Ontario Tumour Bank

Report to the Information and Privacy Commissioner Ontario in Respect of the Ontario Tumour Bank's Status as a Prescribed Person under Section 39(1)(c) of the *Personal Health Information Protection Act, 2004*

October 26, 2016
Ontario Institute for Cancer Research

Contents

BACKGROUND INFORMATION

Introduction

The Ontario Tumour Bank (OTB) is a province-wide biorepository and data bank focused on collection of tumour-related human biospecimens. It provides academic and industry cancer researchers with a diverse selection of high quality tumour-related specimens and data obtained directly by dedicated tumour bank staff, who follow a stringent set of procedures and ethical guidelines.

The biospecimens and clinical data are an important resource for scientists engaged in translational research who are developing better diagnostic tools and new drug therapies. Researchers depend on the OTB to provide research biospecimens of high quality, diversity and integrity.

Operating at state-of-the-art hospitals and cancer centres across Ontario, the OTB coordinates the collection, storage, analysis, annotation, and distribution of tumour and peripheral blood samples. Working in collaboration with local pathologists, medical oncologists, surgeons and other hospital personnel, specially trained staff obtain patient consent, collect tissues and assemble comprehensive clinical information about each donor and the corresponding samples.

OTB is a program of the Ontario Institute for Cancer Research (OICR). Funded by the Government of Ontario, OICR is a not-for-profit corporation that supports research on the prevention, early detection, diagnosis, treatment and control of cancer.

Background

OTB was established in 2004, to respond to a growing need for a provincial tissue and health data bank to support cancer research. OTB is a multi-centred program that collects blood and tissue samples as well as personal health information (PHI) from consenting research participants who have agreed to participate in the OTB. OTB is a source of high quality tumour-related bio-specimens and data for academic and industry-based researchers to conduct cancer research. The outcomes of the research studies are expected to contribute to the provision of health care for cancer patients by providing information that may lead to an increased understanding of the disease and the development of new diagnostic tools and therapies.

OTB has dedicated staff at four hospital-based Collection Centres across Ontario. At each Centre, OTB provides a Principal Investigator with operating funds and establishes contractual obligations for funded staff to execute a common set of standard operating procedures. Each Collection Centre has a Local Management Committee, a clinical research coordinator, and a pathologists' assistant.

OICR was established as a prescribed person under the *Personal Health Information Protection Act, 2004* (PHIPA or the "Act") for its activities associated with OTB. As a Prescribed Person, OICR in respect of OTB, has particular rights and obligations under the Act to collect, use, and disclose PHI for the purposes of compiling and maintaining a registry for the storage of donated tissues.

Data collected by OTB Collection Centre staff includes sample data (e.g., sample details) and clinical data (e.g., demographics, diagnosis, stage, treatments, patient history, outcome details). Data is stored and

managed in an application called TissueMetrix 2, an integrated web application with a central database located at OICR's premises in Toronto.

Ontario Tumour Bank highlights:

- Ontario-wide biorepository and data bank, collecting blood and tissue samples;
- Four academic teaching hospitals participate as Collection Centres:
    - Kingston General Hospital,
    - London Health Sciences Centre,
    - St. Joseph's Healthcare Hamilton, and,
    - The Ottawa Hospital;
- Dedicated staff at each Collection Centre collect samples and clinical data from participating consented donors;
- Stringent procedures and ethical guidelines;
- Samples consented for a wide range of uses, including the development of commercial products;
- OTB makes no claims to intellectual property developed by the recipient of the material; and
- Is a resource for academic and industry researchers: OTB dispenses samples and discloses de-identified data to qualified recipients under a Material Transfer Agreement.

Definitions

Acronym	Definition
AIM	Artificial Intelligence in Medicine
BCP	Business Continuity Plan – Ontario Tumour Bank
DSA	Data Sharing Agreement
KGH	Kingston General Hospital
IGC	Information Governance Committee
IPC	Information and Privacy Commissioner/Ontario
ISO	Information Security Officer
LHSC	London Health Sciences Centre
MARC	Material Access Review Committee
MTA	Material Transfer Agreement
OICR	Ontario Institute for Cancer Research

OTB	Ontario Tumour Bank
PIA	Privacy Impact Assessment
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
PO	Privacy Officer
SJHH	St. Joseph's Healthcare Hamilton
SOP	Standard Operating Procedure
TOH	The Ottawa Hospital
VPN	Virtual Privacy Network

PART 1 – PRIVACY DOCUMENTATION

1. Privacy Policy in Respect of OTB's Status as a Prescribed Person

OTB has comprehensive privacy practices and procedures in place in relation to the personal health information it receives and uses with respect to its status as a prescribed person under section 39(1)(c) of *Ontario's Personal Health Information Protection Act, 2004*. The privacy practices and procedures are articulated in two overarching documents, the *Ontario Tumour Bank Privacy Policy* and OICR's *IT Information Security Program Overview* (collectively, the "Privacy Policy"), which address the matters outlined below.

Status under the Act

OICR, in respect of OTB, is a prescribed person under the Act and its regulation and has all the duties and responsibilities that arise as a result of this designation. OTB has implemented policies, procedures and practices to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. These policies, procedures, and practices are subject to review by the Information and Privacy Commissioner/Ontario (IPC) every three years.

OTB's policies and procedures support its commitment to comply with the provisions of the Act and its regulation. Furthermore, the Privacy Policy implemented by OTB evidences a commitment by OTB to exercise its mandate in support of a province-wide biorepository and data bank focused on collection of tumour-related human biospecimens.

In this way, OICR ensures OTB will comply with the provisions of the Act and its regulation applicable to prescribed persons.

Privacy and Security Accountability Framework

The Privacy Policy establishes that the President and Scientific Director of OICR is accountable for OTB's compliance with the applicable privacy legislation and regulations and for ensuring compliance with the privacy and security policies, procedures, and practices implemented. The President and Scientific Director has delegated this accountability to the Vice-President, Corporate Services & Chief Financial Officer, who is responsible for ensuring that OICR, in respect of OTB, meets current legal requirements and adheres to the principles of privacy, confidentiality and security.

The Privacy Officer and Information Security Officer have been delegated day-to-day authority to manage the privacy and information security program. A matrix reporting structure is in place for both of these positions to report to the Vice-President, Corporate Services & Chief Financial Officer for this purpose (see organizational chart in Part 4, Section 1 "Privacy Governance and Accountability Framework"). Other positions and committees that support the privacy and security programs include the Privacy Leads and the Information Governance Committee (IGC). The duties and responsibilities of these positions along with the key activities of the privacy and security programs are described in the *OICR Privacy and Information Security Accountability Terms of Reference*.

Collection of Personal Health Information

The Privacy Policy describes the purpose for which OTB collects personal health information, the type of PHI it collects, and the organizations from which it collects the information. The Privacy Policy further specifies that the collection of PHI must be consistent with the collection of PHI permitted by the Act and its regulation.

