last name of 14 patients	Feb-06-2013	Privacy report was completed and sent to PAO. Email deleted from all folders.	Feb-06-2013	Sender reminded to not send PHI via email	Feb-06-2013
Privacy Specialist	Feb-06-2013	PDRP Associate emailed a document that contained a OHIP#. Associate sent by mistake wrong version of file that was being edited using "Redactit"	Internal	OHIP #	Feb-06-2013	PDRP associate contacted all who received the email to delete the attachment containing the PHI from all folders	Feb-06-2013	Sender reminded to not send PHI via email	Feb-06-2013
Privacy Specialist	Feb-05-2013	PHI was included in email to Product Manager (**Mgr**) from Senior Informatics Analyst within CCO	Internal	2 renal patients IDs with last treatment type and active/inactive status	Feb-05-2013	Product Mgr deleted email and notified sender to do as well	Feb-05-2013	Sender reminded to not send PHI via email	Feb-05-2013
Privacy Specialist	Feb-04-2013	PHI data was included in an email to CCO Service Desk as an attachment in reference to a compliance feedback	External	Patient's name, OHIN of 114 patients	Feb-04-2013	CCO Service desk removed PHI content and advised end user and PAO	Feb-05-2013	Sender reminded to not send PHI via email	Feb-05-2013
Privacy Specialist	Jan-28-2013	PHI data in email to ATC from a User at a hospital in an effort to resolve an issue the sender was having with submitting data	External	MRN, Treatment date and drug info	Jan-25-2013	OHD removed PHI content and advised end user & PAO	Jan-25-2013	PAO, in partnership with EISO is assisting the business unit to resolve the ongoing issues surrounding the emailing of MRN along with other patient info	Jan-25-2013

Privacy Specialist	Jan-25-2013	Email containing PHI (data elements unknown as recipient deleted it before contacting PAO was sent to Supervisor at Finance Dept. and 2 employees at hospital	External	data elements unknown as it was deleted	Jan-25-2013	Supervisor at Finance at CCO deleted email with PHI from all mail boxes. Email was sent to the other recipients to also deleted from all folders	Jan-25-2013	sender informed not to send PHI via email	Jan-24-2013
Privacy Specialist	Jan-18-2013	PHI data was included in an email to OHD from hospital	External	MRN, treatment date & drug information	Jun-18-2013	OHD removed PHI content and advised end user and closed OHD ticket # 128368 - info never entered into SDE. Advised PAO	Jan-16-2013	Sender reminded to not send PHI via email	Jan-16-2013
Privacy Specialist	Jan-17-2013	SETP admin having trouble reading reports thru ORBC emailed Senior (**Sr.**) Bus. Analyst and attached an extract from her record level data file	External	data elements included in the record level data file	Jan-17-2013	Email was discovered during a telephone conversation with many of the senders' peers. After teleconference, an email was sent to the sender to not attached record level data instead to send an email and the SEPT member would contact her w/ resolution steps	Jan-17-2013	Sender reminded to not send PHI via email	Jan-17-2013
Privacy Specialist	Jan-16-2013	PHI data was included in an email to OHD from hospital	External	MRN, OHIN and patient initials	Jan-16-2013	OHD removed PHI content and advised end user & PAO	Jun-16-2013	Sender reminded to not send PHI via email	Jan-16-2013
Privacy Specialist	Jan-15-2013	PHI data in email to OHD from hospital	External	MRN and treatment date	Jan-15-2013	OHD removed PHI content and advised end user & PAO	Jan-15-2013	Sender reminded to not send PHI via email	Jan-15-2013
Privacy Specialist	Jan-09-2013	PHI data in email to OHD from hospital	External	MRN and drug information	Jan-09-2013	OHD removed PHI content and advised end user & PAO	Jan-09-2013	Sender reminded to not send PHI via email	Jan-09-2013
Privacy Specialist	Jan-08-2013	New SETP admin. at hospital sent at email to SETP mailbox with attached monthly data file extract containing patient info.	External	patient info in the data elements (Appendix A of original)	Jan-08-2013	Phone call was made to sender to not attach record level data with email and advised secure method was via ORBS through managed file transfer (MFT)	Jan-07-2013	Sender reminded to not send PHI via email	Jan-07-2013
Privacy Specialist	Jan-07-2013	PHI data in email to OHD from a health centre	External	MRH, Treatment date and Drug Information	Jan-07-2013	OHD removed PHI content and advised end user & PAO	Jan-07-2013	Sender reminded to not send PHI via email	Jan-07-2013
Privacy Specialist	Jan-04-2013	PHI data in an email attachment to SSPA from ADT interface person at the hospital where OPIS is currently being implemented	External	MRN and patient name	Jan-04-2013	SSPA removed the PHI content and advised end user to delete it too. PAO was notified	Jan-04-2013	Sender reminded to not send PHI via email	Jan-04-2013
Privacy Analyst	Dec-21-2012	CBCRP was submitted by fax to CCO general fax line from hospital. Fax contained patient name, HIN, diagnosis and why individual needed a drug funded	External	Fax contained patient name, HIN, diagnosis and explanation or why the individual needed a drug funded	Dec-21-2012	Reception notified Director of Provincial Drugs Reimbursement Program to pick up fax, and Receptionist deleted fax from in box and deleted items. Director of Provincial Drug Reimbursement Programs to contact hospital and explain		Unknown	Unknown

						them the proper method to submit cases to the CBCRP			
Privacy Specialist	Dec-03-2012	PHI data was sent in an email to Informatics Ctr of Excellence in an effort to resolve an issue with Regional Systemic Treatment Program MDS	External	PHI with patient chart and diagnosis code	Dec-03-2012	Informatics notified PAO, contacted the PAO, deleted the email from inbox and deleted folder. Informed the sender of CCO's policy regarding PHI and asked to permanently delete email containing the PHI	Dec-03-2012	Reporter contacted the sender via email to re-iterate that PHI not be sent via email. Permanently delete from both senders and recipient mail boxes and cautioned the sender to take appropriate steps in transferring of PHI in future	Unknown
Privacy Specialist	Nov-30-2012	PHI data (MRN, treatment dates, disease info) was included in an email to OHD from a pharmacist at hospital	external	PHI - MRN, treatment dates, disease info, included in an email	Dec-04-2012	OHD contacted the PAO, deleted the email from inbox and deleted folder. Informed the sender of CCO's policy regarding PHI and asked to permanently delete email containing the PHI	Dec-04-2012	Informed the sender of CCO's policy regarding PHI and asked to permanently delete email containing the PHI	Unknown
Privacy Specialist	Nov-29-2012	PHI data (MRN, treatment dates, disease info) was included in an email to OHD from a pharmacist at hospital	external	PHI - MRN - gender and DOB	Nov-29-2012	OHD contacted the PAO, deleted the email from inbox and deleted folder. OHD emailed sender standard PHI reply approved by PAO.	Nov-20-2012	Informed the sender of CCO's policy regarding PHI and asked to permanently delete email containing the PHI	Unknown
Privacy Specialist	Nov-29-2012	PHI data was included in an email to OHD. Sender sent it in to resolve issue with OPIS	external	PHI - patient name, MRN and NDFP	Nov-30-2012	OHD deleted the email from inbox and deleted folders and emailed sender the standard PHI rely approved by PAO	Nov-30-2012	sender contacted via email to reiterate that PHI must not be sent via email and to delete it from all mail boxes. Cautioned sender to take appropriate steps in transferring PHI in future	Unknown
Privacy Specialist	Nov-27-2012	Email with PHI was sent to CCO. Sent in an effort to resolve sender was having with submitting test data for CCO databook	External	PHI included patient registration number and diagnosis registration info	Nov-27-2012	Systemic Treatment Information Program (**STIP**) deleted email with PHI from inbox and deleted folders immediately and asked sender to not send PHI to CCO	Nov-27-2012	sender contacted via email to reiterate that PHI must not be sent via email and to delete it from all mail boxes. Cautioned sender to take appropriate steps in transferring PHI in future	Unknown

Privacy Specialist	Nov-23-2012	Email with PHI was sent to 4 CCO individuals in response to an inquiry from CCO's Systemic Therapy Program for a project on data collection and reporting system for Specialized Cancer Care Oversight Services	internal	Email contained eligibility forms with patient tracking #, prescribing doctor (**MD**), exam date, radiopharmaceutical, date of MD signature and spreadsheet with more info	Nov-23-2012	one recipient email PAO who in turn requested that a privacy breach report be filled out	Nov-23-2012	The program was previously advised by PAO that emailing of patient tracking number with associated patient info is not PHI. However, PAO is currently reviewing its de-identification guidelines and best practices for transferring of unique identifiers such as patient tracking number	Unknown
Privacy Specialist	Nov-20-2012	PHI data included in email to Helpdesk. Issue was to resolve WTIS	External	PHI - DOB	Oct-19-2012	Helpdesk replied to the sender informing that email had PHI in it. He removed the PHI and deleted the mail fro inbox and deleted folders. Informed send to do the same and advised PAO		Helpdesk took steps detailed in "description of immediate steps taken to contain incident"	Nov-20-2012
Privacy Specialist	Nov-19-2012	PMH submitted low volume data (3records) to Operating Room Benchmark Collaborative application. It is a violation to use Tumbleweed for low volume data submissions	External	Low volume data (3 records)	Nov-19-2012	Email sent to SETP about the violation and PAO would determine if further action was required. A bulletin was sent reminding all of the process and was acknowledge by the person in question and replacement was also informed. A survey was completed and acknowledged that they were aware of the process		Unknown	Unknown
Privacy Specialist	Nov-19-2012	Two hospitals submitted low volume data (5records) to Operating Room Benchmark Collaborative application. It is a violation to use Tumbleweed for low volume data submissions	External	low volume data (5 records)	Nov-19-2012	Email sent to SETP about the violation and PAO would determine if further action was required. A bulletin was sent reminding all of the process and was acknowledge by the person in question and replacement was also informed. A survey was completed and acknowledged that they were aware of the process		Unknown	Unknown
Privacy Specialist	Nov-19-2012	525 elevator door opened into the washroom hallway and was thus accessible without using security pass and thus a possibility an unauthorized person could have accessed	Internal	possibility that someone could have had access to the floor without using security pass	Nov 19, 2012	PAO was advised via email and Director of Facilities was also advised. There is no reason to suspect that unauthorized person could have had access to PHI, it does not constitute a privacy breach		Unknown	Unknown

Privacy Specialist	Nov-14-2012	PHI data was included in STIP related email to CCO in an effort to resolve an issues with Admission/Discharge/Transfer interface and thought since it was encrypted it was OK to send	External	PHI included next of kin and patient health card #	Nov-14-2012	Emails deleted from inbox and deleted folders immediately. Sender informed to not to send files to CCO		sender contacted via email to reiterate that PHI must not be sent via email and to delete it from all mail boxes. Cautioned sender to take appropriate steps in transferring PHI in future	Unknown
Privacy Specialist	Nov-08-2012	PHI was included in a fax from hospital physician to the CCO general fax line	external	Hospital sent fax to CCO general line, intended for CCO positron emission Tomography (PET) with patient name, treatment details, PET scanning	7-Nov.12	Privacy Specialist instructed Reception to permanently delete email from fax inbox and Privacy Specialist would contact the sender. Also ensure the physical document was shredded	8-Nov.12	delete the fax from the inbox and deleted items folder. Physical document was shredded and sender was notified of the breach.	Unknown
Privacy Specialist	Nov-08-2012	PHI data was included in email to CCO in an effort sender was having with LRT. Initially record was submitted in error and after a month of attempts to resubmit the record it was finally sent. Sender sent an email confirmation to CCO with PHI data for this record	Internal	PHI contained DOB, Patient name, and HIN	Nov-08-2012	Emails deleted from inbox and deleted folders immediately. Sender informed to delete it from its inbox and deleted folders. Help desk was sent an email for the purpose of submitting a record to LRT		Sender contacted via email to reiterate that PHI must not be sent via email and to delete it from all mail boxes. Cautioned sender to take appropriate steps in transferring PHI in future	Unknown
Privacy Specialist	Nov-07-2012	Email with PHI was sent to CCO. Sent in an effort to resolve sender was having with submitting test data for CCO databook	External	PHI contained registration # and diagnosis registration info	Nov-07-2012	Emails deleted from inbox and deleted folders immediately. Sender informed to not to send files to CCO		Sender asked not to send data to CCO	Unknown
Privacy Specialist	Nov-06-2012	PHI data included in email to OHD. Issue was to resolve OPIS	External	Phi contained MRN, Gender, DOB, address	Nov-06-2012	OHD contacted the PAO, deleted the email from inbox and deleted folder. OHD emailed sender standard PHI reply approved by PAO.	Nov-06-2012	Informed the sender of CCO's policy regarding PHI and asked to permanently delete email containing the PHI	Unknown
Privacy Specialist	Nov-05-2012	PHI data included in email to OHD. Issue was to resolve OPIS	External	PHI contained MRN, treatment date, drug info	Nov-05-2012	OHD contacted the PAO, deleted the email from inbox and deleted folder. OHD emailed sender standard PHI reply approved by PAO.	Nov-05-2012	Informed the sender of CCO's policy regarding PHI and asked to permanently delete email containing the PHI	Unknown

Privacy Specialist	Oct-29-2012	A "failed Fax" notice was left at 505, 16th fl printer. The body contained a medical report from one physician to another	internal	Fax failed as there was no answer and no one outside CCO received it. It was ultimately determined that fax was sent by CCO employee on behalf of a family member	Oct-29-2012	PAO notified. The sender was advised of her obligation concerning the safe handling of PHI in the custody and control of CCO. She was contacted again by her director to reiterate that PHI must not be left on fax machine or anywhere else that individuals not requiring access could access it	Oct-22-2012	The sender was advised of her obligation concerning the safe handling of PHI in the custody and control of CCO. She was contacted again by her director to reiterate that PHI must not be left on fax machine or anywhere else that individuals not requiring access could access it	Unknown
Privacy Specialist	Oct-24-2012	email from OHD contained PHI. Was sent in an effort to resolve issue sender was having with OPIS	External	PHI - MRH, treatment date, drug info	Oct-23-2012	OHD removed PHI content and advised end user and PAO.	Oct-23-2012	sender contacted via email to reiterate that PHI must not be sent via email and to delete it from all mail boxes. Cautioned sender to take appropriate steps in transferring PHI in future	Unknown
Privacy Specialist	Oct-17-2012	MRN-PHI data was included in email from employee sent in an effort to resolve issues sender was having with submitting data for the WTIS	external	PHI - MRN included in an email	Oct-17-2012	CCO helpdesk deleted email from inbox and deleted folders. Sender emailed that PHI was sent in an email and instructed them to delete the email from sent and deleted folders. PAO-CCO notified	Oct-10-2012	CCO Helpdesk took steps detailed in "description of immediate steps taken to contain the incident	Unknown
Privacy Specialist	Oct-16-2012	Hospital submitted low volume data (5 records) to ORBC application. This is a violation- PAO recommended in Feb 2012 to use Tumbleweed for low volume data submission (< 5 records)	External	low volume data		email sent to hospitals Primary and back up SETP administrators indicating they had violated previously communicated SETP privacy policy and the PAO would be consulted if any further action was required	Oct-16-2012	CCO Informatics conduction data quality analysis: identified issue with hospital submitting low volume data submissions through ORBC	Unknown
Privacy Specialist	Oct-12-2012	Potential PHI was included on a sample form posted on Chronic Kidney Disease Reg Leadership Site. PHI included potential name of Patient, Unit # and Physician name	External	PHI included potential name of Patient, Unit # and Physician name	Oct-12-2012	Form containing the PHI was deleted from the site and also deleted from the recycling bin. After running the report of registered users of the site, it was determined that potentially 5 users could have viewed the document and Internally approx. 7 users. The audit report was snot enabled, therefore no confirmation if anybody viewed the document		Unknown	Unknown