The Privacy Policy states that OTB will not collect personal health information if other information will serve the purpose. The Privacy Policy also states that OTB only collects PHI for its stated purpose and that it collects the minimum amount of PHI required to fulfill its stated purpose. OTB's privacy & security policies and procedures ensure that both the amount and the type of PHI collected is limited to that which is reasonably necessary for its stated purpose.

OTB's Privacy Policy includes the requirement to maintain a list of its data holdings of personal health information and identifies the Privacy Officer as the contact for obtaining further information in relation to the purposes, data elements, and data sources of each data holding.

Use of Personal Health Information

The Privacy Policy also describes the purpose for which OTB uses PHI and includes policies and procedures that distinguish between the use of PHI under section 39(1)(c) of the Act and the use of de-identified and/or aggregate information. The Privacy Policy also states that OTB does not use PHI for research purposes. As such, OTB does not disclose personal health information to researchers. The Privacy Policy further specifies that any use of PHI must be consistent with the uses of PHI permitted by the Act and its regulation.

The Privacy Policy states that OTB will not use PHI if other information will serve the purpose and that it will not use more PHI than is reasonably necessary to meet the purpose. Policies, procedures, and practices have been implemented in this regard to establish limits on the use of PHI. These policies are

outlined in the OTB Privacy Policy within Principle 2 (Identifying Purposes) and within Principle 4 (Limiting Collection).

In addition, the Privacy Policy also states that that OTB remains responsible for PHI used by its agents and identifies the policies procedures and practices implemented to ensure that its agents only collect, use, disclose, retain and dispose of personal health information in compliance with the Act and its regulation and in compliance with the privacy and security policies, procedures and practices implemented.

Disclosure of Personal Health Information

The Privacy Policy identifies the purposes for which PHI is disclosed, the organizations to whom information is disclosed and the requirements that must be satisfied prior to such disclosures. OTB ensures that each disclosure is consistent with the disclosures of PHI permitted by the Act and its regulation.

The Privacy Policy distinguishes between the purpose for which and the circumstances in which PHI is disclosed and the purposes for which and the circumstances in which de-identified and/or aggregate information is disclosed. It further indicates that OTB will review all de-identified and/or aggregate information prior to its disclosure in order to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.

The Privacy Policy also articulates a commitment by OTB not to disclose PHI if other information will serve the purpose and not to disclose more PHI than is reasonably necessary to meet the purpose. Specifically, the Privacy Policy sets out, in principles 4 (Limiting Collection) and 5 (Limiting Use, Disclosure, and Retention), clear rules for limiting collection, use, and disclosure of personal health information and the statutory requirements that must be satisfied prior to disclosure. Further, personal health information in the custody or control of OTB is only disclosed as is permitted or required by law, including the Act and its regulation.

Secure Retention, Transfer and Disposal of Records of Personal Health Information

The Privacy Policy addresses the secure retention of records of PHI in both paper and electronic format, including how long records of PHI are retained, whether the records are retained in identifiable form and the secure manner in which they are retained. It also addresses the manner in which records of PHI in both electronic and paper format is securely transferred and disposed of.

Implementation of Administrative, Technical and Physical Safeguards

The Privacy Policy also describes the security measures that OTB has in place to safeguard PHI and protect the privacy of individuals to whom the information pertains. The policies and procedures cover administrative, physical, and technical security controls implemented to protect PHI from unauthorized access, copying, modification, use, disclosure, theft, loss, and improper disposal. The safeguards in place include:

- Physical measures: e.g., locked facility with tracked card access, locked filing cabinets, restricted access to offices, internal/external video monitoring of OICR server rooms.
- Organizational measures: e.g., employee confidentiality agreements (with the potential for immediate dismissal where applicable), limiting access on a "need-to-use" basis, staff training to ensure awareness of the importance of maintaining the confidentiality of personal health information.
- Technological measures: e.g., the use of firewalls, Virtual Privacy Networks (VPN), separation of networks, passwords, encryption, audit logs, data modification logs, backup and recovery systems.

Inquiries, Concerns or Complaints Related to Information Practices

The Privacy Policy identifies the Privacy Officer of OICR as the contact to whom individuals may direct inquiries, concerns, or complaints related to the privacy policies, procedures, and practices of OTB and questions related to OTB's compliance with the Act and its regulation. The Privacy Policy specifies that contact information, including the name and/or title and mailing address for the Privacy Officer will be provided on OTB's website and that information on how to make privacy inquiries, challenges and complaints will be made available to the public for lodging inquiries or complaints.

The Privacy Policy also states that individuals may direct complaints regarding OTB's compliance with the Act and its regulation to the IPC and that OTB provides the mailing address and contact information for the IPC.

Transparency of Practices in Respect of Personal Health Information

The Privacy Policy commits OTB to be transparent regarding its practices in respect of handling personal health information. In this regard, the Privacy Policy requires that frequently asked questions (FAQs), and other relevant documents be freely available to the public on its website.

2. Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices

OTB has in place the *Administration of Standard Operating Procedures* that governs how it manages OTB SOPs. In addition OICR has a *Development and Management of Policies, Procedures and Guidelines* which governs the regular review of OTB's privacy policies, procedures and practices. The policy states that OICR shall review its privacy program at minimum on an annual basis, or more frequently should there be changes in technology, best practices and the Act and its regulation. The policy further states that a review of relevant policies and procedures shall be taken following a breach of privacy or security to determine if modifications to the policies and procedures are necessary to avert a similar breach in the future.

The policy states that it is the responsibility of the Privacy Officer and Information Security Officer to initiate a review process, that a committee shall be organized to carry out the review and that in the event that proposed changes represent a material change to daily operations these changes shall be communicated via education and training to all affected OICR individuals.

In undertaking the review and determining whether amendments and/or new privacy policies, procedures, and practices are necessary, OICR's *Development and Management of Policies, Procedures and Guidelines* indicates that updates or changes to OTB's privacy and information security related documents will take into consideration:

- Any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation;
- Evolving industry privacy and security standards and best practices;
- Technological advancements;
- Amendments to the Act and its regulation relevant to OICR; and
- Recommendations arising from privacy and information security audits, privacy impact assessments and investigations into privacy complaints, and privacy and information security breaches.

The review process also addresses whether the existing privacy policies and procedures continue to be consistent with actual practices and whether there is consistency between and among the privacy and security policies, procedures and practices implemented.

This policy further states that the policy sponsors are responsible for communicating the amended or newly developed privacy policies, procedures, and practices. For staff, the sponsors are guided by OICR's *Training and Development Framework* which clearly stipulates that the sponsors will be responsible for communicating any amended or newly developed privacy policies, procedures, and practices.

The Privacy Policy also ensures that all documents available to the public and other stakeholders are current and continue to be made available to the public and other stakeholders on the OTB website.

Compliance with the policies and procedures is mandatory for all agents of OTB and is monitored by OICR's Privacy Officer. The Privacy Policy specifies that a contravention of the policies and procedures constitutes a breach and includes policies and procedures for corrective actions to be taken in the event of non-compliance.

OICR's *Policy and Procedures in Respect of a Security and a Privacy Audit* is intended to assess compliance with OTB policies and to demonstrate OTB's privacy protection commitment to data providers, the public, and data users.

The Privacy Policy states that OICR's Privacy Officer, in collaboration with the OTB Director, will conduct a privacy audit every two years.

3. Policy on the Transparency of Privacy Policies, Procedures and Practices

OTB's Privacy Policy indicates that it is committed to openness relating to the privacy policies and procedures relating to the management of PHI. This information is made available upon request, in written format, and where applicable, is posted on its website. The information available on the OTB website includes the following:

- OTB's Privacy Policy;

- Brochures or frequently asked questions related to the privacy policies, procedures and practices implemented by OTB;
- Documentation related to the review by the Information and Privacy Commissioner of Ontario of the policies, procedures and practices implemented by OTB to protect the privacy of individuals whose personal health Information is received and to maintain the confidentiality of that information;
- A list of the data holdings of personal health information maintained by OTB; and
- The title, mailing address and contact information of the agent to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the Act and its regulation may be directed.

In particular, the website content describes the status of OTB under the Act, the duties and responsibilities arising from this status and the privacy policies, procedures and practices implemented in respect of personal health information, including:

- The types of personal health information collected and the persons or organizations from which this personal health information is typically collected;
- The purposes for which personal health information is collected;
- The purposes for which personal health information is used, and if identifiable information is not routinely used, the nature of the information that is used; and
- The circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to which it is typically disclosed.

The website content also identifies some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

4. Policy and Procedures for the Collection of Personal Health Information

OTB has policies and procedures, including its Privacy Policy, that identify the purposes for which personal health information is collected, the nature of the PHI that is collected, the health information custodians from whom the personal health information is collected and the secure manner in which personal health information is collected.

The policies and procedures articulate a commitment by OTB not to collect PHI unless the collection is permitted by the Act and its regulation, not to collect PHI if other information will serve the purpose and not to collect more PHI than is reasonably necessary to meet the purpose.

Personal health information is collected on an on-going basis from Collection Centres. OTB requires its agents at Collection Centres to comply with its policies and procedures by executing a Confidentiality Agreement. OTB also has a legally binding agreement with AIM Inc. for the on-going operations and

support of the TissueMetrix 2 system that requires AIM Inc., as its agent, to implement and comply with OTB's privacy and security policies and procedures.

OTB requires agents to comply with its policy and procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

Review and Approval Process

The *Policy and Procedures for the Collection of Personal Health Information – Ontario Tumour Bank* state that the Privacy Officer is responsible for reviewing and determining whether to approve the collection of personal health information and the process that must be followed and the requirements that must be satisfied in this regard.

The policy and procedures set out the criteria that must be considered for determining whether to approve the collection of personal health information. The criteria require that the collection is permitted under the Act and its regulation and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied. The criteria also require determining whether other information, such as de-identified and/or aggregate information, will serve the identified purpose such that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

The policy and procedures also sets out the manner in which the decision approving or denying the collection of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated. The Privacy Policy states that de-identified data is disclosed to academic and industry-based researchers who have a valid research ethics board approval for their research study and only if their application is approved by the OTB and the OTB's Material Access Review Committee (MARC). Researchers must also sign a Material Transfer Agreement which includes provisions to ensure that the researcher will maintain the confidentiality of the data and will not attempt to identify donors.

Conditions or Restrictions on the Approval

The policy and procedures state that no PHI shall be collected in the absence of a legally binding Data Sharing Agreement (DSA) between OTB and the requestor of the information, and that all DSAs shall have regard to the requirements of the Act and its regulation. Furthermore, the policies require that each data holding be documented with a statement of purpose, a statement of permitted use and a statement of retention. It is the responsibility of the OTB Director to ensure that these conditions have been met prior to the collection of PHI.

Secure Retention

OTB's Privacy Policy requires that records of personal health information are retained in a secure manner and includes policies and procedures addressing and restricting the secure storage of personal health information on paper records, portable media, mobile devices, email, and computer file/database systems. The PHI collected by OTB is stored in the TissueMetrix2 database system housed within a secured data-centre at OICR with restricted access in accordance with the policies and procedures for the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

Secure Transfer

OTB's Privacy Policy requires that records of personal health information are transferred in a secure manner and includes policies and procedures addressing and restricting the secure transfer of personal health information using paper records, portable media, mobile devices, email and computer file/database systems. The day-to-day collection of PHI from Collection Centres is accomplished by secure encrypted electronic transfer that does not involve human intervention in accordance with the policies and procedures for the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

Secure Return or Disposal

The policy and procedures for the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* identify the Privacy Officer of OICR as being responsible for ensuring that records of personal health information that have been collected are either securely returned or securely destroyed upon expiry of the retention period as documented in the statement of retention for the PHI in question. In general, the PHI in TissueMetrix2 is retained in perpetuity.

The Privacy Policy states that records of personal health information that are to be returned to the organization from which they were collected must be returned in a secure manner in accordance with the policies and procedures for the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

The Privacy Policy states that records of personal health information that are to be destroyed at the expiry of the retention period must be destroyed in accordance with the policies and procedures for the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

5. List of Data Holdings Containing Personal Health Information

OICR, in respect of OTB, retains an up-to-date list and summary description of the data holdings of personal health information maintained by OTB.

6. Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information

OICR has a *Policies and Procedures for Statements of Purpose for Data Holdings Containing Personal*

Health Information which governs the creation, review, amendment and approval of statements of purpose for data holdings containing personal health information. The policy and procedures require the statements of purpose to describe the purpose of the data holding, the personal health information contained in the data holding, the sources of the personal health information and the need for the PHI in relation to the identified purpose.

The policy and procedures specify that the Privacy Officer is responsible for maintaining up-to-date statements of purpose and describe the process to be followed in completing the statements of purpose for the data holdings containing personal health information. The policy and procedures require that the sources of the data holdings be consulted in completing the statements of purpose and specify that the Privacy officer is responsible for approving the statements of purpose.

The policy and procedures state that statements of purpose are made available to the health information custodians from whom personal health information is collected—in particular, the Collection Centre that provide test results to TissueMetrix2.

The policy and procedures require that the statements of purpose be reviewed on an on-going basis, and at minimum, on an annual basis to ensure their continued accuracy and in order to ensure that the personal health information collected for purposes of the data holding is still necessary for the identified purposes.

The policies and procedures specify that the Privacy Officer is responsible for the annual review of the statements of purpose and the process to be followed in reviewing the statements of purpose and in amending the statements of purpose. The policy and procedures require that the sources of the data holdings be consulted when amending the statements of purpose and specify that the Privacy Officer is responsible for approving amended statements of purpose. The policy and procedures state that amended statements of purpose are to be made available to the Collection Centres from whom PHI is collected.