Privacy Specialist	Oct-11-2012	PHI data was included in an internal CCO email from employee to 5 individuals containing 12 patient records including all kinds of PHI data elements	internal	12 patients PHI patients health card #, DOB, address, gender etc sent in an email to 5 individuals	Aug-08-2012	Upon receipt, team was asked and confirmation received to permanently delete message from inbox/deleted items. It was made sure that everyone understood that PHI cannot be emailed.	Aug-09-2012	Sender of PHI to re-do the Privacy Refresher training	Unknown
Privacy Specialist	Oct-10-2012	MRN-PHI data was included in email from employee sent in an effort to resolve issues sender was having with submitting data for the Wait time Info System	external	PHI - MRN included in an email	Oct-10-2012	CCO helpdesk deleted email from inbox and deleted folders. Sender emailed that PHI was sent in an email and instructed them to deleted the email from sent and deleted folders. PAO-CCO notified	Oct-10-2012	CCO Helpdesk took steps detailed in "description of immediate steps taken to contain the incident	Unknown
Privacy Specialist	Oct-03-2012	Hospital requested reactivation of account. After reset, hospital employee was able to access patient info from all centers and notified CCO	external	PHI - name, DOB, disease info and treatment	Oct-02-2012	IT revokes access to all centers in the application and provide access to the required site only	Oct-03-2012	IT revoked access to all centers in the application and provide access to the required site only	Unknown
Privacy Specialist	Sep-27-2012	text message which created a “white list” email that was linked to PHI	External	PHI	Sep-20-2012	Access to environment containing PHI was restricted until PHI was resolved from affected environments		All short term resolution activities are completed as ATC contacted the sender of the PHI into the conformance environment to reiterate all PHI be sent to the production environment only and cautioned sender to take appropriate steps in transferring PHI in future	Unknown
Privacy Specialist	Sep-19-2012	PHI was included in 4 emails sent to OPIS Helpdesk from OPIS users at various hospital	External	PHI contained MRN, drug and disease info	Sep-19-2012	OPIS reminded by PAO that MRN plus any other patient info sent in an email constitutes a break.	Sep-19-2012	sender contacted via email to reiterate that PHI must not be sent via email and to delete it from all mail boxes. Cautioned sender to take appropriate steps in transferring PHI in future	Unknown
Privacy Specialist	Sep-07-2012	PHI data was included in an email to ATC from employee. It was to resolve issue with Wait Time.	external	PHI contained patient name and MRN	10-Sepr-12	Helpdesk replied to the sender informing that email had PHI in it. He removed the PHI and deleted the mail from inbox and deleted folders. Informed send to do the same	Sep-10-2012	sender contacted via email to reiterate that PHI must not be sent via email and to delete it from all mail boxes. Cautioned sender to take appropriate steps in transferring PHI in	Unknown

								future	
Privacy Specialist	Jul-26-2012	Screenshot of PHI data was sent in an email to ATC	external	PHI data	Jul-26-2012	ATCH deleted email from their inbox and deleted items. Help desk was informed and told to delete the email in sent and deleted items. The ticket was closed and a separate one was created without the PHI	26-07-12	Breach was contained as a result of: 1) reporter contacted send of PHI and re-iterated that PHI must not be emailed 2) email permanently deleted from both senders and recipients mailboxes 3) Reporter cautioned sender to take appropriate steps in transferring PHI in future	Unknown
Privacy Analyst	Jun-21-2012	Data file for Breast Intensity Modulated Radiation Therapy (**IMRT**) indicator with MRN numbers sent via email from hospitalto 3 CCO employees in and effort to resolve a technical issue with their data book upload.	External	Data file for Breast IMRT indicator with MRN numbers	June 21. 2012	Informatics employee deleted email for Inbox and deleted items. Informatics employee notified hospital that they had sent PHI via email and that this is a breach of our Info. Security Code of Conduct. Informatics employee also notified the other two CCO staff members who received the email that email contained PHI and both those staff members deleted the email from the inbox and deleted items before opening it.	Jun-25-2012	Bulletin to be sent to all participating hospitals reminding them not to submit PHI over email	Jun-19-2012
Privacy Analyst	Jun-21-2012	Screenshot of PHI data was included in an email to service Desk from a radiation therapy clerk at hospital in an effort to resolve an issue the sender was having with submitting data for WTIS	External	Screenshot of PHI data	Jun-21-2012	Service desk deleted the email from their inbox and deleted items. Service desk emailed the sender, informed them that the email they had sent contained PHI and instructed them to delete the email from their sent items and deleted items	Jun-21-2012	Service desk to contact the sender of the PHI via email to re0iterate that all PHI must not be sent via email. Service Desk at ATC will caution the sender to take the appropriate and expected steps in transferring PHI in the future. PAO to notify the Privacy Office at Hospital of this breach and request confirmation of the steps taken in responding to this breach. Bulletin to be	Jun-21-2012

								sent to all participating hospitals reminding them not to submit PHI over email	
Business Unit	Jun-21-2012	Data file for Breast IMRT indicator with MRN numbers sent via email from hospitalto 3 CCO employees in and effort to resolve a technical issue with their data book upload.	External	Data file for Breast IMRT indicator with MRN numbers	Jun-21-2012	Informatics employee deleted email for Inbox and deleted items. Informatics employee notified hospital that they had sent PHI via email and that this is a breach of our Info. Security Code of Conduct. Informatics employee also notified the other two CCO staff members who received the email that email contained PHI and both those staff members deleted the email from the inbox and deleted items before opening it.	Jun-25-2012	Bulletin to be sent to all participating hospitals reminding them not to submit PHI over email	June 25. 2012
Business Unit	Jun-21-2012	Screenshot of PHI data was included in an email to service Desk from a radiation therapy clerk at hospital in an effort to resolve an issue the sender was having with submitting data for WTIS	External	Screenshot of PHI data	Jun-21-2012	Service desk deleted the email from their inbox and deleted items. Service desk emailed the sender, informed them that the email they had sent contained PHI and instructed them to delete the email from their sent items and deleted items	Jun-21-2012	Service desk to contact the sender of the PHI via email to re-iterate that all PHI must not be sent via email. Service Desk at ATC will caution the sender to take the appropriate and expected steps in transferring PHI in the future. PAO to notify the PAO at Hospital of this breach and request confirmation of the steps taken in responding to this breach. Bulletin to be sent to all participating hospitals reminding them not to submit PHI over email	Jun-21-2012

Privacy Analyst	Jun-20-2012	Hospital sent production data via “Health Level 7” (**HL7**) messages to a test environment. These HL7 messages contained PHI. The facility's interface was pointed to the incorrect IP address.	External	Production data via HL7 messages to a test environment. These HL7 messages contained PHI.	Jun-19-2012	WTIS test environments were made unavailable to users. eHealth was notified and EMPI Conformance environment was subsequently taken offline. Communication to WTIS users was issued advising that the test environments and EMPI conformance would be unavailable until further notice. Complete list of records that may contain PHI was sent to eHealth and CCO IT Operations so that the PHI data could be scrubbed prior to making the environments available to users.	Jun-20-2012	ATC to contact the sender of the PHI into the conformance environment to reiterate that all PHI must be sent to the production environment only, ATC will caution the sender to take the appropriate and expected steps in transferring PHI in the future. PAO to notify the Privacy Officer at hospital of this breach and request confirmation of the steps taken in responding to the breach. Bulletin to be sent to all the participating hospitals reminding them to submit PHI to the production environment only.	Jun-20-2012
Privacy Specialist	Jun-19-2012	June 18, 2012 A document relating to eligibility for breast cancer screening that contained PHI was found unattended at a printing station on the 13th floor at 505 University by a CCO employee	Internal	A document relating to eligibility for breast cancer screening that contained PHI	Jun-19-2012	The document was uploaded to the H drive for secure storage and the original paper copy was shredded	Jun-28-2012	Since the owner of the document cannot be identified and the PHI cannot be returned, the reporter of the breach to be advised to delete document containing PHI from the H: drive.	
Privacy Specialist	Jun-15-2012	3 hospitals submitted low volume data submissions to ORBC. This violation of a policy that was recommended by the PAO in Feb 2012 to use Tumbleweed for low volume data submissions. The policy for low volume data submissions has been communicated to hospitals through several bulletins and in a Tumbleweed Instructional Guide. In addition, the SETP data Check Tool was enhanced to identify low volume submissions and prompt hospitals to submit these through Tumbleweed and not ORBC	External	Low volume data submissions to ORBC.		An email was sent to all 3 hospitals indicating they had violated the previously communicated SETP privacy policy and that the CCO PAO would be consulted to determine if further actions were required.	Jun-25-2012	The Briefing not prepared by the P&A office on Feb 2, 2012 confirms that mitigating strategies were implemented to address the high risk reports/data sets. In order to meet the suggested strategy for risk mitigations set out in the de-identification guidelines the: Surgery date must be removed, data must be encrypted or altered to a partial	Jun-25-2012

								date for the transmission from HICs to service provider, Small cell suppression (where n<=5) must be applied by the Hospital when disclosing data to service provider and when hospitals are submitting records of less than 5, they will be instructed to use Tumbleweed. If the strategies are not properly implemented to de-identify the data then any improper disclosure of data would constitute a 'breach of PHI"	
Privacy Analyst	Jun-12-2012	CCO Staff member picked up the transmission log from the counter in the photocopy room and looked at it to try to decipher whose fax it may be finding that it contained PHI. CCO staff member put the transmission log back on the fax machine for someone to claim it. When no one claimed it by 5pm, CCO staff member contacted the PAO through email. CCO staff member kept the transmission log in a locked drawer in her desk until she heard back from the PAO as to what the next steps would be	Internal	Transmission log at the fax machine that contained PHI	Jun-13-2012	Member of the P&A office picked up the transmission sheet and locked it away. Also asked the CCO staffer who found the transmission log and asked for a list of programs on the 16th floor. Privacy staff member contacted the OFCCR program to see if one of their staff members faxed pathology info on June 12. OFCCR manager identified the CCO staff member who did. Transmission log was shredded on June 15, 2012	Jun-15-2012	OFCCR Program Manager informed the P&A office that she has re-informed all OFCCR staff to use cover sheets when faxing and wait for the transmission log. CCO staff member who sent the fax to re-do Privacy & Security training and send the PAO a signed acknowledgment form that training has been re-completed. CCO staff member who discovered the fax transmission log to review CCO's Privacy Breach Management Procedure.	Jul-04-2012
Privacy Specialist	Jun-07-2012	Health card numbers received via emailed from Data Analyst at hospital.	External	Health card numbers	Jun-07-2012	Email deleted in inbox and deleted items folder. Notified sender of the breach	Jun-07-2012	Manager, DAP to speak with analyst as soon as possible about this incident and to discuss ways to prevent future incidents. Manager, DAP to send out and email to all regions	Jun-07-2012

								reminding staff not to email PHI. Sender - to undergo remedial training and complete the Privacy & Security Modules. Sender to also sign a document attesting to the completion of the Modules	
Privacy Analyst	May-17-2012	Project Document (Change Request) Containing PHI circulated internally to 6 team members via email. The PHI documentation in question was a completed screening report form containing patient's address, exam results and physicians name	Internal	Project Document (Change Request) Containing a completed screening report form containing patient's address, exam results and physicians name	May-08-2012	Team member were directed to delete any emails containing the Change Request and/or PHI from all email boxes. The PHI page within the Project Change Request has been deleted from P: drive	May-17-2012	Sender of email to undergo remedial training and complete Privacy & Security Modules. Sender to sign a doc. Attesting to the completion of the modules and provide the signed attestation to the PAO. QA Lead and Program Manager to establish responsibilities for the process of reporting privacy breaches to the PAO in the future.	Jun-25-2012
Privacy Specialist	Apr-20-2012	An OBSP result letter containing PHI was marked 'return to sender' and was sent by mail to CCO. Letter generated by OBSP regional site and not CCO. Letter received and opened by a CCO employee to determine where it was to be directed. The person opening the letter did not think it would have PHI. Letter was provided to the ICS Contact Centre for follow-up.	Internal	PHI in a letter relating to OBSP	Apr-20-2012	The Senior Project Manager, ICS Regional Operations, provided the letter containing the PHI to the ICS contact Centre in order that they may conduct an investigation into the misdirected correspondence. The PAO was notified.	Apr-23-2012	CCO should consider implementing a requirement for OBSP sites mandating that the correct return address be clearly indicated on the envelope	Apr-23-2012
Privacy Specialist	Mar-09-2012	An email containing PHI of approximately 9 individuals was sent from a CCO employee to two other CCO employees in Quality Assurance Services	Internal	Email containing PHI	Mar-09-2012	The sender and both recipients were advised to delete the email containing PHI from all Sent, Inbox and Deleted Items folders	Mar-09-2012	Manager, Quality Assurance Services, to send out email reminding staff not to email PHI. Sender of email to undergo remedial training and complete all Privacy & Security Modules. Sender also to sign a document attesting to the completion of the	Apr-12-2012

						modules.			
Privacy Specialist	Dec-12-2011	Email w/ PHI sent by CCO employee to two CCO employees	Internal	Email containing PHI		Sender and recipients deleted emails. Sender confirmed that the email was not sent to anyone else	Dec. 5, 2011	Unknown	Unknown
Privacy Specialist	Dec-05-2011	An email containing PHI was sent by a CCO employee to two other CCO employees	Internal	Unknown	Dec-05-2011	P&A office requested that the email be deleted from all CCO mail boxes - deletions confirmed	Jan-27-2012	All CCO employees to be reminded that PHI must not be sent by email via the annual refresher training and Senior Program Manager, Prevention and Screening to send out an email reminding staff not to email PHI. Confirm EISO policy does not require removal of emails containing PHI from backups.	Dec. 31, 2011/ Jan. 22, 2012 / Jan. 30, 2012
Privacy Manager	Nov-03-2011	PHI was saved in a location (JIRA, name of an IT Tool – not an acronym) where unauthorized users may have been able to access it.	Internal	Unknown	Nov-03-2011	Report containing PHI was removed from the JIRA. Privacy Lead investigated whether unauthorized users had accessed the report and it was determined that, though there is potential that unauthorized users could have accessed it, only a select group of people, all who are authorized to view PHI, would access it regularly.	Nov-09-2011	Unknown	Unknown

Summary of PP Breaches (non-Contact Center)

for the period between November 1st, 2011 to October 31st , 2013

Title	Date of Breach Report	Investigating Agent	Date of Incident	Date Sr. Mgmt Notified	Extent of Breach	Internal vs External	Nature of PHI	Containment Measure	Date Investigation Completed	Recommendation

Fax containing Participant Information form sent to CCO's general fax line	Oct-30-13	Privacy Analyst	Oct-25-13	Oct-25-13	Fax with Participant Information Form sent by client who wanted to withdraw from correspondence for all CCO's screen programs. Fax should have been sent to the Contact Centre via secure fax provided on the sheet provided with the form. Receptionist sent an email to Privacy mailbox believing fax was misdirected as she did not read the attachment	External	PHI - patient name, date of birth, phone, address, health card number.	Privacy Analyst informed receptionist to delete email from all mailboxes. Analyst uploaded the PDF fax into InScreen and deleted the email from all mailboxes.	Oct-25-13	Fax should have been sent to the Contact Centre via secure fax
Fax containing Participant Information form sent to CCO's general fax line	Oct-29-13	Privacy Analyst	Oct-27-13	Oct-28-13	Fax with Participant Information Form sent by client who wanted to withdraw from correspondence for all CCO's screen programs. Fax should have been sent to the Contact Centre via secure fax provided on the sheet provided with the form. Receptionist provided a hard copy to the Privacy Analyst.	External	PHI - patient name, date of birth, phone, address, health card number.	Receptionist brought hard copy to Privacy. Privacy analyst hand delivered the hard copy of fax to Contact Centre.	Oct-28-13	Fax should have been sent to the Contact Centre via secure fax.
PHI in fax to CCO general fax line	Oct-29-13	Privacy Analyst	Oct-28-13	Oct-28-13	Fax containing OBSP high-risk requisition for a mammogram was sent to CCO's fax line instead of the screen site.	External	PHI - patient name, date of birth, telephone number, address, description of patient high risk status.	Physician's office faxed the requisition to CCO's primary fax number. Reception reported the breach to Privacy who then let the sender know.	Oct-28-13	Sender advised where to direct fax.
Email to Privacy mailbox	Oct-8-13	Privacy Analyst	Oct-8-13	Oct-8-13	Client enrolled in CCO operated screen program sent an email to the Privacy mailbox to request an address update.	External	Client's name, address phone number, screen program and description of previously completed screen tests.	Privacy Analyst uploaded the email into InScreen to enable the Contact Centre to follow-up and then deleted the email from all folders.	Oct-9-13	Sender advised not to send PHI by email.
Email in Privacy mailbox	Oct-8-13	Privacy Analyst	Oct-8-13	Oct-8-13	Email to Privacy mailbox requesting an address update contained PHI.	External	Client's name, address, phone and screening program	Privacy Analyst uploaded the email into InScreen to enable the Contact Centre to follow-up and then deleted the email from all folders.	Oct-9-13	Sender advised not to send PHI by email.

Fax with patient info	Oct-3-13	Privacy Analyst	Oct-3-13	Oct-3-13	Physician's office faxed a patient information request to CC asking for mammogram results.	External	Patient name, address and test result request	When fax was discovered, Customer Services Representative logged the activity in physician's record, deleted the email containing the fax and reported the breach to Privacy.	Oct-3-13	Customer Services Representative called the Physician's office and instructed them to send such requests directly to the screen site of the patient and not the general inquiry line. Informed them that their action has resulted in a breach.
PHI in email	Sep-9-13	Privacy Analyst	Sep-4-13	Sep-5-13	PHI in an email to Senior Lead at Cancer Control.	External	PHI - name, age, telephone, email, and program name	Customer Services Representative was informed via email advising them that the email containing PHI has been deleted and notified Privacy of the breach.	Sep-5-13	Sender advised not to send PHI by email.
PHI over the phone to wife	Sep-4-13	Privacy Analyst	Sep-3-13	Sep-3-13	Caller asked to verify the address and ask CCO to send a FOBT kit. Analyst proceeded to authenticate and caller provided name, date of birth, address and thus disclosed PHI. The caller then asked access to her record at which point it was stated that she had called on her husband's behalf.	External	PHI - Name of client's physician and participation in CCC program	No further PHI was discussed with the caller. Caller had called posing as the husband. Privacy advised of the breach.	Sep-3-13	Caller informed CCO does not access nor disclose PHI to a spouse without authorization from the client.
PHI in fax	Aug-21-13	Privacy Analyst	Aug-22-13	Aug-22-13	Fax containing consultation notes and progress reports for 7 patients from a surgeon's office. It did not contain a cover sheet and was not intended for CCO and was intended for 7 different physicians providing care to the patients.	External	PHI - patients names, date of birth, and HINs	Facilities coordinator contacted Privacy to advice of the fax with PHI. Fax destroyed.	Aug-22-13	N/A. CCO was not the intended recipient.
PHI included in email sent to CCO OBSP inbox	Aug-16-13	Privacy Analyst	Aug-16-13	Aug-16-13	Email with PHI - name, date of birth, address and phone number, HIN	External	Name, date of birth, address and phone number, HIN	Analyst contacted Privacy, deleted from all email folders.	Aug-16-13	Called physician office and informed them of the breach and reminded them that all result inquiries to be direct to screen sites.