OTB requires its agents to comply with the policy and procedures. Compliance is monitored by the Privacy Officer in accordance with OICR's *Policy and Procedures in Respect of a Security and a Privacy Audit*, which addresses the consequences of breach. The policy and procedures stipulate that audits are performed every two years and more frequently as required. The Privacy Officer will assume primary responsibility for the privacy audit in collaboration with the OTB Director.

The policy and procedures require agents to provide notice at the first reasonable opportunity of a breach or potential breach of privacy, in accordance with OICR's *Policy and Procedures for Information Security and Privacy Breach Management* for identifying a breach of privacy, reporting a breach of privacy and actions to be taken following a breach of privacy.

7. Statements of Purpose for Data Holdings Containing Personal Health Information

OICR's *Policies and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information* require that a statement of purpose is documented and retained in the privacy document archives for each data holding containing personal health information, identifying the purpose of the

data holding, the PHI contained in the data holding, the sources of the PHI and the need for the PHI in relation to the identified purpose.

8. Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information

OTB has policies and procedures in place to limit access to and use of personal health information by its agents. The *Policy and Procedures for Data Access and Use – Ontario Tumour Bank* prescribe that access and use of personal health information is limited to select individuals on the basis of the "need to know" principle. The purpose of this policy and its procedures is to ensure that agents of OTB access and use both the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities.

The *Policy and Procedures For Data Access and Use – Ontario Tumour Bank*, identify the limited and narrowly defined purposes for which, and circumstances in which, agents are permitted to access and use personal health information and the levels of access to PHI that may be granted. OTB ensures that the duties of agents with access to PHI are segregated in order to avoid a concentration of privileges that would enable a single agent to compromise PHI.

As stated earlier, TissueMetrix2 is an application that facilitates the collection of PHI from donors at participating Collection Centres. Only a few individuals are granted access to the application, specifically two staff per Collection Centre have access to data subjects at their respective institutions. In addition, four OTB staff at OICR have access, but only one has access to PHI while the others may view only de-identified data.

For all other purposes and in all other circumstances, The *Policy and Procedures For Data Access and Use – Ontario Tumour Bank* require agents to access and use de-identified and/or aggregate information in accordance with OICR's policies and procedures regarding the de-identification of personal health information and limits on the aggregation of data. These policies and procedures explicitly prohibit access to and use of PHI if other information, such as de-identified and/or aggregate information, will serve the identified purpose and prohibit access to or use of more PHI than is reasonably necessary to meet the identified purpose.

The policies and procedures also prohibit agents from using de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

Review and Approval Process

The OTB Senior Analyst is responsible for administering requests for access to OTB data and maintaining related documentation such as the OTB Data Access Form and the OTB Data Access Log. An OTB Data Access Form is completed for each user requesting access to OTB record-level data. Section 1 of this form is completed by the OTB Senior Analyst and describes the need for access, level of access required, and period of access.

The maximum period for access will be one year with an automatic expiry after one year from the date approval is granted. For OTB users that require ongoing use of OTB data, the Senior Analyst is again required to request approval for users to access OTB data in accordance with this policy and its procedures.

The following criteria must be met in order for a new request for access or renewal to be approved:

- The user must have signed a Confidentiality Agreement with OICR;
- The user must have completed (initial or ongoing) privacy and information security training provided by the OTB within the past 12 months;
- The requested access and use must be permitted by the Act and its regulation;
- The user requires access to record-level OTB data to perform their employment obligations;
- The least amount of, and least identifiable form of, record-level OTB data will be accessed and used; and
- If access to PHI is requested, that the intended purpose cannot be reasonably accomplished without PHI and that de-identified or aggregate information will not serve the intended purpose.

If the request is approved by both the OTB Director and Information Security Officer, the necessary signatures will be obtained in Section 1 of the OTB Data Access Form and the OTB Data Access Log will be updated by the OTB Senior Analyst. A copy of the form will be retained within OTB files and the requestor will be informed of the decision.

If the request is denied, the reason will be noted on the form, and the OTB Director will inform the requestor in writing. The OTB Director will work with OICR's IT department and the OTB Senior Analyst to install the required applications and set up the required accounts, using Section 2 the OTB Data Access Form.

Conditions or Restrictions on the Approval

As stated above, all access to OTB data must be approved by the OTB Director and OICR Information Security Officer (including access for the OTB Director which must also be approved by the Program Director and Information Security Officer). OTB agents will be granted access to OTB data under the following conditions:

- User has entered into a confidentiality agreement with the OICR;
- User has completed (initial or ongoing) privacy and information security training within the past 12 months;
- Access to data is on a "need to know" basis for the performance of assigned duties only;
- User will not be granted access to, or use PHI, if other information, such as de-identified and/or aggregate information, will serve the purpose;
- User must not be granted access to or use more PHI than is reasonably necessary to meet the identified purpose;

- Remote access to PHI is prohibited if other information, such as de-identified and/or aggregate information, will serve the purpose and from remotely accessing more PHI than is reasonably necessary for the identified purpose;
- OICR strictly forbids the use of OTB data for anything other than the identified purpose for which the data was provided;
- User is responsible for understanding and carrying out their duties in compliance with OTB policies, including this policy, the Ontario Tumour Bank Privacy Policy, the confidentiality agreements signed by them, as well as all applicable privacy legislation;
- An OTB Data Access Form must be completed, including all required approvals, prior to an OTB Agent being granted access to OTB data;
- User is prohibited from using de-identified or aggregate information, alone or in combination with other information, including prior knowledge, to identify an individual;
- User must not create temporary or permanent data linkages (i.e., new data holdings) unless compliant with *Policy and Procedures for Data Linkages - Ontario Tumour Bank*;
- User must ensure that all disclosures of OTB data are in accordance with *Policy and Procedures for Data Disclosure – Ontario Tumour Bank, TB312 Material and Data Request and Release* and the Act; and
- User accessing OTB data will securely retain, transfer and dispose of PHI and de-identified record-level data in accordance with related OICR policies: *Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information, Clean Desk, Sending/Receiving Personal Health Information, Personal Information and Confidential/Sensitive Information and OICR Policy Statements 3.0 Encryption, 4.0 Secure Electronic Data Retention, Backup, Disposal and Destruction, 5.0 Data Protection (Encryption, Transmission and Storage), 22.0 Remote Access* and *28.0 Mobile Devices Security*.

Notification and Termination of Access and Use

Access to OTB data must be terminated as of the effective date when an agent is no longer employed with OICR, transfers to another program within OICR, starts a leave of absence or for any other reason no longer requires access to the OTB data. All accounts and applications (as per the OTB Data Access Form) must be deactivated as required. OICR's *Termination Policy* provides additional details on the procedure and documentation requirements for termination of access.

The policy states that an agent granted approval to access and use personal health information must notify OTB when the agent is no longer employed or retained by OTB or no longer requires access to or use of the PHI.

The policy also outlines the notification process that must be followed. In particular, the policy and procedures identify that the OTB Director and the Information Security Officer must be notified; the time frame within which this notification must be provided; the format of the notification; the documentation that must be completed, provided and/or executed, if any; the agent who is responsible for completing, providing and/or executing the documentation; the agent to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also identify the agents responsible for terminating access to and use of the PHI, the procedure to be followed in terminating access to and use of the PHI, and the time frame within which access to and use of the PHI must be terminated.

Secure Retention

OICR's policy and procedures require that agents of OTB granted approval to access and use personal health information to securely retain the records of PHI in compliance with OICR's *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

Secure Disposal

OICR's policy and procedures require that agents of OTB granted approval to access and use personal health information to securely dispose of the records of personal health information in compliance with OICR's *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

Tracking Approved Access to and Use of Personal Health Information

OICR, in respect of OTB, ensures that a log is maintained of agents granted approval to access and use personal health information and identifies the OTB Senior Analyst as the agent responsible for maintaining the log. The policy and procedures also state that documentation related to the receipt, review, approval, denial, or termination of access to and use of PHI is retained by the OTB, which is also responsible for retaining this documentation.

Compliance, Audit and Enforcement

OICR also requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach.

In addition to the audits described in OICR's *Logging and Auditing* policy, the scheduled audits listed below take place to review active accounts and access to the OTB Central Database. The OTB Senior Analyst will be responsible for performing each of these audits, maintaining related documentation in the IT Request Tracker system, notifying the Information Security Officer of the findings, and reporting any suspected breaches immediately as described in OICR's Policy Statement 10.0 *Information Security Incident Response*. Audits consist of the following reviews:

- Biannual review of TissueMetrix and Oracle accounts: to verify that only active OTB employees have active accounts;
- Biannual review of TissueMetrix login information: to verify that only active OTB employees have logged into TissueMetrix, and to investigate anything unusual. The OTB Senior Analyst will produce a report from the TissueMetrix production database detailing login information (i.e., username, login date/time and logout date/time);
- Biannual review of Oracle login information: to verify that only active OTB employees have logged into the database via other applications (e.g., Crystal Reports), to review System account login attempts (AIM remote access), and to investigate anything unusual; and

- Biannual review of other accounts listed in the OTB Data Access Form (e.g., SharePoint and contact management system), to ensure that only active OTB employees have access to other OTB files.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

9. Log of Agents Granted Approval to Access and Use Personal Health Information

OICR, in respect of OTB, maintains a log of agents granted approval to access and use personal health information. The log includes the name of the agent granted approval to access and use personal health information; the data holdings of personal health information to which the agent has been granted approval to access and use; the level or type of access and use granted; the date that access and use was granted; and the termination date or the date of the next audit of access to and use of the personal health information.

10. Policy and Procedures for the Use of Personal Health Information for Research

OTB does not perform research and therefore does not use, disclose or retain PHI or de-identified data for its own research purposes. The use, disclosure and retention of data that is collected by OTB is for the stated purpose, which is to maintain a high quality registry of patient-donated biospecimens and accompanying clinical data for the facilitation of cancer research without the use of identifiable information.

As stated earlier, OTB has a commitment not to use or to disclose PHI if other information will serve the purpose and not to use or disclose more PHI than is reasonably necessary to meet the research purpose.

OTB remains responsible for PHI used by its agents. *Policy and Procedures for Data Access and Use - Ontario Tumour Bank* ensures that OTB agents only access and use PHI in compliance with the Act and its regulation and in compliance with the privacy and security policies, procedures and practices implemented.

OTB discloses de-identified clinical data to researchers for the purposes of research but does not permit PHI (i.e., identifying information) to be disclosed for research under any circumstances. All disclosed data sets must be reviewed and classified as de-identified or aggregate according to *Policy and Procedures for Data Disclosure – Ontario Tumour Bank* to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. This de-identified data is disclosed to academic and industry-based researchers who have a valid research ethics board approval for their research study and only if their application is approved by the Ontario Tumour Bank and the OTB's Material Access Review Committee (MARC). Researchers must also sign a Material Transfer Agreement which includes provisions to ensure that the researcher will maintain the confidentiality of the data and will not attempt to identify donors.

All disclosures will be in accordance with *Policy and Procedures for Data Disclosure - Ontario Tumour Bank*. The above-mentioned policies, procedures and practices have been implemented by OTB to ensure that both the amount and the type of PHI used and disclosed is limited to that which is reasonably necessary for its purpose.

All OTB agents that access and use OTB data must be compliant with OTB policy and its procedures. Compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit* and OICR Policy Statement 37.0 *Logging and Auditing*. The Privacy Officer and Information Security Officer will be responsible for conducting such audits every two years and ensuring compliance with the policies and its procedures. Issues of non-compliance will be dealt with on an individual basis by the appropriate authority within OICR. Additional details may be found in OICR's *Progressive Discipline Policy*. OICR agents must also notify the PO and the ISO at the first reasonable opportunity, in accordance with OICR's *Policy and Procedures for Information Security and Privacy Breach Management* and/or Policy Statement 10.0 *Information Security Incident Response*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

Where the Use of Personal Health Information is Permitted for Research

OTB does not permit personal health information to be used for research purposes.

Distinction between the Use of Personal Health Information for Research and Other Purposes

OTB is permitted to use PHI for the purposes set out in s.39(1)(c) of the Act.

Review and Approval Process

OTB does not permit personal health information to be used for research purposes.

Conditions or Restrictions on the Approval

OTB does not permit personal health information to be used for research purposes.

Secure Retention

OTB does not permit personal health information to be used for research purposes.

Secure Return or Disposal

OTB does not permit personal health information to be used for research purposes.

Tracking Approved Uses of Personal Health Information for Research

OTB does not permit personal health information to be used for research purposes.

Where the Use of Personal Health Information is not Permitted for Research

OTB does not permit personal health information to be used for research purposes, as such, the policy and procedures expressly prohibit the use of PHI for research purposes and indicate that only de-identified and/or aggregate information may be used for research purposes.

Review and Approval Process

OTB does not permit personal health information to be used for research purposes.

Conditions or Restrictions on the Approval: OTB does not permit personal health information to be used for research purposes.

11. Log of Approved Uses of Personal Health Information for Research

OTB does not permit personal health information to be used for research purposes therefore OTB does not maintain such a log.

12. Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research

The *Policy and Procedures for Data Disclosure – Ontario Tumour Bank*, identify when and under what circumstances personal health information is permitted to be disclosed for purposes other than research.

The policy and procedures articulate a commitment by OTB not to disclose personal health information if other information will serve the same purpose and not to disclose more PHI than is reasonably necessary to meet the purpose.