PHI in a fax to CCO OBSP email inbox	Aug-15-13	Privacy Analyst	Aug-16-13	Aug-16-13	Fax intended to transfer patient's files over to an Imaging Centre contained, name, date of birth and Heath Information Number (HIN)	External	Fax contained PHI - name, date of birth and HIN	Fax deleted from all mailboxes	Aug-16-13	Cancer Screening Program contacted Privacy and the sender and instructed them to direct results to the Imaging Centre.
PHI in email	Aug-7-13	Privacy Analyst	Aug-7-13	12-Aug-13	An email from a medical organization contained client's name and address. Subject line indicated type of cancer screening test client received	External	PHI - client name, address and test received	Privacy notified and requested organization to delete email from all folders and a breach report was completed	Aug-8-13	Organization reminded not to send PHI by email.
Potentially identifiable data in an email	Jul-22-13	Privacy Analyst	Jul-23-13	Jul-23-13	Potentially identifiable data sent in an email.	External	Colonoscopies by age group and how much they cost at a hospital	Once email sent, attempt to recall message failed. Privacy was notified as to next steps. Financial Planning Analyst confirmed that email had been deleted from all folders.	Jul-23-13	Sender advised not to send potentially identifiable information by email.
Email sent to wrong address	Jul-18-13	Privacy Analyst	Jul-17-13	Jul-18-13	Personal health information sent to wrong email address	External	Data included GI Endoscopy volumes broken down, including suite, day surgery etc. and potentially identifiable info i.e. cells counts below 5	Unintended recipient asked if she should forward it to correct LHIN CEO. She was advised not to forward and delete it from all folders. Project Manager would forward it. Privacy was informed and asked Project Manager to also delete it from all folders.	Jul-31-13	Privacy to advise on secure transfer for data including cell counts below 5.
PHI in email	Jun-19-2013	Privacy Analyst	Jun-20-2013	Jun-19-2013	Research associate sent PHI (table of patients who rec'd FOBT thru mobile coach including first name, middle, surname and accession ID in an email instead of being saved on H drive for the Sr. Project Analyst to pick up	Internal	PHI (table of patients who rec'd FOBT thru mobile coach including first name, middle, surname and accession ID)	When email rec'd by Sr. Project Analyst, he informed PAO of incident. All deleted email from their inbox/sent items and deleted items folder and Privacy analyst rec'd confirmation that the email had indeed been deleted.	Jun-19-2013	Sender and recipient to delete email from inbox, sent items and deleted items folders.
PHI in a voicemail in PAO Mail box	Jun-11-2013	Privacy Analyst	Jun-11-2013	Jun-11-2013	Voicemail with PHI was rec'd in the PAO mailbox. PAO coord. Then forwarded the voicemail in an email to the Privacy Analyst to advise on next steps.	Internal	Voicemail from the OBSP client wanting to update her address contained Client name, address and the fact she is enrolled in the OBSP	Privacy Analyst took down info on paper and called Cancer Screening Contact Centre and transferred the info for them to follow up. Privacy Analyst advised PAO coord. To delete voicemail from PAO inbox, send and deleted items and also deleted the email from her own mailboxes and deleted folders.	Jun-11-2013	Sender and recipient to delete email from inbox sent items and deleted items folders.
CCO Gen. Fax rec'd a request from	May 29 2013	Privacy Analyst	May-29-2013	May-29-2013	CCO Gen. Fax rec'd a request from hospital for mamo films for a client containing PHI	External	PHI - patient name, DOB, Health Insurance and dated of screening	620 Reception contacted PAO. Privacy Analyst retrieved hard copy of the fax and saved it to H drive to CCC to pick up.	May-29-2013	CCO is not the appropriate organization to receive requests for mamo films thus it constitutes

Alberta Health Services										an unauthorized collection of PHI
2 completed lab forms from lab sent to the Contact Centre	May-10-2013	Privacy Analyst	May-09-2013	May-09-2013	Contact Centre received 2 completed lab forms in separate envelopes from lab sent in error by lab staff	External	2 separate completed lab forms(requisitions) rec'd by Contact Center from lab	Lab was contacted as to why the forms were sent, and was asked to stop sending requisitions form in the Mail and to use CCO's Contact Center secure fax line instead. PAO notified	May 9,2013	Lab Analyst to contact lab and investigate why requisition forms were sent via regular mail and reiterated to lab to use CCO secure fax number
Contact Centre Representative (**CSR**) in a phone conversation disclosed test results to a family member	May-07-2013	Privacy Analyst	May-03-2013	May-03-2013	CSR in an attempt to contact a client with a positive FOBT result via phone unintentionally disclosed to a family member with the same name that a Colon Cancer test result was waiting to be sent.	internal	a positive FOBT result to a person with the same name	CSR, once finding out that it was not the right person, did not disclose any further info. PAO was informed.	May-07-2013	PAO is review scripts for unattached patients calls to ensure that no PHI is disclosed prior to the client being authenticated
CCO rec'd 2 excel files containing PHI via email and fwd it to a colleague in Informatics and to Cancer Screen inbox.	May-06-2013	Privacy Analyst	May-02-2013	May-02-2013	The excel files contained PHI i.e. Dates of data affected, patient names, Health Card # and patient chart #. Email with excel file sent by clinic	External	PHI i.e. Dates of data affected, patient names, Health Card # and patient chart #.	Individual managing the Screening Box notified Sr. Project Mgr and Informatics colleague. All 3 recipients deleted the email from their inbox/sent and deleted folders. Sr Project Mgr informed the Clinic to delete it from their folders too and instructed not to send PHI via email	May-02-2013	Sender of PHI informed CCO does not accept PHI via email. Recipients to delete email from all folders
PHI data in a fax	Apr-29-2013	Privacy Analyst	Apr-29-2013	Apr-29-2013	fax with PHI data sent to CCO from a doctor's office. Fax was a OBSP high risk form and should have been sent to OBSP site.	External	PHI - name, address, HIN, required tests and their enrolment in the OBSP program	Sender to be contacted and informed not to send these to CCO but to OBSP High Risk Form. Receptionist to delete fax from fax inbox and deleted folders.	Apr-29-2013	Sender to be contacted and informed not to send these to CCO but to OBSP High Risk Form. Receptionist to delete fax from fax inbox and deleted folders.

PHI data in fax	Apr-24-2013	Privacy Analyst	Apr-24-2013	Apr-24-2013	PHI data included in fax sent to CCO from doctor in Calgary asking for mamo records and ultrasound images for a client.	External	PHI data - name, DOB and health insurance #	Hard copy printed and deleted from all mail boxes by 620 reception. Hard copy walked over to CSP Contact Centre (**CC**). CC called the sender and informed them not to send to CCO but to OBSP site to obtain such records	Apr-25-2013	CSR asked sender in Calgary to not send such faxes to CCO. All recipients of the form to delete it from all mail boxes
PHI data in FEDex envelope	Apr-24-2013	Privacy Analyst	Apr-24-2013	Apr-24-2013	A returned FEDex envelope contained FOBST positive follow-up letter destined for Contact Centre was misdirected to CCO who opened it and return it to reception as address was wrong. The letter was sent to fulfillment house but FEDex was unable to deliver due to incorrect address. Was repackaged and sent to fulfillment house and due to the size of the package, was taped to the outside. The reception incorrectly referred it back to a "Tracy" at CCO who opened it thus a breach.	External	PHI - client name, address and test result info	Employee notified Analyst who picked up the envelope and began investigating the reason for breach. CCO contacted fulfillment house and it was determined that error occurred as the 2 letters were taped together and agreed in future to send all returned mail in one large envelope. Contact Centre notified PAO	Apr-21-2013	Fulfillment house to send all correspondence containing PHI in one envelope with a precise and clearly marked recipient
PHI data in fax	Apr-22-2013	Privacy Analyst	Apr-19-2013	Apr-18-2013	PHI data in fax fwd on to Cancer Screening email box thinking it was the recipient of it. Cancer Screening contact PAO advising there were not the proper recipient of the fax.	External	PHI data - gender, DOB, age, Doctor, Lab, urine chemistry test result, when taken etc.	fax deleted from all boxes and email.	Apr-22-2013	CSR asked sender to not send such faxes to CCO. All recipients of the form to delete it from all mail boxes
PHI in email	Apr-18-2013	Privacy Analyst	Apr-18-2013	Apr-18-2013	PHI data in a email to OBSP with fax attachment sent to 620 Reception. The fax was an OBSP High Risk Form	External	PHI Data in email - name, DOB, Health Insurance #	CSR contacted Privacy analyst and removed PHI content by deleting from the OBSP in box and deleted items. CSR contacted sender in Calgary and requested these form not be sent to CCO.	Apr-18-2013	CSR asked sender in Calgary to not send such faxes to CCO. All recipients of the form to delete it from all mail boxes
PHI data in fax	Apr-18-2013	Privacy Analyst	Apr-18-2013	Apr-18-2013	PHI data in fax fwd to Breast Screening mailbox sent by clinic in Calgary who needed past mamos of a client.	External	PHI data in fax - name, DOB, Health Insurance #	CSR contacted Privacy analyst and removed PHI content by deleting from the Breast Screening in box and deleted items. CSR contacted sender in Calgary and requested these form not be sent to CCO.	Apr-18-2013	CSR asked sender in Calgary to not send such faxes to CCO. All recipients of the form to delete it from all mail boxes

PHI in fax	Apr-16-2013	Privacy Analyst	Apr-16-2013	Apr-16-2013	A fax with PHI was fwd to reception at 620 university Avenue to OBSP inbox via email.	External	client's name, DOB and health insurance #	CSR removed PHI content by deleting it from the OBSP inbox and the deleted items. Also contacted sender in Calgary not to send these forms/requests to CCO	Apr-17-2013	CSR to inform sender not to send this form to CCO. CSR and reception-620 to delete the email/fax from all folders.
PHI in Email	Apr-16-2013	Privacy Analyst	Apr-16-2013	Apr-16-2013	PHI data in a email to OBSP with fax attachment sent to 620 Reception. The fax was an OBSP High Risk Form	External	PHI Data in email - name, DOB, Health Insurance #	CSR contacted Privacy analyst and removed PHI content by deleting from the OBSP in box and deleted items. CSR contact send in Calgary and requested these form not be sent to CCO.	Apr-17-2013	CSR asked sender in Calgary to not send such faxes to CCO. All recipients of the form to delete it from all mail boxes
PHI in fax	Apr-10-2013	Privacy Analyst	Apr-10-2013	Apr-10-2013	OBSP high risk form was faxed to general CCO fax line instead of OBSP program site.	External	clients name, DOB, Health insurance # and address	Reception informed PAO and printed a copy and deleted the fax from all folders. A hard copy was walked over to Cancer Screening Contact Centre. CCC Rep called hospital to inform them not to send this form to CCO but to OBSP site	Apr-10-2013	CCC rep to call send of the fax and advise them that CCO is not receive these forms and to send them to OBSP site
PHI in email	Apr-08-2013	Privacy Analyst	Apr-08-2013	Apr-08-2013	PHI included in email to Executive Assistant for VP from filing at 620 reception. Reception rec'd a call from CCC participant about breached correspondence. Email was sent in effort to resolve caller's inquire.	Internal	client's name, enrollment in the CCC screening program and breached occurred during to an incorrect address in our system	Executive Assistant advised the reception filling in to not send PHI via email. Email, in hard copy sent to CCC so that correspondence can be addressed. PAO advised all involved to deleted email from all folders	Apr-08-2013	Sender and recipient to delete email from inbox sent items and deleted items folders.
PHI in email	Mar-27-2013	Privacy Analyst	Mar-27-2013	Mar-27-2013	CSR responded to an email inquire from a client without opening a new email thread. Original email contained PHI - name, phone number current and previous doctors and fact that enrolled in OBSP	External	PHI - name, phone number current and previous doctors and fact that enrolled in OBSP	CSR contacted Cancer Screening Privacy Analyst immediately. Removed PHI content from the email and sent email to OBSP to delete from their folders	Mar-27-2013	CSR to review method for responding to inquiries that contain PHI. Privacy to review current CC processes for dealing with inquiries that contain PHI from the public
PHI in email	Mar-27-2013	Privacy Analyst	Mar-26-2013	Mar-26-2013	PHI including patients first/last name, FOBT date, screening update was included in an email to CCC-primary care email boss from a PCP the CC had contacted regarding +5 reds on their screening Activity report. It was sent in an effort to let CCC know the status update of the	External	PHI including patients first/last name, FOBT date, screening update	CSR called PCP to let her know of the breach and not to include PHI in email in the future	Mar-26-2013	CC to inform PCP we do not require Follow-up info on the status of their patients and not to email PHI to CCO. Privacy to amend CC script for SAR +5 reds calls to unregister PCPs to make explicit that CCO does not require any F/U info. Any F/U info on status

					patients the CC had informed him about					of patients the PCP proceed to give a verbal update over the phone
some PHI in an email	Mar-25-2013	Privacy Analyst	Mar-22-2013	Mar-25-2013	ColonCancerCheck (CCC) client emailed PAO instead of the CCC program to insure about the last date of their FOBT. Email included name, address, health insurance # and the fact that they had taken an FOBT	External	Name, address, health insurance number	Privacy analyst phoned Contact Centre to determine a secure method to transfer email and saved email onto H Drive where Contact Centre can retrieve it. Mail deleted from PAO inbox and deleted items	Mar-25-2013	Privacy analyst to delete email from PAO inbox and deleted items
PHI in a letter	Mar-13-2013	Privacy Analyst	Mar-13-2013	Mar-13-2013	Letter requesting OBSP client's health records with PHI was received by fax to CCO general fax line and fwd by email to OBSP inbox by reception at 620	External	PHI - name, DOB, Hear insurance #	CSR deleted email from OBSP inbox and the deleted items. Reception deleted fax from inbox and other sent items folder	Mar-13-2013	Privacy to draft a response letter to the requestor informing them to contact the primary source for this data
PHI in a fax	Mar-12-2013	Privacy Specialist	Mar-11-2013	Mar-11-2013	PHI in a fax from a physician to CCO general fax line sent to the Director following a telephone conversation with a physician to explain why some patients appear on "Patients Requiring Action" portion of a CCC screening activity report	External	Fax included extensive information about 3 patients including their lab results and examination reports	Sr.Privacy Specialist obtained the fax from CCO's reception and redacted all PHI in the document while the investigating took place. Email containing the fax was permanently deleted. The fax was then picked up by the report from PAO and ultimately destroyed.	Mar-11-2013	Program informed the physician to not send PHI via CCO general fax line and the fax was destroyed. The program to work with their privacy resource in future to ensure that request info with PHI is sent by a method approved by the Secure Transfer of Personal Health Information Policy
PHI included in email	Feb. 21-2013	Privacy Analyst	Feb-21-2013	Feb.21-2013	PHI - medical record # and statement of medical assessment was included in a 2mail sent to CCO from hospital	External	PHI - medical record # and statement of medical assessment	CCO removed PHI content and advised sender that email sent contained PHI and not to send this via email	Feb. 21-2013	Program to deleted email from all folders and informed sender that PHI is not to be sent via email
PHI data in email	Feb.6-2013	Privacy Analyst	Feb-06-2013	Feb.6-2013	PHI data was included in an email to break screening mailbox from CCO fax mailbox at CCO in an effort to further assist Calgary clinic looking for	External	PHI - Name, DOB and past history	Privacy and reception at Breast screening mail box to delete fax and advised not to direct such requests to CCO but to the OBSP site	Feb.6-2013	Inform sender that CCO is not the appropriate organization to send these requests to and directed the sender to where they should be

					previous records for this OBSP client. Name, DOB and the fact this client had mamo done in the past was included in the Fax.					sent
PHI data sent in a fax	Feb.6-2013	Privacy Analyst	Feb-06-2013	Feb. 6-2013	620 Univ. reception received fax and fwd it to OBSP mailbox. The fax was an OBSP high risk requisition which included name, DOB, address. The physician was asking the client to be enrolled in the OBSP High Risk program	External	PHI - name, DOB, and address	CSR called the physician's office and contained the breach and emailed the PAO to let them know of the breach. CSR as well as receptionist deleted fax/email from all mailboxes. Statement added to the form and replaced the form.	Feb. 6-2013	OBSP Program to include a note at the top of the High Risk Requisition form to send the form to the OBSP High Risk site
PHI data in a CCO fax	Feb-06-2013	Privacy Analyst	Feb-06-2013	Feb-06-2013	PHI data rec'd in CCO Fax and fwd to CCC mailbox from receptionist who administers CCO Fax mailbox. Email was send to resolve inquiry CCC sent to a doctor for one of our unattached cases. Fax sent by doctors office confirmed date/time of appointment, name and that client is increased risk for colorectal cancer and needs a referral for colonoscopy.	External	PHI, name, date/time of appointment and risk of Colorectal cancer	CSR and receptionist deleted email from all folders. CSR emailed sender and instructed them to delete it too from all folders. SCR created a 2nd ticket with PHI and closed the other ticket	Feb-06-2013	CC to block CCO general fax number from appearing on outgoing faxes
Lab requisition with PHI	24/1/13	Privacy Analyst	Jan-24-2013	24/1/13	A lab requisition form containing PHI was emailed to the CSP from a lab.	External	PHI	Sr. Project Analyst deleted the received email from inbox and deleted folders and emailed the lab to not send PHI over email and to resend it thru secure fax line	24/1/13	Sender informed that CCO does not accept PHI by email
PHI captured on a video commissioned by CCO	Apr-17-2013	Privacy Manager & Privacy Specialist	Jan-19-2013	Mar-26-2013	PHI was inadvertently captured on a video commissioned by CCO while filming 2 patients at hospital for the purposes of promoting symptom mgt. Patients HIN appeared on an ESAS results sheet and Is visible in the video for 1 second. The videos were included in a Toolkit provided to 14	Internal	A patient's HIN appeared on a video for 1 second	Once informed PAO of the incident, the copies of the video were permanently deleted from the common P drive. CCO asked staff to delete at copies they had retained and emails sent and rec'd containing the video as attachment. With assistance from EISO and Help Desk asked 18 recipients to securely deleted the video. 1st Patient returned the USB, 2nd patient's (deceased) family was contacted asked not to disseminate/distribute and return the USB to hospital. The videographer asked to permanently delete the footage with the	Apr-19-2013	CCO Communications and PAO to develop and implement a process for sign off by PAO; Consent form to be reviewed by PAO and revised where required; as per CCO info Security Code of Conduct, CCO staff and contractors are not to copy, store or transport unencrypted