OTB requires agents to comply with its Privacy Policy and also requires that OICR's Privacy Officer to enforce compliance and to address the consequences of any breaches that may occur. The OICR *Policy and Procedures in Respect of a Security and a Privacy Audit*, stipulate that compliance will be audited and sets out the frequency with which the policy and procedures will be audited and identify the Privacy Officer as responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

This policy also requires agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management* if an agent breaches or believes there may have been a breach of this policy or its procedures.

Where the Disclosure of Personal Health Information is Permitted

The *Policy and Procedures for Data Disclosure – Ontario Tumour Bank*, permit personal health information to be disclosed for purposes other than research and sets out the circumstances in which the disclosure of PHI is permitted. They further require that all disclosures of personal health information comply with the Act and its regulation.

Review and Approval Process

The requestor must submit a Request for Data in writing to the OTB Director. The request must include the following:

- Type(s) of data required;
- Reason(s) that the data is required;
- Intended use(s) of the data; and
- Length of time data will be used.

The Request for Data will be reviewed by the Privacy Officer and Information Security Officer, in consultation with the Information Governance Committee (IGC). *OICR Privacy and Information Security Accountability Terms of Reference* provides details on the responsibilities of the IGC. In determining whether to approve the request for disclosure, the following criteria must be satisfied:

- The disclosure is permitted by the Act and its regulation and all conditions or restrictions set out have been satisfied;
- PHI is required, and other information, namely de-identified or aggregate data, will not serve the purpose;
- No more PHI is being requested than is reasonably necessary to meet the purpose; and
- The recipient has in place adequate privacy and security policies and procedures.

The decision to approve or to deny the request for disclosure, along with the reasons for the decision, should be documented in writing and signed by the OTB Director, PO and ISO. The OTB Director will communicate the decision to the requestor in writing.

Conditions or Restrictions on the Approval

Prior to any disclosure of PHI, a Data Sharing Agreement must be executed, in accordance with OICR's policy on the *Execution of Data Sharing Agreements*. All PHI must be securely transferred according to the requirements described in the DSA and as per OICR's policies for *Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information, Sending/Receiving Personal Health Information, Personal Information and Confidential/Sensitive Information* and OICR *Policy Statements 3.0 Encryption and 5.0 Data Protection* (Encryption, Transmission and Storage).

The OTB Director is responsible for ensuring that the requirements of the DSA are satisfied as described in OICR's policy on the *Execution of Data Sharing Agreements*. This includes ensuring that the PHI is either securely returned or securely destroyed at the end of the retention period or date of termination of the DSA. If the PHI is not securely returned or securely destroyed within 5 business days following the retention period or date of termination described in the DSA, the OTB Director is responsible for alerting the PO and/or ISO immediately and the incident will be reported and handled as a privacy breach per OICR's *Policy and Procedures for Information Security and Privacy Breach Management*.

The OTB Director is responsible for receiving and maintaining the following documentation in OICR's SharePoint system:

- Request for Data (i.e., PHI);
- Decision to approve or deny the request (including rationale);
- Data Sharing Agreement; and
- Certificate of Destruction (if applicable), or confirmation that the data has been returned to OICR.

Secure Transfer

All PHI must be securely transferred according to the requirements described in the DSA and per OICR's policies for *Retention, Transfer and Disposal of Records Containing Personal Information and Personal*

Health Information, Sending/Receiving Personal Health Information, Personal Information and Confidential/Sensitive Information and OICR *Policy Statements 3.0 Encryption and 5.0 Data Protection* (Encryption, Transmission and Storage).

Secure Return or Disposal

All disclosures of OTB data (i.e., data that includes PHI) must comply with OICR's policy and procedures for *Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information* and *Policy and Procedures for Data Disclosure – Ontario Tumour Bank*. These policies and procedures identify the OTB Director as responsible for ensuring that records of personal health information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement.

These policies and procedures further address the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received within a reasonable period of time following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement. These include the agent responsible for implementing this process and the stipulated time frame following the retention period or the date of termination within which this process must be implemented.

Documentation Related to Approved Disclosures of Personal Health Information

All disclosures of OTB data must be compliant with *the Policy and Procedures for Data Disclosure – Ontario Tumour Bank*. Compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*. The Privacy Officer will be responsible for conducting such audits every 2 years and ensuring compliance with the policies and its procedures. Issues of non-compliance will be dealt with on an individual basis by the appropriate authority within OICR. For additional details refer to OICR's *Progressive Discipline Policy*. OICR agents must also notify the PO at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

Where the Disclosure of Personal Health Information is not Permitted

This section does not apply to OTB.

13. Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements

The OTB Privacy Policy states that personal health information in the custody of OTB shall not be disclosed or used to conduct research or support research on individuals or groups of individuals. As such, OTB does not accept requests from researchers or research organizations to access and use PHI for research purposes and does not have policies and procedures in place to manage such requests or execute such requests.

14. Template Research Agreement

The OTB Privacy Policy states that personal health information in the custody of OTB shall not be disclosed or used to conduct research or support research on individuals or groups of individuals. As such, OTB does not maintain template research agreements.

15. Log of Research Agreements

The OTB Privacy Policy states that personal health information in the custody of OTB shall not be disclosed or used to conduct research or support research on individuals or groups of individuals. As such, OTB does not maintain a log of research agreements.

16. Policy and Procedures for the Execution of Data Sharing Agreements

The *Execution of Data Sharing Agreements* policy and procedures require the execution of a Data Sharing Agreement (DSA) and set out the process that must be followed and the requirements that must be satisfied prior to the execution of a Data Sharing Agreement.

The policy and procedures also set out the circumstances requiring the execution of a DSA prior to the collection of personal health information for purposes other than research and requires the execution of a DSA prior to any disclosure of personal health information for purposes other than research.

The policy and procedures further identify the agent(s) responsible for ensuring that a DSA is executed, as well as the process that must be followed and the requirements that must be satisfied in this regard. This includes a discussion of the documentation that must be completed, provided and/or executed; the agents responsible for completing, providing and/or executing the documentation; the agents to whom the documentation must be provided; and the required content of the documentation.

In relation to the disclosure of personal health information for purposes other than research, the agents responsible for ensuring that a DSA is executed must be satisfied that the disclosure was approved in accordance with the *Policy and Procedures for Data Disclosure – Ontario Tumour Bank*. In relation to the collection of personal health information for purposes other than research, the agents responsible for ensuring that a DSA is executed must be satisfied that the collection was approved in accordance with the *Policy and Procedures for the Collection of Personal Health Information – Ontario Tumour Bank*.

The policy and procedures also require that a log of Data Sharing Agreements be maintained and identify the agents responsible for maintaining such a log. In addition, the policy and procedures address where documentation related to the execution of Data Sharing Agreements will be retained and the agents responsible for retention.