					nursing leads at RCCs, 3 nursing leads at community hospital and members of Research Community of Practice at university. The videos were saved on an unencrypted USB and sent via unregistered mail to the 2 patients in the video and 18 recipients.			PHI (and provide a certificate of destruction); edit the video to enable re-distribution and requested raw footage be securely returned to CCO		devices; new mobile devices policy is being defined; PAO to review CCO's Secure Transfer of PHI Policy and associated procedures with Clinic programs to ensure roles and responsibilities per the policy are clear' PAO to provide modified Privacy 101 session to Communications team and thus identify specific privacy issues that may be encountered by Communications.
Fax with DOB & PHI	Nov-30-2012	Privacy Analyst	Nov-30-2012	Nov-30-2012	Fax received in OBSP mailbox from Radiologist containing name, DOB and PHI. Sender needed the clients past mamo and ultrasound reports	Extern al	Name, DOB and PHI	CSR deleted the fax from fax box and deleted items folder. Sender notified that they sent the request to the wrong institution	Nov-30-2012	Recipient to delete fax from the inbox and deleted items and notify the sender that they faxed PHI to the wrong institution.
PHI data in email	Nov-21-2012	Privacy Analyst	Nov-21-2012	Nov-13-2012	PHI data was included in an email to Business Unit from a researcher at an unknown institution. The email was sent to Business Unit in error	Extern al	PHI data	Employee deleted email from her inbox and deleted folders. She emailed the sender, informed them that the email contained PHI and sent to her in error. Informed them that sending of PHI by email is against CCO policy.	Nov-13-2012	Informed sender that he/she has sent PHI in error
PHI data-patients name and DOB	Nov-19-2012	Privacy Analyst	Nov-19-2012	Nov-19-2012	PHI was received by CCC secure fax line from hospital. The fax asked us to send last mammogram reports for a patient. The fax included the patient's name and DOB	Extern al	PHI data- name and DOB	CSR deleted information from the fax folder. Called the sender and instructed them to send these requests only to regional screening site	Nov-19-2012	Recipient to inform sender they have sent PHI via email.
PCP requestin g Patient HIN	Nov-09-2012	Privacy Analyst	Nov-09-2012	Nov-09-2012	ColonCancerCheck fax coversheet faxed back to CCO from PCP requesting patient HIN. The fax contained patient's name, and ColonCancerCheck letterhead and was sent to the general fax # used by the Contact	Internal	Patient's HIN	Privacy instructed switchboard operator to delete the email from the fax inbox and deleted items folder	Nov-09-2012	ICS Fax Cover Sheet to be updated to replace the general CCO fax number with the ICS Contact Centre fax number

					Centre					
email contacting name of ColonCanterCheck client	Nov-08-2012	Privacy Analyst	Nov-08-2012	Nov-08-2012	Breach notification template with a file name containing the name of the ColonCancerCheck client was sent via email from ICS Contact Centre rep to the ICS Privacy Analyst for review	Internal	Name re: Colon CancerCheck	CSR and ICS Privacy Analyst deleted the email from their sent items/inbox and deleted items folder	Nov-08-2012	ICS Program to present to Privacy the steps taken to help mitigate the risk of Contact Centre staff emailing PHI. One such option is to include a posted in the contact Centre displaying the number of error/breach-free weeks
Email inquiry from ServiceOntario through email	Nov-16-2012	Privacy Analyst	Oct-17-2012	Oct-17-2012	An inquiry was escalated to ICS Contact Centre from Service Ontario info line through email which contained patient's name and contact info and her inquiry stated she was part of OBSP high risk. Contact centre fwd the email to another member of the Contact Centre and was again forwarded to another member and then reported to Privacy	External and Internal	Patient's name, contact info and indication that she was part of OBSP high risk	ICS Privacy Analyst instructed for all Contact Centre staff to sent or received the email to delete the email from their sent items/inbox and deleted items folder	Oct-17-2012	ICS Program to present to Privacy the steps taken to help mitigate the risk of Contact Centre staff emailing PHI. One such option is to include a poster in the contact centre displaying the number of error/breach-free weeks
Fax with PHI data sent to CCC fax line	Oct-15-2012	Privacy Analyst	Oct-12-2012	Oct-12-2012	PHI data sent to CCC fax line from hospital in a referral form with no contact information of sender or intended receiver	External	Patient's name, HIN, patient's address.	Privacy lead responded to the notification from the Contact Centre to make sure that the fax had been deleted	Oct-15-2012	Since there is no way to contact the sender to inform them of the breach and to advise them not to send these faxes to CCO in the future, there is no resolution that can be implemented
Fax with PHI data sent to CCC fax line	Oct-15-2012	Privacy Analyst	Oct-12-2012	Oct-12-2012	Someone at hospital sent what appears to be a referral form for the patient to an oncologist to the CCC fax line by mistake. It contained patients name, HIN and address. No information on the sender or the	External	patients name, HIN and address	Privacy lead responded to the notification to make sure that the fax had been deleted	Oct-15-2012	Since there is no way to contact the sender to inform them of the breach and to advise them not to send these faxes to CCO in the future, there is no resolution that can be implemented

					intended receiver					
email with PHI account hacked	Sep-24-2012	Privacy Analyst	Sep-12-2012	Sep-12-2012	potentially identifiable data was included in an excel spreadsheet in an email attachment.	internal	Potentially identifiable record level data	Privacy informed the researcher of the potential that PHI resided in the account and asked that she delete the email from their archived emails and deleted items.	Sep-25-2012	Since the data elements, according to CCO's De-identification Guidelines are classified as having a moderate risk of re-identification, the likelihood that an individual could be re-identified is low therefore this is considered a privacy risk.
Email containing PHI	Sep-11-2012	Privacy Specialist	Sep-07-2012	Sep-11-2012	Unknown	Internal	Unknown	The sender and all 5 recipients confirmed that the email containing PHI was deleted from all Inbox, Sent, and Deleted Items folders.	Jul-09-2012	1) The CCO employee who sent the email containing PHI must re-take the 2011 Privacy Refresher Training and provide written confirmation of completion to the PAO. 2) As this is the third breach resulting from PHI being sent by email by the ICS Contact Centre since Aug. 22, 2012, the PAO will conduct in-person privacy refresher training with Contact Centre staff in order to raise awareness of the issue and prevent further privacy breaches
Email w/ additional PHI	Aug-30-2012	Privacy Specialist	Aug-22-2012	Aug-22-2012	An ICS Contact Centre employee sent an email containing 2 attachments which contained PHI to the PAO. The email was copied to 5 other CCO employees.	Internal	2 attachments which contained PHI	The sender and all 3 recipients confirmed that the email containing PHI was deleted from all Inbox, Sent, and Deleted Items folders	Aug-23-2012	1) The CCO employee who sent the email w/ PHI must re-take the 2011 Privacy Refresher Training and provide written confirmation of completion to the PAO.
email with PHI	Aug-30-2012	Privacy Specialist	Aug-22-2012	Aug-22-2012	While providing confirmation to the P&A Office that an email	Internal	Unknown PHI	The sender and all recipients confirmed that the email containing PHI was deleted from all Inbox, Sent and deleted items folder.	Aug-23-2012	The CCO employee who sent the email containing PHI must

					containing PHI was sent by the ICS contact Centre, a Contact Centre employee sent additional PHI in an email to 3 CCO employees					retake the 2011 Privacy Refresher Training and provide written confirmation of completion to the privacy and Access Office.
Email from CCC participant	Aug-30-2012	Privacy Specialist	Aug-21-2012	Aug-22-2012	While providing confirmation to the P&A Office that an email containing PHI was sent by the ICS contact Centre, a Contact Centre employee sent additional PHI in an email to 3 CCO employees	Internal	Unknown PHI	The emails containing PHI were saved in InScreen and were deleted from the Inbox, Sent, and Deleted Items folders.	Aug-28-2012	1) Updates to Contact Centre SOPs with respect to ad hoc correspondence required a) Email responses must not include PHI b) P&A Office to be an approver of ad-hoc correspondence, in addition to a subject matter expert (to permit the office to review the final draft and confirm 1) whether it contains PHI) 2) The CCO employee who sent the email containing PHI must re-take the 2011 Privacy Refresher Training and provide written confirmation of completion to the PAO
email inquiry and response contained PHI	Aug-30-2012	Privacy Specialist	Aug-21-2012	Aug-28-2012	An email inquiry from a participant in the CCC program which contained PHI was received by the ICS Contact Centre. Contact Centre staff sent in response to this inquiry by email, and this response also included PHI	Internal	Name of screening program participant, name of screening program.	The emails containing PHI were saved in InScreen and were deleted from the Inbox, Sent, and Deleted Items folders.	Aug-28-2012	The following updates to ICS Contact Centre Standard Operating Procedures with respect to AD Hoc Correspondence to be confirmed: 1) email responses must not include PHI 2) PAO to be an approver of ad-hoc correspondence in addition to a subject matter to expert (or permit the PAO to review the final draft and confirm whether it contains PHI) . The CCO employee who sent the email must re-take the 2011 Privacy

										Refresher Training and provide written confirmation of completion to the PAO.
SAR Presentation	Aug-12-2012	Privacy Specialist	Aug-12-2012	Dec-19-2011	PHI was projected onto a screen during a closed meeting where a SAR report design layout was being reviewed by 8 CCO employees. There were individuals who did not have ODDAR approval. The same PHI was presented at and earlier demo with 2 regional leads who were not CCO employees.	External and Internal	Demographic information for 2 patients	Report design layouts were re-populated with fabricated data and all PHI was removed	May-01-2012	PAO to advise the project team leads that in the future, demonstrations must not contain any PHI and that fabricated data must be used instead. Project Manager to inform the entire project team of the breach and of the resolution in order to prevent future breaches.
Health Card info	0-Jun-2012	Business Unit	Jun-07-2012	Jun-07-2012	Health Card numbers received via email from Data Analyst at hospital.	External	HIN	Email deleted from inbox and deleted items folder. Notified sender of the breach	Jun-07-2012	Manager, Quality Assurance Services, to send out email reminding staff not to email PHI. Sender of email to undergo remedial training and complete all Privacy and Security Modules. Sender also to sign a document attesting to the completion of the module
OBSP result letter opened by CCO employee	Apr-20-2012	Privacy Specialist	Apr-20-2012	Apr-20-2012	An OBSP result letter containing PHI was marked "Return to Sender" (**RTS**) and was sent by mail to CCO. The letter was generated by an OBSP regional site and not CCO. The letter was received and opened by a CCO employee (who did not anticipate it would contain PHI) to	Internal	Client name, client address, mammogram result	The Senior Project Manager, ICS Regional Operations, provided the letter containing the PHI to ICS Contact Centre in order that they may conduct an investigation into the misdirected correspondence. The PAO was notified.	Apr-23-2012	CCO should consider implementing a requirement for OBSP sites mandating that the correct return address be clearly indicated on the envelope.

					determine where to direct it.					
CCC letter with PHI emailed	Apr-12-2012	Privacy Specialist	Apr-11-2012	Apr-11-2012	An email inquiry from a participant in the CCC program which contained PHI was received by the ICS Contact Centre. Contact centre staff sent in response to this inquiry by email, and this response also included PHI	Internal	Unknown PHI	The sender and all 7 recipients were advised to immediately delete the emails containing PHI from all Sent, Inbox and Deleted Items folders.	Apr-12-2012	1) Sender of email to undergo remedial training and complete all Privacy & Security Modules. Sender to also sign a document attesting to the completion of the modules.
Emailed screenshots containing PHI	Mar-28-2012	Privacy Specialist	Mar-12-2012	Mar-14-2012	An email containing screenshots which included records of PHI was sent from a CCO employee to 3 other CCO employees in the PCCIP on March 12, 2012. As there was no response to the original email, the same email was re-sent to the same recipients on Mar. 14, 2012.	Internal	Unknown PHI	The sender and all three recipients were advised to immediately delete the emails containing PHI from all folders	Mar-20-2012	1) PCCIP to consider feasibility of rule that screenshots must not be sent by email in order to prevent future email breaches from occurring. 2) Sender of email to undergo remedial training and complete all Privacy and Security Modules. Sender to also sign a document attesting to the completion of the modules.
Fax with DOB, HIN of a client	Mar-12-2012	Privacy Analyst	Mar-12-2012	Dec-03-2012	Fax received in OBSP mailbox from health centre. It contained, name, DOB, and HIN. The sender needed client's past mamo and ultra sound reports so provided the PHI. This is a second time this clinic has sent a similar request	External	Name, DOB and PHI	CSR called the sender and informed them we cannot help as we do not have the information. CSR explained that in future they should contact the site where patient went for screening. CSR deleted the fax from fax inbox and deleted items folders	Dec-03-2012	CSR to delete the fax from both the fax inbox and deleted items and notify the sender that they have sent the request to the wrong institution
email with PHI	Mar-12-2012	Privacy Specialist	Mar-09-2012	Mar-09-2012	An email containing PHI of approximately 9 individuals was sent from a CCO employee t two other CCO employed in Quality Assurance Services	Internal	Unknown PHI	The sender and both recipients were advised to delete the email containing PHI from all Sent, Inbox and Deleted Items folders	Mar-09-2012	Manager, Quality Assurance Services, to send out email reminding staff not to email PHI. Sender of email to undergo remedial training and complete all Privacy

										and Security Modules. Sender also to sign a document attesting to the completion of the modules.
Email from OHP	Feb-22-2012	Privacy Specialist	Feb-21-2012	Feb-21-2012	Email with PHI was received by a CCO employee from an external OHP requesting assistance with the uploading of a file. The email contained an attachment with PHI. The email recipient forward the email to other CCO employees	External and Internal	Unknown PHI	The sender and all email recipients deleted the email form all email folders as soon as the breach was identified. The original CCO recipient notified both her manager and the P7A office of the breach. An email was sent to all OHPs from the Project Manager reminding them not to send PHI to CCO by email.	Feb-21-2012	1) A reminder email was sent to all OHP's by the project manager that PHI should never be sent to CCO via email.
Email from MOHLTC	Feb-09-2012	Privacy Specialist	Jan-13-2012	Jan-13-2012	Email with an attachment with PHI was sent to a CCO employee from stakeholderand forward to another CCO employee. Was then identified that the email contained PHI.	External and Internal	Unknown PHI	The sender and CCO recipients were asked immediately to delete the email from sent, inbox and deleted boxes. The attachment containing PHI was saved to the H-drive. The above all took place within a 20 minute period	Jan-13-2012	1) Senior Program Manager, Prevention and Screening to send out email reminding staff not to email PHI
screenshot with PHI during a closed meeting	Dec-01-2011	Privacy Specialist	Dec-19-2011	Dec-19-2011	PHI was projected onto a screen during a closed meeting where a SAR report design layout was being reviewed by 8 CCO employees. There were individuals who did not have ODDAR approval. The same PHI was presented at and earlier demo with 2 regional leads who are not CCO employees. The demonstration contained demographic information only for two patients. All other data had been asked at the application level.	Internal	Demographic information for two patients.	As soon as the record level information was presented during the closed meeting, it was noted that this was potentially PHI, and the reports containing PHI were closed immediately. The report design layouts have now been populated with fabricated data to be used for future demonstrations.		Privacy to advise the project team leads, that in future, demonstrations must not contain any PHI and that fabricated data must be used instead. Senior Project Manager, to inform entire project team of the breach and of the resolution above in order to prevent future breaches.

SAR reports sent by CCO Developer	Dec-19-2011	Privacy Specialist	Dec-13-2011	Dec-19-2011	Screenshots of SAR reports containing PHI sent in and email by a CCO developer to 3 CCO employees	Internal	Screenshots of SAR reports containing PHI sent in and email by a CCO developer to 3 CCO employees	The sender and all recipients were asked immediately to delete the email from sent, inbox and deleted boxes	Jan-27-2012	All CCO employees to be reminded that PHI must not be sent by email via the annual Privacy Refresher training launched December 2, 2011 -Senior Program Manager, Prevention and Screening to send out email reminding staff not to email PHI

Summary of PP Breaches (Contact Centre)

for the period between November 1st, 2011 to October 31st, 2013

Investigating Agent	Date of Incident	Date Sr. Mgmt Notified	Internal vs External	Nature of PHI	Containment Measure	Date Investigation Completed	Notification Provided to individual
Privacy Analyst	Jun-24-2013	Jun-24-2013	External	Birthday letter opened by unintended recipient	Client called as his son's ex-wife rec'd a letter for him at an address he had never lived at. Was confused and annoyed. CSR explained that it is because of NCOA and apologized. CSR told his that the issue was corrected and would send him another copy of the letter for his record. Letter sent and a breach notification letter sent	Unknown	New letter and breach notification letter sent to the correct address
Privacy Analyst	Jun-24-2013	Jun-24-2013	External	Results letter opened by unintended recipient	Opened negative result letter from returned to FH. CSR was able to contact the client and obtain correct address. Breach notification letter was sent to client	Jul-03-2013	Breach notification letter sent to client
Privacy Analyst	Jun-24-2013	Jun-24-2013	External	Birthday letter opened by unintended recipient who returned the letter	FH returned an opened birthday letter CSR was unable contact the client to obtain correct address	Jul-30-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-24-2013	Jun-24-2013	External	Reminder letter opened by unintended recipient	Contact Centre rec'd a call from an unintended recipient who rec'd a reminded letter for a client who no longer lived at the address and agreed to return the letter but was never received.	Jul-25-2013	CSR was unable to contact client to confirm correct address

Privacy Analyst	Jun-19-2013	Jun-19-2013	External	Birthday letter opened by unintended recipient	FH returned a birthday letter with sticker marked "moved/unknown/RTS". CSR was unable to confirm correct address	Jun-19-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-19-2013	Jun-19-2013	External	Birthday letter opened by unintended recipient	FH returned birthday letter with sticker "moved/Unknown RTS". CSR was unable to contact the client to obtain correct address	Jul-08-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-14-2013	Jun-14-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter. CSR was unable to contact client to confirm correct address	Jun-14-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-14-2013	Jun-14-2013	External	Results letter opened by unintended recipient	FH returned an opened results letter. CSR was able to contact the client and confirm address. A breach notification letter was sent and a copy of the results letter	Jun-21-2013	A breach notification letter was sent and a copy of the results letter
Privacy Analyst	Jun-14-2013	Jun-14-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter. CSR was unable to contact client to confirm correct address	Jun-28-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-14-2013	Jun-14-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter. CSR was unable to contact client to confirm correct address		CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-14-2013	Jun-14-2013	External	Reminder letter opened by unintended recipient	FH returned opened reminder letter. CSR was unable to contact client to confirm correct address	Jun-18-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-14-2013	June 14. 2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter. CSR was unable to contact client to confirm correct address		CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-11-2013	Jun-11-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter. CSR was unable to contact the client to confirm the correct address	Jun-11-2012	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-11-2013	Jun-11-2013	External	Birthday letter opened by unintended recipient	FH returned open birthday letter. CSR was able to contact the client and obtain the correct address	Jun-28-2013	Breach notification letter sent to client
Privacy Analyst	Jun-11-2013	Jun-11-2013	External	Birthday letter opened by unintended recipient	FH returned an opened birthday letter due to incorrect RPDB address. CSR was unable to contact client	Jun-28-2013	CSR was unable to contact client to confirm correct address

Privacy Analyst	Jun-10-2013	Jun-10-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to report that she had received her sister's birthday letter who had never lived at this address and wanted to know why we have her sister's address. InScreen showed we have the correct address and no letter was mailed to her but a record of a different client with same name, and different HIN with the address of unintended recipient. Both records have same name, DOB and different HINs. Thus this letter got breached twice - once by the unintended recipient and the second time when the recipient gave the letter to her sister who has the same name as the actual client. Recipient agreed to return the letter. CSR was unable to contact client to confirm address	Jun-10-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-04-2013	Jun-04-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to inform he had rec'd and opened birthday letter for this client. He said that this client does not live at this address. He was asked to return the letter which he did. CSR was unable to contact the client to confirm the correct address	Jun-10-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-04-2013	Jun-04-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to say she had rec'd a birthday letter for ex-husband's new wife. She was concerned that the client was giving out her address. It was explained to her that it was a glitch in the use of “National Change of Address” (**NCOA**) database and applies for a family move. She agreed to return the letter. CSR was unable to contact the client and confirm the correct address	Jun-12-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-04-2013	Jun-04-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to say she had rec’d a birthday letter for her ex-husband's new wife, and worried that client was giving out her address for some reason. CSR explained it is a glitch sometimes caused when using NCOA and applies "family move". Said she would return the letter back. CSR was unable to contact client to get correct address	Jun-12-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jun-03-2013	Jun-03-2013	External	Results letter opened by unintended recipient	CC recd an opened normal results letter for a client via FH mail. CSR was unable to contact client to obtain correct address	Jun-13-2013	CSR was unable to contact client to obtain correct address
Privacy Analyst	May-28-2013	May-28-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called in regards to CRC birthday letter rec'd at the wrong address. CSR was unable to contact client to confirm correct address	May-13-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-28-2013	May-28-2013	External	Birthday letter opened by unintended recipient	FH returned a birthday letter with sticker marked "moved/unknown/RTS". CSR was unable to confirm correct address	May-28-2013	CSR was unable to contact client to confirm correct address

Privacy Analyst	May-28-2013	May-28-2013	External	Birthday letter opened by unintended recipient	FH retuned an opened birthday letter with the top third of the letter removed. With no activity or name it was not possible to identify the intended recipient. No containment necessary but it is still a privacy breach	May-28-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-27-2013	May-27-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter	May-28-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-27-2013	May-27-2013	External	Results letter opened by unintended recipient	FH returned results letter with sticker "RTS". CSR was unable to confirm correct address	Jun-07-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-27-2013	May-27-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to say he had rec'd a birthday letter for his ex-wife's husband who never lived at his address and was informed it was a glitch with NCOA and agreed to return the envelope. CSR was unable to contact client to obtain correct address	May-28-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-27-2013	May-27-2013	External	Birthday letter opened by unintended recipient	FH returned a birthday letter. CSR was unable to confirm correct address	Jun-06-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-27-2013	May-27-2013	External	Birthday letter opened by unintended recipient	FH returned a birthday letter indicating client move in Nov. 2012 CSR was unable to confirm correct address	Jun-13-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-27-2013	May-27-2013	External	Results letter opened by unintended recipient	Unintended recipient called to report she opened a letter for someone who does not live at her address. CSR was able to contact the client and confirm correct address	Jun-17-2013	CSR was able to contact client to confirm correct address
Privacy Analyst	May-23-2013	May-23-2013	External	Birthday letter opened by unintended recipient	FH returned mail an opened birthday. CSR was unable to contact the client and confirm the correct address.	May-31-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-22-2013	May-22-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to say she rec'd a birthday letter for someone with same name. InScreen showed no letter was sent. CSR was unable to contact the client to return the correct address.	Jun-13-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-17-2013	May-13-2013	External	Birthday letter opened by unintended recipient	FH returned mail an opened birthday. CSR was able to contact the client and confirm the correct address.	Jun-13-2013	CSR was able to contact client to confirm correct address
Privacy Analyst	May-17-2013	May-17-2013	External	Birthday letter opened by unintended recipient	CC recd an FH returned letter that was breached for a client, opened with a yellow sticker "moved/RTS". CSR was unable to contact the client to confirm correct address	Jun-03-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-13-2013	May-13-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter. CSR was unable to contact the client to confirm the correct address	May-13-2013	CSR was unable to contact client to confirm correct address

Privacy Analyst	May-13-2013	May-13-2013	External	Birthday letter opened by unintended recipient	FH return opened birthday letter. CSR was unable to contact the client to confirm the correct address	May-13-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-13-2013	May-13-2013	External	Birthday letter opened by unintended recipient	Call Center rec'd an opened birthday letter via FH returned mail. CSR was able to contact the client and confirm correct address	May-13-2013	CSR was able to contact client to confirm correct address.
Privacy Analyst	May-13-2013	May-13-2013	External	Birthday letter opened by unintended recipient	Unintended recipient reported that she had rec'd a birthday letter and agreed to return the letter. CSR unable to contact client to verify correct address	May-13-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-13-2013	May-13-2013	External	Reminder letter opened by unintended recipient	FH returned opened reminder letter. CSR was able to contact client and confirm correct address	May-22-2013	CSR was able to contact client to confirm correct address
Privacy Analyst	May-13-2013	May-13-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter. CSR was unable to contact client and confirm correct address	May-24-2013	CSR was unable to contact client and confirm correct address
Privacy Analyst	May-10-2013	May-10-2013	External	Results letter opened by intended recipient	Client called re: Change of address and that the last results letter was sent to the old address and why was it not marked private or confidential. Assured her that correct address was on file and she should let her PCP to ensure this does not happen again	May-13-2013	Assured her CCO has her correct address and she should advise her PCP of the new address.
Privacy Analyst	May-08-2013	May-08-2013	External	Birthday letter opened by unintended recipient	FH returned opened Birthday letter to CC	May-08-2013	No valid phone # listed InScreen, 411 and the client does not have a PCP
Privacy Analyst	May-07-2013	May-07-2013	External	Birthday letter opened by unintended recipient	Contact Centre received opened Birthday letter from fulfillment house with hand written note "R.T" CSR was unable to contact client to confirm the correct address	May-13-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-07-2013	May-07-2013	External	Birthday letter opened by unintended recipient	FH returned mail opened birthday letter. CSR was able to contact the client and confirm the correct address	May-09-2013	CSR was able to contact client to confirm correct address. Breach notification letter sent to client
Privacy Analyst	May-07-2013	May-07-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to let us know that he had rec'd correspondence for a client. He was irate and refused to send letter back. CSR was unable to instruct him to destroy the letter. CSR was unable to contact the client to confirm the correct address	May-07-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-07-2013	May-07-2013	External	Birthday letter opened by unintended recipient	CC rec'd a returned birthday letter, opened and taped from FH red stamped "Ontario Works reception, April 15, 2013" and hand written "not here". CSR was unable to contact the client and confirm correct address	May-07-2013	CSR was unable to contact client to confirm correct address

Privacy Analyst	May-07-2013	May-07-2013	External	Birthday letter opened by unintended recipient	FF house returned a birthday letter stamped "RTS". CSR was able to contact the client but client would not give our info to authenticate thus CSR was unable to confirm correct address	May-08-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-06-2013	May-06-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to say he had rec'd a birthday letter for someone who does not live at this address. Refused to return it but would shred the opened letter. CSR was unable to contact client to confirm correct address	May-06-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	May-03-2013	May-03-2013	External	Birthday letter opened by unintended recipient	Rec'd voicemail from unintended recipient stating he had received a birthday letter for a client who did not live at her address. No call back number. CSR was able to contact client to confirm correct address		CSR was able to contact client to confirm correct address
Privacy Analyst	May-02-2013	May-02-2013	External	Birthday letter opened by unintended recipient	FH returned a birthday letter with a sticker "moved". CSR was able to contact the client and confirm correct address		CSR was unable to contact client to confirm correct address
Privacy Analyst	May-02-2013	May-02-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called re: birthday letter received for a client (her ex-husband who never lived at this address) said she would return the letter but never received. CSR was unable to contact the client to confirm correct address		CSR was unable to contact the client to confirm correct address
Privacy Analyst	May-01-2013	May-01-2013	External	Reminder letter opened by unintended recipient	unintended recipient reported she opened a letter that had been a delivery error by Canada Post. CSR was able to contact client and notify client of breach and that the recipient had hand delivered the letter to her.		CSR sent a breach notification to the client.
Privacy Analyst	May-01-2013	May-01-2013	External	Results letter opened by unintended recipient	Client's daughter called to say her father had moved to China and to remove her address. This is a NCOA. CSR was unable to update the address and deactivated the daughter's address. Since the daughter is not an SDM, this is a breach		CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-30-2013	Apr-30-2013	External	Birthday letter opened by unintended recipient	Letter was returned with moved/RTS. CSR was unable to contact client to confirm correct address		CSR was unable to contact client to confirm address
Privacy Analyst	Apr-30-2013	Apr-30-2013	External	Birthday letter opened by unintended recipient	FH returned letter with RTS. CSR was unable to contact client to confirm correct address		CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-30-2013	Apr-30-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to say the client used to live at the address but no longer does. She agreed to mail back the opened letter, however upon follow-up CSR informed that the recipient had taken it to the client		CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-30-2013	Apr-30-2013	External	Birthday letter opened by unintended recipient	Caller called in regards a CRC Birthday letter that was rec'd to the wrong address and agreed to return the letter back to CCO. CSR was unable to contact the client to confirm the correct address	May-13-2013	CSR was unable to contact client to confirm correct address

Privacy Analyst	Apr-30-2013	Apr-30-2013	External	Birthday letter opened by unintended recipient	FH returned a breached birthday letter to call centre. The letter was opened and marked "moved". CSR unable to contact client and confirm correct address	May-13-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-30-2013	Apr-30-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called re: birthday letter received for a client and opened. CSR sent a pre-paid envelope to return the letter in. CSR was unable to contact the client to confirm correct address	Apr-30-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-30-2013	Apr-30-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to say she rec'd a birthday letter for ex-husband and did not want anything going to her address. Mailing address provided and she would return the letter to CCO. Breach result of NCOA	Apr-30-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-28-2013	Apr-28-2013	External	Birthday letter opened by unintended recipient	Unintended recipient rec'd birthday letter for a client who no longer lives at the address and agreed to return the letter but never rec'd. CSR unable to contact client to confirm correct address	May-10-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-26-2013	Apr-26-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter cause by NCOA. Client added to manual mailing list. CSR unable to contact client to confirm correct address	Apr-26-2013	Client added to manual mailing list. CSR was unable to contact client to confirm address
Privacy Analyst	Apr-26-2013	Apr-26-2013	External	Birthday letter opened by unintended recipient	CSR was unable to contact client and confirm the correct address	Apr-26-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-26-2013	Apr-26-2013	External	Birthday letter opened by unintended recipient	CSR was able to contact the client and obtain correct address. A breach notification and copy of the birthday letter were sent to client's new address	Apr-26-2013	CSR was able to contact client to confirm correct address. Breach notification letter sent to client
Privacy Analyst	Apr-26-2013	Apr-26-2013	External	Birthday letter opened by unintended recipient	FH returned opened letter. CSR was unable to contact the client to confirm correct address		CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-24-2013	Apr-24-2013	External	Birthday letter opened by unintended recipient	Unintended recipient rec'd birthday letter, opened it as it was for her daughter who had moved to the US…daughter instructed her to shred the letter. When asked to return the letter, she refused saying her daughter asked that it be shredded. CSR unable to obtain correct address	Apr-24-2013	CSR unable to contact client who is in the US to get the correct address
Privacy Analyst	Apr-24-2013	Apr-24-2013	External	Birthday letter opened by unintended recipient	FH returned a birthday letter with a sticker "moved/RTS". CSR was able to contact the client and confirm correct address	Apr-24-2013	CSR was able to contact client to confirm correct address. Breach notification letter sent to client

Privacy Analyst	Apr-24-2013	Apr-25-2013	External	Birthday letter opened by unintended recipient	FH returned a letter marked "Return to Sender". CSR was able to contact client and confirm correct address. A breach notification letter and original letter sent to client	Apr-25-2013	Breach notification letter sent to client
Privacy Analyst	Apr-23-2013	Apr-23-2013	External	Birthday letter opened by unintended recipient	Rec'd an opened birthday letter from FH. CSR tried the # provided by PCP but unable to contact client	Apr-30-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-23-2013	Apr-23-2013	External	Birthday letter opened by unintended recipient	FH returned to CC a birthday letter that was opened and taped and put in a Cda Post clear bag with yellow sticker - moved/return to sender. CSR was unable to contact client to confirm correct address	May-16-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-23-2013	Apr-23-2013	External	Birthday letter opened by unintended recipient	Fulfillment house returned birthday letter with yellow sticker "moved/unknown RTS". CSR was unable to contact client to confirm correct address	May-03-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-23-2013	Apr-23-2013	External	Results letter opened by unintended recipient	Unintended recipient called to say he had received a results letter, opened it and agreed to send it back to CCO, but never received. CSR was able to contact the client and confirm correct address		CSR was able to contact client to confirm correct address
Privacy Analyst	Apr-22-2013	Apr-22-2013	External	Birthday letter opened by unintended recipient	Unintended recipient rec'd birthday letter for a client who no longer lives at the address and agreed to return the letter but never rec'd. CSR followed with the person who claimed did not remember receiving the letter. CSR unable to contact client to confirm correct address	May-15-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-19-2013	Apr-19-2013	External	Birthday letter opened by unintended recipient	Unintended recipient rec'd birthday letter and opened it. CSR was unable to confirm the correct address	Apr-19-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-17-2013	Apr-17-2013	External	Birthday letter opened by unintended recipient	Call center rec'd a FH return birthday letter that was opened with "return to sender"	N/A	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-17-2013	Apr-17-2013	External	Birthday letter opened by unintended recipient	Call Centre received FH birthday letter returned that was opened with a sticker "moved/RTS"	Apr-17-2013	Client moved, did not provide updated address
Privacy Analyst	Apr-17-2013	Apr-17-2013	External	Birthday letter opened by unintended recipient	FH returned an opened birthday letter. CSR unable to contact client to confirm correct address	Apr-17-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-15-2013	Apr-15-2013	External	Birthday letter opened by unintended recipient	Unintended received a letter for a client who does not live there and refused to return the letter so asked that it be shredded. CSR was able to obtain correct address and breach letter sent. Client informed that he goes by his middle man and roommate thought it was an error. Recommendation was to send a manual breach letter notification and a copy of the birthday letter with the middle name. Client added to manual mailing list	Apr-16-2013	Breach notification letter and the birthday letter sent to client