OTB also requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, and set out the frequency with which the policy and procedures will be audited and identify the Privacy Officer and Information Security Officer as responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

17. Template Data Sharing Agreement

For the disclosure of data containing PHI, OTB ensures that a Data Sharing Agreement is executed in the circumstances set out in its policy and procedures for *Execution of Data Sharing Agreements*. OTB's policies and procedures require that a Data Sharing Agreement Template be kept on file and that all Data Sharing Agreements address the following areas set out below. For the disclosure of de-identified data, a Material Transfer Agreement (MTA) is executed as set out in its Material and Data Request and Release.

General Provisions

The Data Sharing Agreement Template describes the status of OTB under the Act and the duties and responsibilities arising from this status. It also specifies the precise nature of the personal health information subject to the DSA and provides a definition of personal health information that is consistent with the Act and its regulation.

The DSA also identifies the person or organization that is collecting personal health information and the person or organization that is disclosing personal health information pursuant to the DSA.

Purposes of Collection, Use and Disclosure

OICR's Data Sharing Agreement Template identifies the purposes for which the personal health information subject to the DSA is being collected and for which the personal health information will be used. The DSA explicitly states whether or not the personal health information collected pursuant to the DSA will be linked to other information, and if so, the DSA identifies the nature of the information to which the personal health information will be linked, the source of the information to which the personal health information will be linked, how the linkage will be conducted and why the linkage is required for the identified purposes.

The DSA template includes an acknowledgement that the personal health information collected pursuant to the DSA is necessary for the purpose for which it was collected and that other information, namely de-identified and/or aggregate information, will not serve the purpose and that no more personal health information is being collected and will be used than is reasonably necessary to meet the purpose.

The Data Sharing Agreement Template also identifies the purposes for which the personal health information subject to the Data Sharing Agreement may be disclosed and any limitations, conditions or restrictions imposed thereon.

The Data Sharing Agreement Template requires the collection, use and disclosure of personal health information subject to the DSA to comply with the Act and its regulation and sets out the specific statutory authority for each collection, use and disclosure contemplated in the DSA.

Secure Transfer

OICR's Data Sharing Agreement Template requires the secure transfer of the records of personal health information subject to the DSA. The DSA sets out the secure manner in which the records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that will be followed in ensuring that the records are transferred in a secure manner. OICR's *Sending/Receiving Personal Information, Personal Health Information and De-Identified Health Information and Policy Statement 5.0 Data Protection (Encryption, Transmission and Storag*e) prescribe acceptable methods for the secure transfer of personal health information in various formats and media.

Secure Retention

OICR's Data Sharing Agreement Template addresses the retention period of personal health information to ensure that the information is retained only for as long as required to fulfill the purpose for which personal health information is collected.

The Data Sharing Agreement Template requires that records of personal health information are stored in a secure manner consistent with OICR's *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* and *Policy Statement 4.0 Secure Electronic Data Retention, Backup, Disposal and Destruction* for the secure storage of PHI in various formats and media, which address steps to be taken to ensure that the personal health information subject to the DSA is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of PHI are protected against unauthorized copying, modification or disposal. The Data Sharing Agreement Template also identifies the precise methods by which records of PHI in paper and electronic format and records stored on other media will be securely retained. It also indicates whether records of PHI will be retained in identifiable or de-identified form.

Each instance of a Data Sharing Agreement describes the secure manner in which personal health information will be stored by the parties to the agreement and the steps to be taken to protect the information against theft, loss, unauthorized use or disclosure, copying, modification and disposal.

Secure Return or Disposal

The Data Sharing Agreement Template also addresses whether the records of personal health information subject to the DSA will be returned in a secure manner or will be disposed of in a secure manner following the retention period set out in the DSA or following the date of termination of the DSA, as the case may be.

If the records of personal health information are required to be returned in a secure manner, the Data Sharing Agreement specifies the time frame following the retention period, or the date of termination of the agreement, within which the records of personal health information must be securely returned, that the records should be returned to the OTB Director or as defined in the DSA, and the manner of secure return consistent with OICR's *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

The Data Sharing Agreement specifies the time frame following the retention period, or the date of termination of the agreement, within which the records of personal health information must be securely destroyed and a Certificate of Destruction to be sent the OICR Administrative Contact attesting to the destruction of the records. The Certificate of Destruction includes: a description of the record set that was destroyed, the date, time, location the records were destroyed, the method of secure disposal employed and the name and signature of the person attesting to the destruction of the records.

If the records of personal health information are required to be disposed of in a secure manner, the Data Sharing Agreement further describes acceptable methods of destruction, consistent with the policies and procedures for the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* in various formats and media, which are consistent with the Act and its regulation, and give regard to orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information.

Notification

OICR's Data Sharing Agreement Template requires that notification be provided at the first reasonable opportunity if the DSA has been breached or is suspected to have been breached or if the personal health information subject to the DSA is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. OICR's *Policy and Procedures for Information Security and Privacy Breach Management* require the notification to be made in writing to the Privacy Officer of OTB, and set out the steps to be taken to contain the breach.

Consequences of Breach and Monitoring Compliance

The Data Sharing Agreement Template outlines the consequences of breach of the agreement and indicates that compliance with the DSA will be audited and the manner in which compliance will be audited and the notice that will be provided of the audit per OICR's *Policy and Procedures in Respect of a Security and a Privacy Audit*. All persons who will have access to PHI under the Data Sharing Agreement will be required to sign a Terms and Conditions under Personal Health Information Acknowledgement Form (Appendix D of the Data Sharing Agreement Template) prior to being granted access to PHI. Completion of the Data Sharing Agreement Under PHI – Terms and Conditions Acknowledgement Form, indicates the person has read, understood and will abide by the terms and conditions governing the access and use of PHI as specified in the Data Sharing Agreement.

18. Log of Data Sharing Agreements

OICR, in respect of OTB, maintains a log of executed Data Sharing Agreements. The log includes the following details:

- The name of the person or organization from whom the personal health information was collected or to whom the personal health information was disclosed;

- The date that the collection or disclosure of personal health information was approved, as the case may be;
- The date that the Data Sharing Agreement was executed;
- The date the personal health information was collected or disclosed, as the case may be;
- The nature of the personal health information subject to the Data Sharing Agreement;
- The retention period for the records of personal health information set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement;
- Whether the records of personal health information will be securely returned or will be securely disposed of following the retention period set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement; and
- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date by which they must be returned or disposed of.

19. Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information

OICR's policy on *Execution of Third Party Services Agreements* requires a written agreement to be entered into with third party service providers whenever such services entail access to, or use of PHI, prior to permitting third party service providers to access and use the PHI. The policy and procedures require the written agreements to contain the relevant language from OICR's Third Party Services Agreement template.

The policies and procedures state the process that must be followed and the requirements that must be satisfied prior to the execution of such an agreement and that the Office of the Deputy Director is responsible for ensuring that a Third Party Service Agreement is executed in all cases where such services involve access to or use of PHI. This policy does not apply to third party services where access to or use of PHI is not required.