Privacy Analyst	Apr-12-2013	Apr-12-2013	External	Birthday letter opened by unintended recipient	Opened Birthday letter was returned via FH. CSR was unable to contact the client to confirm correct address	Apr-12-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-12-2013	Apr-12-2013	External	Birthday letter opened by unintended recipient	Reporter call to say she had received a birthday letter which she had opened and agreed to return it.	Apr-25-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-12-2013	Apr-12-2013	External	Birthday letter opened by unintended recipient	Unintended recipient called to report she had rec'd mail for a client who had never lived at this address. It is a NCOA birthday letter breach. She agreed to return if she was sent a portage paid envelope, CSR mailed it to her but the letter was never returned and f/u efforts was not successful. CSR unable to contact client to confirm correct address	Apr-30-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-09-2013	Apr-09-2013	External	results letter opened by unintended recipient	Reporter called to report a breach. She confirmed she rec'd a result letter for this client and claimed this person never lived at this address. Agreed to mail the result letter back. CSR called & on 4 and 5 attempts, female claimed to be the client but does not understand and when asked if she needed a translator, she hung up. CSR was unable to get the correct address	Apr-16-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-08-2013	Apr-08-2013	External	results letter opened by unintended recipient	Contact Centre rec'd opened result letter returned via FH. Letter was opened and envelope was taped with yellow sticker "moved and return to sender". CSR was able to contact the client and confirm correct address. Breach notification and copy of original letter was sent to client	Apr-10-2013	Breach notification letter sent to client.
Privacy Analyst	Apr-08-2013	Apr-08-2013	External	Birthday letter opened by unintended recipient	Colorectal Cancer (**CRC**) birthday letter came back from FH returned mail. CSR able to confirm correct address	Apr-15-2013	CSR was able to contact client to confirm correct address. Breach notification letter sent to client
Privacy Analyst	Apr-08-2013	May-13-2013	External	Birthday letter opened by unintended recipient	Unintended recipient rec'd a birthday letter for a client and called reception line. Receptionist took down the info and emailed it to the CC (separate breach report filled out for this incident). CC phone the unintended recipient back and he agreed to return the breached letter. CSR was unable to contact the client to confirm correct address		CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-04-2013	Apr-04-2013	External	Call Centre rec'd a FH result letter that was opened with no note or return sticker	Call Center rec'd an opened FH result letter with no note or sticker. CSR was able to contact the client	Apr-08-2013	Breach notification letter sent to client

Privacy Analyst	Apr-04-2013	Apr-04-2013	External	Reminder letter opened by unintended recipient	FH returned opened letter. CSR was unable to contact the client to confirm correct address	Apr-17-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Apr-04-2013	Apr-04-2013	External	Reminder letter opened by unintended recipient	Unintended recipient received and opened, agreed to mail it back but never received. CSR was able to contact the client and confirm correct address and breach notification letter sent	Apr-22-2013	Breach notification letter sent to client
Privacy Analyst	Apr-03-2013	Apr-03-2013	external	Reminder letter opened by unintended recipient	Unintended recipient call Contact Centre to report had rec'd a letter for someone else, had opened it and will return the letter. CSR obtain the correct address and a breach notification and copy of original letter was mailed	Apr-17-2013	Breach letter and result letter sent to client
Privacy Analyst	Mar-27-2013	Mar-27-2013	External	Birthday letter opened by unintended recipient	Reporter of the breach called to say she received for somebody not at the address. She opened the letter and wants us to stop sending them to her address. Refused to return the letter and got angry when asked to shred it and hung up. CSR was unable to obtain a name or info and could not call back. CSR unable to contact client to confirm address	Apr-10-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Mar-27-2013	Mar-27-2013	External	Reminder letter opened by unintended recipient	Unintended recipient with same name, received and opened a reminder letter. CSR was able to confirm the correct address and breach notification letter and copy of the reminder letter was sent	Apr-03-2013	Breach notification letter sent to client
Privacy Analyst	Mar-25-2013	Mar-25-2013	External	Birthday letter opened by unintended recipient	Public Affairs saved email from an unintended recipient on H drive and notified CC. The unintended recipient had received and opened a birthday letter for client who does not live at that address and agreed to return the letter to CCO but was never received. CSR was unable to confirm the correct address	Apr-11-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Mar-21-2013	Mar-21-2013	External	Reminder letter opened by unintended recipient	Unintended recipient called to say that she rec'd a letter for her ex-boyfriend. Said the client has moved and staying with his mother and had called him. Said would return the letter to CCC and mailing address was provided. CSR unable to contact the client	Apr-03-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Mar-19-2013	Mar-19-2013	External	Results letter opened by unintended recipient	Unintended received and opened a results letter, agreed to send it back to CCO, however never received. CSR was able to contact client and breach letter was sent to correct address	Mar-19-2013	Breach notification letter sent to client
Privacy Analyst	Mar-18-2013	Mar-18-2013	External	Reminder letter opened by unintended recipient	Unintended recipient called to say she opened a reminder letter for a person who used to live at that address and did not have the correct address. She agreed to mail the letter back to CCO. CSR was unable to confirm correct address	Mar-20-2013	CSR was unable to contact client to confirm correct address

Privacy Analyst	Mar-14-2013	Mar-14-2013	External	Birthday letter opened by unintended recipient	CC received an opened birthday letter from FH. CSR was unable to contact the client to confirm the correct address	Apr-04-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Mar-11-2013	Mar-11-2013	External	Birthday letter opened by unintended recipient	The client, who was the ex-husband no longer lived at the address. Unintended recipient agreed to return the letter to CCO, however upon f/u said she gave it to her ex-husband. CSR was unable to contact client to confirm correct address	May-01-2013	CSR was unable to contact the client and confirm correct address
Privacy Analyst	Mar-08-2013	Mar-08-2013	External	Results letter opened by unintended recipient	CSR received a call from an individual who reported he had received a result letter from someone who does not live at his address. The reporter agreed to mail the results letter back to us	Mar-29-2013	CSR was unable to contact the client and confirm correct address
Privacy Analyst	Mar-07-2013	Mar-07-2013	External	results letter opened by unintended recipient	Unintended recipient called to say he received a results at his address. He returned letter to CCC. CSR was able to contact client and confirm address. A breach notification letter and copy of result letter was mailed to client's updated address	Mar-27-2013	Breach notification letter and copy of result letter was mailed to client's updated address
Privacy Analyst	Mar-07-2013	Mar-07-2013	External	Results letter opened by unintended recipient.	CC received an opened reminder letter from FH returned mail. CSR was unable to contact the client and confirm correct address	Mar-25-2014	CSR was unable to contact the client and confirm correct address
Privacy Analyst	Mar-04-2013	Mar-04-2013	External	Results letter opened by unintended recipient	The CC received a results letter from FH returned mail. The letter was opened. CSR was unable to contact the client for correct address	Mar-08-2013	CSR was unable to contact the client for correct address
Privacy Analyst	Mar-04-2013	Mar-04-2013	External	Birthday letter opened by unintended recipient	CC received opened Birthday letter from fulfillment house with hand written note "not at this address". CSR unable to contact client to confirm correct address	Apr-12-2013	CSR unable to contact client to confirm correct address
Privacy Analyst	Mar-04-2013	Mar-04-2013	External	Results letter opened by unintended recipient	FH returned an opened result letter. CSR was able to confirm the correct address and a breach notification letter was sent	Apr-03-2013	Breach notification letter sent to client
Privacy Analyst	Feb-19-2013	Feb.19-2013	External	Client called to say neighbor had opened her results letter. Client gave the correct address.	CSR requested a copy of lab form and confirmed that the PCP had entered the wrong apartment number. CSR sent out the breach notification letter for people who report their own breaches	Feb-22-2013	Breach notification letter sent to client
Privacy Analyst	Feb-14-2013	Feb-14-2013	External	Birthday letter opened by unintended recipient	FH dropped off opened birthday letter	Feb-14-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Feb-12-2013	Feb. 12-2013	External	Birthday letter opened by unintended recipient	Open birthday letter fwd from FH. CSR was able to speak to the client, who refused to confirm his address and said he would contact his PCP about Cancer screening	Feb-22-2013	Client did not confirm address and notification letter was not sent.

Privacy Analyst	Feb-12-2013	Feb. 12-2013	External	Results letter opened by unintended recipient	Call Centre received an opened results letter via FH with a sticker "moved". Client gave permission to speak to his wife and CSR was able to confirm the correct address. A breach notification letter and copy of the letter was sent to the client	Feb-22-2013	Breach notification letter sent to the client
Privacy Analyst	Feb-12-2013	Feb-12-2013	External	Reminder letter opened by unintended recipient	opened recall letter returned through FH returned mail. CSR was unable to contact the client	Feb-22-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Feb-08-2013	Feb. 8-2013	External	Birthday letter opened by unintended recipient	Recipient asked to stop sending letters to her address and would not mail back the opened letter. She was asked to shred the letter. CSR was unable to confirm the correct address	Feb-22-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Feb-02-2013	Feb.6-2013	External	Results letter opened by unintended recipient.	CSR was able to contact the client, confirm the address.	Feb-22-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Feb-02-2013	Feb-12-2013	External	Birthday letter opened by unintended recipient	FH dropped opened birthday letter. CSR unable to contact client	Feb-26-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Feb-01-2013	Feb-1-2013	External	Birthday letter opened by unintended recipient	Opened letter received from FH returned mail. CSR was unable to contact the client and confirm correct address	Feb-1-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Feb-01-2013	Feb-1-2013	External	Results letter opened by unintended recipient	FH returned opened results letter to CCO. CSR was able to contact client and confirm correct address	Feb-2-2013	Breach notification letter sent to the client
Privacy Analyst	Feb-01-2013	Feb.2-2013	External	Birthday letter opened by unintended recipient returned with a sticker "moved"	CSR was unable to contact client and confirm the correct address	Feb-22-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Feb-01-2013	Feb-01-2013	External	Birthday letter opened by unintended recipient	Opened birthday letter returned from FH. CSR was unable to contact client to confirm correct address	Feb-08-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Feb-01-2013	Feb-01-2013	External	Results letter opened by unintended recipient	FH returned an opened result letter. CSR was able to confirm the correct address and a breach notification letter was sent	Feb-06-2013	Breach notification letter sent to client
Privacy Analyst	Jan-29-2013	Feb.22-2013	External	Results letter opened by unintended recipient - reporter agreed to mail back the letter	CSR was able to contact the client, confirm the address and a breach notification letter along with the result letter was sent to the client	Feb-22-2013	Breach notification letter sent to the client
Privacy Analyst	Jan-25-2013	Jan-25-2013	External	Birthday letter opened by unintended recipient	FH returned opened birthday letter. CSR was unable to contact the client to confirm correct address	Jan-25-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jan-23-2013	Jan-23-2013	External	Results letter opened by unintended recipient	CC received opened result letter from FH. CSR was able to contact the client to confirm the correct address. Another copy of the result and a breach letter notification was sent	Mar-15-2013	Breach notification letter sent to the client

Privacy Analyst	Jan-23-2013	Jan-23-2013	External	Reminder letter opened by unintended recipient	Unintended recipient called to say she has been receiving letters for a client and does not know anyone by that name. She will shred the letter. CSR was unable to contact the client	Jan-23-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jan-23-2013	Jan-23-2013	External	Results letter opened by unintended recipient	Results letter was returned opened from FH with moved sticker. CSR was unable to contact client	Jan-23-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jan-22-2013	Jan-22-2013	External	Results letter opened by unintended recipient	Unintended recipient called to report she had received the client's result letter. She has been at that address since 1976 and has received various other mail. She agreed she would mail back the result letter. CSR was able to contact the client and confirm the correct address. CSR send breach notification letter	Jan-22-2013	Breach letter sent to client
Privacy Analyst	Jan-18-2013	Jan-18-2013	External	Client called to complain her letter had gone to wrong unit in her apartment bldg. And was opened by neighbor but was in her possession	CSR confirmed the correct address with the client and sent a breach notification letter	Jan-18-2013	Breach notification letter sent to client
Privacy Analyst	Jan-16-2013	Apr-18-2013	External	Results letter opened by unintended recipient.	Unintended recipient called to say he is receiving CCC correspondence for two people who do not live at this address. Last letter he threw out and todays letter he would return to CCO. CSR was able to locate file for the 2nd client and confirm address but unable to locate the first client	Jan-24-2013	CSR was unable to contact both clients to confirm correct address.
Privacy Analyst	Jan-15-2013	Jan-15-2013	External	Reminder letter opened by unintended recipient	Unintended recipient called to report he had received a letter that was not for him. He opened the letter and has misplaced it and would not return it to CCO. CSR asked him to destroy it. InScreen has the same number as the unintended recipient. PCP also has ben same number and no valid number was found in 411. CSR could not contact the client to confirm correct address	Jan-15-2013	No valid phone # listed InScreen, 411 and the client does not have a PCP
Privacy Analyst	Jan-15-2013	Jan-15-2013	External	Reminder letter opened by unintended recipient	Reminder letter was returned to the call center via FH returned mail. Letter was opened and then taped with sticker say "moved/return to sender" CSR unable to contact the client to confirm correct address	Jan-15-2013	No valid phone # listed InScreen, 411 and the client does not have a PCP
Privacy Analyst	Jan-15-2013	Jan-15-2013	External	Birthday letter opened by unintended recipient	Unintended recipient, the new resident of the address, called to say she had opened a birthday letter for the old resident who has moved away to China and claimed she had torn it up and disposed it. CSR unable to verify if client has indeed moved to China or to confirm the correct address	Jan-20-2013	CSR was unable to contact client to confirm correct address

Privacy Analyst	Jan-15-2013	Jan-15-2013	External	Birthday letter opened by unintended recipient	Received opened CRC Birthday letter from FH returned mail. Someone had opened it and "wrong address" marked on it and a Canada Post sticker "moved" on it. There was no phone # and CSR was unable to contact the client to confirm the correct address	Jan-15-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jan-15-2013	Jan-15-2013	External	Birthday letter opened by unintended recipient	CSR rec'd a call from an individual who reported receiving a birthday letter - pointed out that she has been receiving mailings for people she bought the house from who have since moved overseas. The mail had been discarded. CSR unable to contact the client	Jan-25-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jan-09-2013	Jan-9-2013	External	Birthday letter opened by unintended recipient	CRC birthday letter came back from FH returned mail with notification "moved". CSR unable to confirm correct address	Jan-9-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jan-09-2013	Jan-9-2013	External	Results letter opened by unintended recipient	Fulfillment house dropped of a package of returned mail. In it was the opened results letter with "moved" note. CSR able to contact client to confirm address and a breach notification was sent out	Jan-18-2013	Breach notification letter was sent out
Privacy Analyst	Jan-09-2013	jan-9-2013	External	Results letter opened by unintended recipient	Breach letter came back from FH return mail marked "moved". CSR was able to contact the client and confirm the correct address	Jan-24-2013	Breach notification letter sent to client
Privacy Analyst	Jan-03-2013	Jan-3-2013	External	Birthday letter opened by unintended recipient	Client's birthday letter was returned by FH. CSR was unable to contact the client to confirm the correct address	Jan-18-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Jan-03-2013	Jan-03-2013	external	Results letter opened by unintended recipient.	Clients daughter called to say she received letter intended for her mother (has the same last name) and will return the letter to mom and not mail it back to CCO. CSR to call client in February to confirm the correct address. CSR contacted the client, confirmed address and a breach notification letter and result letter was sent to client	Feb-04-2013	Breach letter and result letter sent to client
Privacy Analyst	Jan-02-2013	Jan-02-2013	External	Results letter opened by unintended recipient	Recipient called to report he has received a results letter, however he has never done an FOBT test. The letter had his name on it and said there are at least 4 people in town with the same name. CSR looked by callers files and no correspondence had been sent to him. CSR instructed home to send the letter back to CCO. CSR was able to find the individual and contacted him to confirm the address and sent out a breach notification letter	Jan-2-2013	Breach notification letter sent to client
Privacy Analyst	Dec-19-2012	Dec-19-2012	external	Results letter opened by unintended recipient	Unintended recipient called to say she received a results letter for someone else and had opened it. Agreed to return letter. CSR contacted the client and confirmed the correct address.	Jan-02-2013	breach notification letter and a copy of the result letter was sent to client

	Dec-17-2012	Dec-17-2012	External	Results letter opened by unintended recipient	Unintended recipient call to say received a results letter for someone else and opened it. Agreed to return letter back to CCO but never received by CSR. CSR was able to contact the client, confirm the correct address		Breach notification letter and a copy of results was sent to the client
Privacy Analyst	Dec-12-2012	Dec.12-2012	External	Results letter opened by unintended recipient	Unintended recipient called to inform that he received a result letter for someone else and he had opened it. He agreed to send the letter back to CCO but was never returned to CCO. CSR unable to contact client to confirm the correct address	Dec-13-2013	CSR was unable to contact client to confirm correct address
Privacy Analyst	Nov-24-2012	Nov-24-2012	External	Birthday letter opened by unintended recipient who returned the letter to the client	CSR was able to contact client and confirm the correct address and a breach letter was sent	Nov-26-2013	CSR was able to contact client to confirm correct address
Privacy Analyst	Aug-09-2012	Aug-9-2012	External	Birthday letter opened by unintended recipient	Unintended recipient send letter back to CCO, however CCO never received it. When called, told the client would not be back in the country until 2013 but when contacted again…still out the country. Program left to decide whether to close the case and they decided to close the case.	Jan-21-2013	CSR was unable to contact client to confirm correct address

APPENDIX I: Indicators – Summary from the Log of Security Audits & Information Security Breaches

Vulnerability Assessments

#	Name	Project	Date
1	VA for CBCRP Upload Tool	EBP	12-Oct-11
2	VA Scan for OPIS	STIP	18-Nov-11
3	VA Scan for Drug Formulary Enhancement/Content Management System (**CMS**)	CMS	9-Dec-11
4	VA Scan for CIRT	PCCIP	19-Jan-12
5	VA Scan for DAP/EPS	DAP/EPS	19-Jan-12
6	VA Scan # 2 for CIRT	PCCIP	26-Jan-12
7	Performing a Malware Scan	INFRAST	9-Feb-12
8	VA for MS Exchange 2010 Servers	INFRAST	13-Feb-12
9	VA for ICS Release 2.0 PROD	PCCIP	22-Feb-12
10	VA for ICS Release 3.0 UAT	PCCIP	23-Feb-12
11	VA for Tumbleweed	INFRAST	8-Mar-12
12	VA for ICMS Project	PCCIP	16-Apr-12
13	VA for OBSP PACS	PCCIP	23-May-12
14	VA for ISAAC new Development	ISAAC	24-May-12
15	VA for Data Book Automation Project	Data Book	28-May-12
16	VA for Secure Messaging	INFRAST	20-Jun-12
17	VA for Secure Messaging	INFRAST	6-Jul-12
18	VA for eLab	INFRAST	23-Jul-12
19	VA for CMS	INFRAST	2-Aug-12
20	VA for WTIS	WTIS	9-Aug-12
21	VA for FIT Pilot project	WTIS	24-Aug-12
22	VA for Databook Automation	WTIS	31-Aug-12
23	VA for Timekeeper	INFRAST	17-Sep-12
24	VA for Web Application Firewall	INFRAST	26-Sep-12
25	VA for OHIP Integration	EDW	26-Sep-12
26	VA for FIT Project PRD Environment	INFRAST	26-Sep-12
27	VA for eLab PRD Environment	eLab	4-Oct-12
28	VA for Informatica	EDW	15-Oct-12
29	VA for new CMS	CMS	19-Oct-12

Threat Risk and other Assessments

#	Name	Date
1	Wait Times TRA	17-Oct-11
2	SharePoint External Collaboration TRA	27-Oct-11
3	EDW Integration Project TRA	31-Oct-11
4	DAP - EPS TRA	1-Nov-11
5	Diagnostic Data Upload Tool TRA	16-Nov-11
6	Secure Messaging TRA	17-Feb-12
7	OBSP-PACS TRA	1-Mar-12
8	Conceptual NDFP TRA	4-Mar-12
9	Telecommuting TRA	23-Apr-12
10	New Data center TRA	10-May-12
11	DataBook Automation TRA	25-May-12
12	eLab TRA	17-Aug-12
13	Head and Neck TRA	15-Sep-12
14	Data Holdings TRA	11-Feb-13
15	eClaims TRA	3-May-13
16	ISAAC TRA	7-May-13
17	Hallogen SSO TRA	10-May-13
18	EDW TRA	13-May-13
19	SSO IS TRA	31-May-13
20	ORRS TRA	6-Jun-13
21	InScreen TRA	6-Jun-13
22	Lync TRA	16-Aug-13
23	SSO IS TRA	20-Oct-13

Other Assessments

#	Name	Date
1	Hosted Email Security Analysis	9-Dec-11
2	ALC RMR Security Framework	16-Feb-12
3	MFT-Tumbleweed Security Assessment	5-Jun-12

30	VA for PROD Databook Automation	Data Book	24-Oct-12
31	VA for PPM Mobile App	Mobile PMO	25-Oct-12
32	VA for Head and Neck PROD	Head & Neck	29-Oct-12
33	VA for CIRT Dev	PCCIP	30-Oct-12
34	VA for SMG	CMS	21-Nov-12
35	VA for DAP/EPS	DAP/EPS	23-Nov-12
36	VA for eClaims	NDFP	3-Dec-12
37	VA for ISAAC 2.0 prePROD	ISAAC	11-Dec-12
38	VA for eReport	Secure Msg	18-Jan-13
39	VA for CCC Migration PROD Environment	PCCIP	24-Jan-13
40	VA for WTIS R16 PrePROD Environment	WTIS	25-Jan-13
41	VA for eClaims	NDFP	28-Feb-13
42	VA for ORRS	ORN	28-Feb-13
43	VA for ISAAC	ISAAC	28-Feb-13
44	VA for EDW	EDW	28-Feb-13
45	VA for PPM Mobile App Phase II	Mobile PMO	20-Mar-13
46	VA for Informatica v9.5.1	PCCIP	21-Mar-13
47	VA for eClaims	eClaims	22-Mar-13
48	VA for CCN Shared Secrets	WTIS-CCN	26-Mar-13
49	VA for EDW	EDW	27-Mar-13
50	VA for KTE Clinical	KTE Clin Tools	10-Apr-13
51	VA for Data Monitor Tool	STIP	10-Apr-13
52	VA for Inscreen	PCCIP	1-May-13
53	VA for SAS Data Quality	SAS	6-May-13
54	VA for eClaims - DSP	NDFP	15-May-13
55	VA for - ISAAC Mobile App VA	ISAAC	23-May-13
56	VA for Data Governance Workflows	Data Gov	24-May-13
57	VA for - eProcurement	eProcurement	27-May-13
58	VA for SCSM Surveys	INFRAST	3-Jul-13
59	VA for ORRS Upload Tool	ORN	3-Jul-13
60	VA for BayesiaLab	BayesiaLab	9-Jul-13
61	VA for WTIS R16 PrePROD Environment	WTIS	26-Aug-13
62	VA for ICMS	ICMS	17-Sep-13
63	VA for eReports	eReports	10-Oct-13

4	FIT Security Profile	20-Jul-12
5	OFCCR Transfer Security Assessment	Mar-13
6	Cloud Assessment	19-Apr-13
7	Enterprise Information Program Assessment and IAM Roadmap	19-Apr-13
8	Enterprise Risk Management Harmonization	8-Oct-13
9	One ID Password Authentication Assessment	31-Oct-13

Information Security Breaches and Suspected Information Security Breaches

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	The date that senior management was notified	The containment measures implemented	The date(s) that the containment measures were implemented	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	The manner in which each recommendation was addressed or is proposed to be addressed
Information Security Incident, triggered by employee reporting a system malfunction.	31-JUL-12	CMS website was compromised with SQL injection attacks.	PHI was not at risk due to segregated networks and no PHI being stored within the CMS.	1-AUG-12	Technical measures were taken to block the modification of the CMS database.	2-AUG-12	31-JUL-12	22-AUG-12	Recommendations made to transition to a new CMS product and to implement additional review and safeguards for current implemented system.	All recommendations have been address as of December 2012. Some recommendations relate to process changes that continue to be applied as new technologies are implemented. e.g. templates for secure configurations of systems	All recommendations were addressed through existing risk management processes, by internal CCO resources.
Information security incident, triggered by employee reporting unusual volumes of SPAM being sent by CCO email servers.	19-AUG-12	A small number (approx.. 10) CCO user accounts were compromised through a phishing attack.	PHI was not at risk based on the impacted email accounts not containing PHI and the containment of the account compromise before other systems could be accessed.	19-AUG-12	All impacted accounts were suspended while the affected users reset their credentials.	19-AUG-12	19-AUG-12	21-AUG-12	Recommendations made to conduct additional security training for users.	All recommendations were addressed as of December 2012	The Privacy and Security annual refresher was updated to include additional training on security threats such as phishing.
Vulnerability discovered within the ESS-VIP (payroll)	1-JUL-13	Low	No PHI/No breach.	1-JUL-13	Third party provider notified.	16-JUL-13	1_JUL-13	16-JUL-13	Asked 3rd party provider to perform a full TRA and vulnerability assessment	16-JUL-13	Notification from the 3rd party to CCO about the VA performed in the system

applicatio n											
Three computer s were infected with Malware and communi cated with the Internet	15-JUL-13	Low	No PHI/No breach	15-JUL-13	Accounts were deactivat ed.	15-JUL-13	15-JUL-13	15-JUL-13	User Education. Patch Management review	15-JUL-13	One-on-one training with the User
Laptop was forgotten in the train	26-JUL-13	Low	No PHI/No breach	26-JUL-13	Laptop was encrypte d as per Policy. User changed his passwor d.	26-JUL-13	26-JUL-13	26-JUL-13	User Education.	29-JUL-13	One-on-one training with the User
Sensitive Docume nts were scanned using an internal multi-function device and sent to the wrong employe e in CCO.	15-AUG-13	Low	No PHI/No breach	15-AUG-13	Wrong recipient deleted the scanned email.	15-AUG-13	15-AUG-13	16-AUG-13	Improve the card registration process	1-SEP-13	Printer vendor created and implemented Script to accept only photo badges thus improving the registration process
A small set of records containin g PHI was mistakenl y copied in a DEV Databas e	2-OCT-13	Low	PHI involved/No breach	2-OCT-13	PHI deleted.	2-OCT-13	2-OCT-13	4-OCT-13	Process Review. User training	4-OCT-13	One-on-one training with the User. Process to load data to DEV environment was revised.

APPENDIX J : Indicators – Log of Statements of Purpose

PRESCRIBED ENTITY

Data Holding	(1) Statement of Purpose & (2) Need for PHI	Data	Source
Dyspnea Management Program	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.	This dataset contains: • Clinical data • Demographic data	Hospitals
Stem Cell Transplant (SCT)	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	This dataset contains: • Patient Demographic data • Clinical / Stem Cell Transplants data • File Descriptor data	Hospitals
Brachytherapy Funding Program	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.	This dataset contains: • Clinical data • Demographic data	Referring physicians
Ontario Cancer Symptom Management Collaborative (OCSMC) Symptom Management Reporting Database	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. 2. PHI is collected to evaluate the provision of symptom management and palliative care planning for cancer patients in Ontario.	This dataset contains: • Demographic data • Clinical data	Hospitals
New Drug Funding Program (NDFP)	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.	This dataset contains: • administrative data • clinical data (eligibility criteria) • demographic data	Hospitals

Evidence-Building Program (EBP)	1. The EBP database stores patient and treatment information about systemic therapy drug utilization at Ontario hospitals, for which reimbursement is being sought through the EBP according to strict eligibility criteria. 2. PHI is collected for CCO EBP to reimburse hospitals for those patients who have met the eligibility criteria.	This dataset contains: • administrative data • clinical data (eligibility criteria) • demographic data	Hospitals
Case-by-Case Review Program (CBCRP)	1. The CBCRP database stores patient and treatment information about systemic therapy drug utilization at Ontario hospitals, for which reimbursement is being sought through the CBCRP according to strict eligibility criteria. 2. PHI is collected for CCO CBCRP to reimburse hospitals for those patients who have met the eligibility criteria.	This dataset contains: • administrative data • clinical data (eligibility criteria) • demographic data	Hospitals
Ontario Positron Emission Tomography Scan Evidence-Based Program (EB-PET Program)	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 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.	This dataset contains: • Clinical data • Patient demographic data • Physician demographic data -Administrative data	• Referring physicians • Diagnostic centres
Collaborative Staging	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 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, screening, and treatment data.	This dataset contains: • administrative data • clinical data • demographic data - facility data	• Ontario Cancer Registry • Pathology Datamart • Hospital patient health records

Diagnostic Assessment Program (DAP)	1. The purpose of the data holding is to securely store data (including PHI) collected from all regional cancer programs for DAP oversight. 2. PHI is collected to evaluate the impact DAPs have on patients in the diagnostic phase of the cancer journey.	This data holding contains the following categories of data: • clinical data, demographic data, wait times data, usage data, administrative data	Hospitals
ePath	1. The Pathology 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. ePath 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 Screening Registry.	This dataset contains: • administrative data • clinical data • demographic data • facility data	• Hospitals • Some commercial laboratories
National Ambulatory Care Reporting System (NACRS)	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.	The dataset contains: • administrative data • demographic data • clinical data	Canadian Institute for Health Information (CIHI)
Discharge Abstract Database (DAD)	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.	The dataset contains: • administrative data • demographic data • clinical data	Canadian Institute for Health Information (CIHI)

Ontario Cancer Registry Information System (OCSRIS)	1. The Ontario Cancer Screening Registry (OCSR) 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 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.	This dataset contains: • administrative data • clinical data • demographic data	• CIHI (DAD, NACRS) • 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, 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
Mortality Data	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 measure cancer survival.	The dataset contains: • administrative data • demographic data	• Ministry of Government Services • Office of the Registrar General
Out of Province (OOP) Data	1. This data holding contains persons with OCSR reportable diseases. The purpose of these records is to serve as source records to create incident cases for the Enterprise Data Warehouse (EDW)-OCSR. 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.	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
Pathology Datamart	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 incidence case data in the OCSR.	This dataset contains • administrative data • clinical data • demographic data • facility data	PIMS

RPDB Datamart	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.	The dataset contains: • Ontario Health Insurance Number • administrative data • demographic data	Ministry of Health and Long-Term Care
Interim Annotated Tumour Project (ATP) Database	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 OCSR, 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.	The dataset contains: • administrative data • clinical data • demographic data	• OICR • CCO's Cancer Registry
Ontario Renal Network (ORN)	1. The purposes of the ORN data holding are • Performance measurement and management; • Monitoring of system quality; • System planning; and • CKD funding model development. 2. PHI is used to support management decision-making, planning, disease surveillance and research activities.	The dataset contains: • Clinical data • Demographic data	Hospitals
Wait Times Information System (WTIS)	1. The purpose of this data holding is to enable the 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 Enterprise Master Patient Index (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.	The dataset contains: • administrative data • clinical data • demographic data	• Hospitals • EMPI
Emergency Room National Ambulatory Reporting System Initiative (ERNI)	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.	The dataset contains: • clinical data • demographic data	Hospital sites submit to CIHI-NACRS. Extract of file is transferred securely from CIHI to ATC Informatics within CCO using Tumbleweed

Ontario Laboratory Reporting System (OLIS)	1. To support CCO's ORN and DAP-EPS Programs in accordance with CCO's Data Privacy Agreement with the MOHLTC as a PE, as amended. 2. PHI is required to enable CCO to link OLIS data with its patient records within other PE data holdings – such linkage is required to carry out health analytics.	This dataset contains: • Laboratory test result information from patients across Ontario	MOHLTC (via eHealth Ontario)
Multidisciplinary Cancer Conference (MCC)	1. The purpose of the data holding is to obtain a better understanding of the outcome of individuals being discussed at MCCs (e.g. other patient conditions, or other patient treatments), as well as to analyze patient movement within and between facilities. 2. PHI is collected to conduct analysis and provide operational advice with respect to MCC initiatives in Ontario, to the MOHLTC, the MCC facilities, and the Local Health Integration Networks (LHINs).	This dataset contains: • Administrative data • Clinical data	Hospitals
eOutcomes – Head & Neck	1. The purpose of the data holding is to capture and monitor outcomes data for patients with head and neck cancer treated with radiotherapy in a provincial, systematic way. 2. PHI is collected to ensure accurate capture of patients' outcomes post-radiotherapy, and to facilitate the identification of inadvertent duplicate cases.	This dataset contains: • Clinical data (e.g. outcomes, diagnosis, radiotherapy details) • Demographic data (patient name, MRN)	• Physicians / Data Managers (outcomes) • ALR Data (diagnosis, radiotherapy details)

PRESCRIBED REGISTRY

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

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

Screening Hub Stage – LIRT	1. The purpose of this data holding is to gather information from laboratories on FOBT results. 2. The data collected through the LIRT are FOBT results that is used for (a) generate participant communications; and (b) monitoring and reporting on FOBT volumes, geographic differences, test quality, variations between participating laboratories and highlighting the need for further awareness or education programs.	This dataset contains: • Administrative Care • Clinical Data • PHI	• Laboratories
Screening Hub Stage - OPDB (Pharmacy Claims)	1. The purpose of this data holding is to gather information of FOBT dispensed by pharmacies. 2. This data will be used to evaluate the level of dispensing of FOBT kits at the pharmacies.	This dataset contains • Administrative Pharma Data • PHI	• MOHLTC
Screening Hub Stage - OCSR	1. The OCSR is a computerized database of information on all Ontario residents who have been diagnosed with cancer ("incidence") and/or who have died of cancer ("mortality"). All new cases of cancer are registered, except non-melanoma skin cancer. 2. This information is used to support OCSR by identifying individuals who are ineligible for colorectal and cervical screening.	This dataset contains: • Administrative Care • Clinical Data • PHI	• CCO as PE
Screening Hub Stage - RPDB	1. This data holding contains information from Registered Person Database. This data is used in operationalization of colorectal and cervical screening. 2. This data will be used to identify Ontarians who are eligible and could be invited to participate in the CCC program. It will also be used for identity validation and data linking for client cancer journey assessment.	The dataset contains: • Administrative Care • Clinical Data • PHI	• MOHLTC
Screening Hub Stage - Siebel	1. The purpose of this data holding is to integrate information for InScreen. 2. Recent Client, Address and Screening related activity within Siebel InScreen, required in the Screening Hub for integration purposes.	The dataset contains: • Client demographics and address information • PHI	• Integration Hub • Call Centre direct entry
Primary Care Provider Reporting	1. This data holding contains information on primary care providers. 2, This is used to store primary care provider screening activity reports. The reports summarizes client level information for providers.	This dataset contains: • Clinical data • PHI	• Integration Hub • Siebel

Ontario Cervical Screening Program (OCSP)	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. PHI is also collected for OCSP client management and operations including, clinical results, direct client interactions and correspondence	This dataset contains: • Administrative data • Clinical data • Demographic data	CytoBase RPDB OCSR
Cytobase	1. The purpose of this data holding is: -to carry out the mandate of the CSP -to facilitate the provision of health care related to cervical cancer screening to allow CCO to notify participants of their results -to maintain the OCSR -to conduct cancer planning and management as well as to perform quality and program management functions.	This dataset contains: • Demographic data about the patient, the requesting physician and the laboratory that assessed the test • Health information number • cervical test result	CytoBase
OCSP - Siebel	1. The purpose of this data holding is to support Integrated Screening Operations, Planning and Performance. 2. Integrated Screening Siebel CRM system. It is a front end system for InScreen client management and operations including, Clinical Results, direct client interaction and Correspondence.	This dataset contains: • Clinical data • Demographic and address data • Call centre operational activities data	• MOHLTC (RPDB, HNS, CHDB, CPDB, CAPE) • Cytobase • Fulfillment House • Statistics Canada (PC to LHIN) • Call Center direct data entry
Oracle Business Intelligence Enterprise Edition (OBIEE)	1. The purpose of this data holding is to provide segmentation of data which enables Siebel CRM, via Campaign Management, to generate invitation, reminder, recall and test result notification correspondence for each of the three Cancer Screening modules (CCC, OCSP and OBSP).	This dataset contains: • Clinical data • Demographic and address data • Call centre operational activities data	• This dataset is populated with data from Siebel CRM and the Integration Hub.
Ontario Breast Screening Program (OBSP)	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. PHI is also collected for OBSP client management and operations, including clinical results, direct client interactions and correspondence.	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,	• data entry by OBSP sites • OCSR data linkage • Death registry linkage

		correspondence data)	
Mortality Data	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 Screening Registry and for measuring cancer survival.	The dataset contains: • administrative data • demographic data	• Ministry of Government Services • Office of the Registrar General

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. CCO continues to strive 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 PAO, 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.

Throughout 2014/15, CCO will be finalizing and implementing a number of enhancements to its privacy and security programs, including initiating the implementation of the de-identification tool, enhancements to the ERM program, refreshing the data stewards, privacy and security leads programs, and creating a more robust privacy and security training program. As the organization is reorganized, CCO will continue to focus on ensuring the continued effectiveness of its privacy and security governance.

The PAO and the EISO continue to work toward integration and harmonization of policies and practices to ensure not only a compliant organization, but effective and meaningful privacy and security programs. As the information needs of the healthcare sector evolve, so too must our data protection efforts. CCO looks forward to a continuing relationship with the IPC to identify, define and manage personal health information for the benefit of all Ontarians.

SWORN AFFIDAVIT

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

1. Cancer Care Ontario (CCO), a prescribed entity 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 and a prescribed person under subsection 13(1) of Ontario Regulation 329/04 for the purposes of subsection 39(1)(c) 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 CCO comply with PHIPA and the regulations thereto.

3. The policies, procedures and practices implemented by CCO 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. CCO 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. CCO 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 of Toronto, in the Province)
)
of Ontario, on _____ 2014.)
)

_____

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
Erica Zarkovich

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

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

4. ***Application for Disclosure of 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 Framework*** contains supporting information for the Business Continuity Plan 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.

9. ***Business Continuity Plan*** guides the business continuity operations for mission critical processes and services in the event of a threat or interruption that compromises the ability for CCO 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. Contact processes for the fan out phase are delineated, message templates are included and can be found in the appendices.

10. ***Business Continuity Worksheet*** is used to document events and activities where disaster or the risk of disaster has been identified and the CIO's Business Continuity Plan has been activated.

11. ***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.

12. ***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.

13. ***Change Management Policy Suite*** controls and manages 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. The Change Management policy suite listed below 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

Supporting documents include:

- Change Management Policy
- Change Management Process (Standard Changes)
- Change Advisory Board Terms of Reference
- Change Management: Request for Change Lead Time
- Standard Change Application Form
- Change Management: Change Calendar (Draft)
- Change Management: Change Category and Type (Draft)
- Change Management Request for Change (RFC)
- Change Request Control Form
- IT Change Control Process Instructions (Draft)

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

15. ***Confidentiality Policy*** clearly 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 PHI.

16. ***Consulting Agreement*** is a services agreement that contains a template schedule entered into between CCO and consultants who will be permitted to access and use PHI. The template schedule, together with the baseline terms of the main Consulting Agreement, sets out

the privacy and security responsibilities of the consultant in respect of PHI that it accesses, retains, transfers or disposes of on behalf of CCO.

17. ***Core Privacy & Security Training eLearning Curriculum*** is a web-based, in-depth, compulsory training program for new employees, including service providers with access to PHI, students, volunteers, researchers and others with access to CCO systems, addressing CCO's Privacy and Information Security Programs. All CCO employees, as well as consultants, students, volunteers, researchers and others with access to CCO systems, must complete the Core Privacy & Security Training Curriculum and accept the Privacy and Security Acknowledgement form prior to receiving access to PHI at CCO.

18. ***Courier Transfer of Personal Health Information Procedure*** establishes the parameters and methods for the secure transfer of personal health information via courier.

19. ***Cryptography Standard*** broadly defines the 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

20. ***CSP Privacy Breach Management Standard Operating Procedure*** applies to CCO in its capacity as a Prescribed Person. This procedure, along with the Privacy Breach Management Procedure, describes how CSP will identify, manage and resolve privacy breaches which occur as the result of misuse or improper/unauthorized collection, use and disclosure of PHI by CCO employees, consultants and contractors. Specifically, the procedure defines a privacy breach, identifies the parties which must be notified of a privacy breach, and outlines the steps to be taken by CCO once a privacy breach has occurred, including the nature and scope of the investigation of the breach, retrieval of PHI, and the steps taken to prepare privacy breach notification communications.

21. ***CSP Privacy FAQs*** are a list of frequently asked questions which the PAO receives regarding its privacy policies and practices in relation to the CSP program. It identifies the status of CCO under PHIPA as a Prescribed Person and the purposes of collection, use and disclosure of PHI within the custody and control of CCO for its CSP program, including how to access patient screening results and contact information.

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

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

24. ***Data Backup Procedure*** defines the operational processes and standards relating to

CCO's backup and recovery services.

25. ***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.

26. ***Data Governance Council Terms of Reference*** (Draft), outlines the major responsibilities of this committee. The Data Governance Council is responsible for ensuring that the overall governance at CCO is conducted efficiently and in accordance with PHIPA.

27. ***Data Linkage Policy*** (Draft) defines the circumstances in which the data linkage of records of PHI is permitted. The policy also outlines the purpose of linking data at CCO, and disclosure of that linked data by CCO.

28. ***Data Linkage Procedure*** (Draft) 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 Person

29. ***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).

30. ***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.

31. ***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.

32. ***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.

33. ***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.

34. ***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.

35. ***De-Identification Guidelines*** (Under Revision) 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.

36. ***Digital Media Destruction Procedure*** describes the process used to securely dispose of digital media.

37. ***Digital Media Destruction Standard*** sets forth CCO's practices for securely disposing of digital storage media and any data contained within.

38. ***Direct Data Access Audit Procedure*** describes the process that is to be used to audit internal 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.

39. ***Disaster Recovery Plan*** is used in conjunction with the Business Continuity Plan and Business Continuity Framework to guide the decision making processes and set out priorities for those decisions. It contains a description of the roles of key staff, and system recovery dependencies. System recovery approaches for the class of services, vendor and key staff contact information are also found in the appendices along with the fan out procedure for Technology Services staff. Supported by the Emergency Preparedness Database (EPD), specifically with respect to the creation of lists of staff and their relevant contact information. The list can be emailed or printed and delivered to managers to utilize to call and log contact success. Communication and training plans have been developed to supplement Disaster Recovery.

40. ***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.

41. ***Employee Exit Process*** ensures that a systematic uniform exit procedure is followed for all employees, contractors, and volunteers, upon the cessation of their employment or other relationship with CCO. The process sets out the roles and responsibilities of departing employees, contractors, 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.

42. ***Enterprise Risk Management Framework*** sets out applicable risk management processes and documents the roles and responsibilities of CCO Staff and CCO's Board in identifying, assessing, mitigating (to the extent possible) and monitoring material risks, and outlines key aspects of CCO's risk management and reporting processes. Provides a comprehensive process to evaluate material risks to integrate and align existing risk management processes across CCO. It provides departments and programs with established risk assessment processes to identify, assess, mitigate (to the extent possible) and monitor risk in accordance with set standards.

.

44. ***Exchanging Encrypted Personal Health Information on Digital Media*** sets out the parameters for and roles and responsibilities of the parties involved in exchanges of PHI on Digital Media.

45. ***Exchanging Personal Health Information via Application Services Procedure*** sets out the parameters for and roles and responsibilities of the parties involved in exchanges of PHI via Applications Services.

46. ***Exchanging Personal Health Information via Secure Managed File Transfer Procedure*** sets out the responsibilities of the Business Unit when conducting exchanges of PHI via file transfer.

47. ***Exiting Employee Data Management*** sets out parameters for management of employee data after their departure.

48. ***Fax Transmission of Personal Health Information Procedure*** sets out the parameters and roles and responsibilities when conducting fax transmissions of PHI.

49. ***Hard Copy Personal Health Information Disposal Procedure*** sets forth CCO's requirements for the secure disposal of hard-copy records containing personal health information, including shredding service vendor contract requirements and shredding disposal requirements.

50. ***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.

51. ***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 managed and all supporting business units are engaged.

52. ***Incident Management Framework*** provides guidance for the development of standards and procedures establishing 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.

53. ***Information Security Code of Conduct and Acceptable Use Policy*** 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.

54. ***Information Security Framework*** defines the foundational components of the information security program and contains informational elements useful to the understanding, implementation, and administration of the program.

55. ***Information Security Incident & Breach Response Management Standard*** defines the baseline practices to address the identification, reporting, containment, notification, investigation and remediation of information incidents and breaches.

56. ***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.

57. ***In Person Transfer of Personal Health Information Procedure*** sets out the parameters and roles and responsibilities when conducting transfer of PHI in person.

58. ***Internal Data Access Policy*** describes the considerations applicable to users requesting direct access to record-level Personal Health Information (PHI) in CCO's data holdings. Specifically, the policy 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.

59. ***Internal Data Access Procedure*** describes the process CCO will use to grant, deactivate, or change direct access to CCO data holdings for internal users (including CCO staff, consultants and contractors) and describes the process and tool (IDAR) used to request direct access to CCO data holdings of PHI for all internal users, including CCO employees, consultants and contractors.

60. ***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
- Senior Privacy Specialist
- Manager, Privacy
- Privacy and Access Analyst
- Privacy Specialist

61. ***Job Description for the Position(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 Manager, Information Security
- Technical Architect, Information Security
- Senior Information Security Specialist
- Technical Specialist, Information Security

62. ***LMAS Threat Modeling Guide*** provides guidelines for identifying and documenting high-risk threat scenarios to CCO's critical assets and describes the process for identifying potential threats to CCO's critical assets and identifying detection controls (e.g. monitoring rules.

63. ***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.

64. ***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.

65. ***Mobile Device and Pager Policy*** defines the terms and conditions for authorizing personally owned mobile devices to access CCO corporate services, including a requirement for technical security controls.

66. ***Mobile Device and Pager Procedure*** sets out the process and standards for authorizing personally owned mobile devices to access CCO corporate services, including responsible parties.

67. ***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.

68. ***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.

69. ***Operational Security Procedure***: ***Patching*** defines the steps taken for patching CCO systems, including the monitoring of availability of patches, implementation of patches, and required documentation.

70. ***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.).

71. ***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.

72. ***PHI Handling Standard*** defines CCO's baseline secure handling practices for Personal Health Information (PHI) throughout the data lifecycle.

73. ***PHI Handling Procedure*** defines the procedures CCO follows with respect to handling of PHI including decision criteria and roles for requesting and reviewing retention of PHI on mobile devices.

74. ***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.

75. ***Physical Security Policy*** outlines the safeguarding of physical environments and sets out requirements with respect to facility access control, facility security, electronic device and media security and disposal, and hard-copy (paper) record security and disposal.

76. ***Policy on Retention of Records Containing Personal Health Information*** sets out the obligations of CCO with respect to the retention of records of PHI and describes the purposes for retention of PHI.

77. ***Principles and Policies for the Protection of Personal Health Information at Cancer Care Ontario (CCO's Privacy Policy)***, applies to CCO in its capacity as a Prescribed Entity and Prescribed Person 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.

78. ***Privacy Audit and Review 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.

89. ***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.

80. ***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.

81. ***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, and is supported by the Privacy Breach Report Form. 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.

82. ***Privacy FAQs*** are a list of frequently asked questions which the PAO 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 PAO's contact information, should there be any further questions or concerns.

83. ***Privacy Governance Framework*** sets out the privacy governance structure at CCO, as well as the operational governance structure, outlining all of the core program controls. It outlines how CCO conducts ongoing monitoring and reporting and mandates an Annual Privacy Management, Oversight and Review Plan.

84. ***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.

85. ***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 PAO will follow in responding to and tracking the inquiry or complaint and how compliance with the procedure is enforced at CCO.

86. ***Privacy and Information Security Risk Management Framework*** defines the approach by which CCO identifies, assesses, responds to and monitors privacy and security risks. It establishes a foundation for mitigating and managing privacy and security risks and sets the boundaries for risk-based decisions in respect of privacy and security within CCO. Provides a comprehensive process to evaluate privacy and security risks, and is used in conjunction with

CCO's Enterprise Risk Management Framework.

87.

88. ***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.

89. ***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.

90. ***Procurement Policy*** specifies the responsibilities of the Board, senior management and business units within CCO throughout each stage of the procurement process and sets out requirements for the protection of PHI in the context of the procurement of goods/services that could result in privacy risk.

91. ***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.

92. ***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.

93. ***Secure Transfer of Personal Health Information Policy*** establishes an enterprise-wide framework of approved methods for the secure transfer of PHI into, within, and out of the custody of CCO. This policy governs the approved methods for the transfer of paper and electronic records containing PHI and establishes accountability and enforcement measures that must be implemented to ensure that PHI is transferred in a secure manner.

94. ***Secure Transfer of Personal Health Information Standard*** sets out duties and responsibilities with respect to secure transfer of PHI and defines the approved methods of securely transferring PHI.

95. ***Security Audit, Testing, and Compliance Standard*** The standard defines the baseline practices for the audit and testing of CCO's information security. The internal audit and testing program is organized around the following core information system audit functions: Compliance and conformance auditing, Risk identification and control auditing, and Operational auditing.

96. ***Security Operations Working Group Terms of Reference***: The Security Operations Working Group (SOWG) is established to facilitate and support the effective delivery of operational security work that spans Service Management, Operational Services, and the Enterprise Information Security Office (EISO).

97. ***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.

98. ***Services Agreement - Template Schedule for Third Party Agreements*** is a services agreement that contains a template schedule entered into between CCO and third parties retained by CCO, such as contractors, consultants and third party providers that will be permitted to access and use PHI. The template schedule, together with the baseline terms of the main Services Agreement, 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.

99. ***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.

100. ***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 PAO's contact information, should there be any further questions or concerns.

101. ***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.

102. ***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.

103. ***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.

104. ***Transfer of Personal Health Information by Regular Mail Procedure*** sets out the parameters for and roles and responsibilities when transferring PHI by regular mail.

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

106. ***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.

107. ***Visitor Access Procedure*** outlines 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 policy requires the Facilities Manager to maintain a log (EasyLobby Visitor Grid) of all visitors to CCO's premises.

APPENDIX ii – 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. ***Enterprise Risk Register*** contains logs of all enterprise risk as well as recommendations to mitigate and manage those risks.

5. ***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.

6. ***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.

7. ***Internal Data Access Request (IDAR)*** tool is used for the logging of internal non-research related access and use of PHI. IDAR 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 IDAR tool logs the name of the employee, job title of the employee, the data holding the employee will have access to, the application that will be used by the individual to access the data, the type of database environment to be accessed, the type of data requested, the expiration of permissions to the data and the current status of the employees' access permissions.

8. ***CCO's PAO Program Logs*** include 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 Access Requests on the eCCO Data Access Request Tool: tracks executed Research Agreements between CCO and all researchers on the online eCCO Data Request Tool.
   iii. Log of Privacy Impact Assessments: tracks all PIAs initiated and/or completed at CCO, including identified risks and mitigating strategies.

iv. Log of Privacy Breaches: tracks all privacy incidents and breaches reported at CCO, including identified risks and mitigating strategies.
v. Log of Privacy Inquiries and Complaints: tracks all inquiries and complaints received by CCO in regards to the Privacy Program, including CSP.
vi. 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.
vii. 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.
viii. Log of Third Party Service Providers with Access to PHI (Procurement Log): tracks agreements with third parties that have access to PHI and includes the relevant dates associated with the agreement and transfer of data, the relevant business lead and responsibilities, a description of the services contracted for, and details regarding the return or destruction of the data.

9. ***Physical Security Access Card Log*** is maintained by the Facilities Coordinator and is a log of agents with access to CCO facilities and is used at sites that do not have Key Scan Software. It is updated upon receipt of notification from IT Help Desk of a termination of an employee/agent or change in access requirements.

10. ***Privacy Risk Register*** contains logs of all privacy risk as well as recommendations to mitigate and manage those risks. The log includes risks or recommendations identified through PIAs, privacy audits, privacy reviews, complaint investigations, breach reports and IPC reviews.

11. ***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.

12. ***Security Risk Register*** security risks and the corresponding asset, vulnerability, and impact information. The log aggregates risks identified through TRAs, security audits, security reviews, incidents and operational security activities.

13. ***CCO's Enterprise Information Security Office Program Logs*** include consolidated and centralized logs which track various components of the CCO security Program. Current logs include:

i. Log of Amended Policies & Procedures: Controlled document library that tracks all interim amendments made to CCO's security policies, standards, and procedures. Communication of policy changes are also tracked including a description of the amendment made and the date it was communicated to CCO employees.

ii. Log of Security Audits: tracks all security audits (TRA's, Vulnerability Assessments, Penetration tests, Security audits) initiated and/or completed at CCO. Results are logged into the Security Risk Register.

iii. Security Incident Log: log of information security breaches (including suspected breaches or "incidents").

iv. Open Media Logs: log of system backups.