The *Policy and Procedures for Data Disclosure – Ontario Tumour Bank*, specifies that OTB shall not provide PHI to a third party service provider if other information, namely de-identified and/or aggregate information, will serve the purpose and will not provide more PHI than is reasonably necessary to meet the purpose. The decision to approve or to deny the request for disclosure, along with the reasons for the decision, should be documented in writing and signed by the OTB Director, PO and ISO.

The policy and procedures specify that the OTB Senior Analyst is responsible for ensuring that records of PHI provided to a third party service provider are either securely returned or are securely disposed of, as the case may be, following the termination of the agreement. In the event that records of personal health information are not returned or a confirmation of destruction of the records is not received within the time frame stipulated in the Third Party Services Agreement, it is the responsibility of the OTB Senior Analyst to inform the third party in writing that failure to return or destroy the records in accordance with the terms and conditions of the agreement constitutes a breach of the agreement. If the third party fails to comply after such notification, the matter is escalated to the OTB Director, and if compliance is not achieved may result in legal action.

OICR's policy requires that a log be maintained of all agreements executed with third party service providers and designates the agents responsible for maintaining the Log of Third Party Services

Agreements in OICR's Corporate Administration – centralized database, including signed copies of all executed agreements.

The terms and conditions of OTB's Third Party Services Agreements require agents to comply with OICR's privacy and security policies and procedures and designate the Privacy Officer as being responsible for monitoring, auditing and ensuring compliance. Compliance will be audited in accordance with OICR's *Policy and Procedures in Respect of a Security and a Privacy Audit*, at a frequency specified and agreed to in the Third Party Services Agreement.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if the third party breaches or believes there may have been a breach of the policy or its procedures.

20. Template Agreement for All Third Party Service Providers

A written agreement is entered into with third party service providers that will be permitted to access and use personal health information of OTB, including those that are contracted to retain, transfer or dispose of records of PHI and those that are contracted to provide services for the purpose of enabling OTB to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information ("electronic service providers"). The written agreement addresses the matters set out below.

General Provisions

The Third Party Services Agreement template describes the status of OTB under the Act and the duties and responsibilities arising from this status. The agreement also states whether or not the third party service provider is an agent of OTB in providing services pursuant to the agreement. All third party service providers that are permitted to access and use personal health information in the course of providing services to OTB are considered agents of OTB. OICR has a robust IT infrastructure, and as such, OTB does not typically engage electronic service providers.

If the third party service provider is an agent of OTB, the agreement requires the third party service provider to comply with the provisions of the Act and its regulation relating to prescribed persons and to comply with specific privacy and security policies and procedures implemented by OTB in providing services pursuant to the agreement.

The agreement provides a definition of personal health information consistent with the Act and its regulation. Where appropriate, the agreement also specifies the precise nature of the personal health information that the third party service provider will be permitted to access and use in the course of providing services pursuant to the agreement.

The agreement also sets out that the services provided by the third party service provider pursuant to the agreement be performed in a professional manner, in accordance with industry standards and practices, and by properly trained agents of the third party service provider.

Obligations with Respect to Access and Use

The agreement identifies the purposes for which the third party service provider is permitted to access and use the PHI of OTB and any limitations, conditions, or restrictions imposed thereon.

In identifying the purposes for which the third party service provider is permitted to use PHI, OTB ensures that each use identified in the agreement is consistent with the uses of personal health information permitted by the Act and its regulation. The agreement prohibits the third party service provider from using personal health information except as permitted in the agreement.

In the case of an electronic service provider that is not an agent of OTB, the agreement sets out that the electronic service provider is prohibited from using personal health information except as necessary in the course of providing services pursuant to the agreement.

Further, the agreement prohibits the third party service provider from using PHI if other information will serve the purpose and from using more PHI than is reasonably necessary to meet the purpose.

Obligations with Respect to Disclosure

The agreement identifies the purposes, if any, for which the third party service provider is permitted to disclose the personal health information of OTB and any limitations, conditions, or restrictions imposed thereon.

In identifying the purposes for which the third party service provider is permitted to disclose personal health information, OTB ensures that each disclosure identified in the agreement is consistent with the disclosures of personal health information permitted by the Act and its regulation and *Policy and Procedures for Data Disclosure – Ontario Tumour Bank*. In this regard, the agreement prohibits the third party service provider from disclosing PHI except as permitted in the agreement or as required by law, from disclosing PHI if other information will serve the purpose and from disclosing more PHI than is reasonably necessary to meet the purpose.

In the case of an electronic service provider that is not an agent of OTB, the agreement prohibits the electronic service provider from disclosing personal health information to which it has access in the course of providing services except as required by law. At the present time, OTB does not have an electronic service provider who is not an agent of OTB.

Secure Transfer

Where it is necessary to transfer records of personal health information to or from OTB, the agreement requires the third party service provider to securely transfer the records of personal health information and sets out the responsibilities of the third party service provider in this regard. In particular, the agreement specifies the secure manner in which the records will be transferred by the third party service provider, the conditions pursuant to which the records will be transferred by the third party service provider, to whom the records will be transferred, and the procedure that must be followed by the third party service provider in ensuring that the records are transferred in a secure manner.

In identifying the secure manner in which records of PHI must be transferred, the agreement references OICR's policy on *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

In addition, where the retention of records of personal health information or where the disposal of records of personal health information outside the premises of OICR is the primary service provided to OICR, the agreement requires the third party service provider to provide documentation to OICR setting out the date, time, and mode of transfer of the records of PHI and confirming receipt of the records of personal health information by the third party service provider. In these circumstances, the agreement obligates the third party service provider to maintain a detailed inventory of the records of PHI transferred.

Secure Retention

The agreement requires the third party service provider to retain the records of personal health information in a secure manner and identifies the precise methods by which records of PHI in paper and electronic format will be securely retained by the third party service provider, including records of personal health information retained on various media.

The agreement further outlines the responsibilities of the third party service provider in securely retaining the records of PHI. In identifying the secure manner in which the records of PHI will be retained, and the methods by which the records of personal health information will be securely retained, the agreement references OICR's policy on *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

The agreement also obligates the third party service provider to maintain a detailed inventory of the records of personal health information being retained on behalf of OICR as well as a method to track the records being retained.

Secure Return or Disposal Following Termination of the Agreement

The agreement addresses whether records of personal health information will be securely returned to OTB or will be disposed of in a secure manner following the termination of the agreement.

Where the records of personal health information are required to be returned in a secure manner, the agreement stipulates the time frame following the date of termination of the agreement within which the records of PHI must be securely returned, the secure manner in which the records must be returned and the agent of OTB to whom the records must be securely returned.

In identifying the secure manner in which the records of personal health information will be returned, the agreement references OICR's policy on *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*. If the records of personal health information are required to be disposed of in a secure manner, the agreement provides a definition of secure disposal that is consistent with the Act and its regulation and identifies the precise manner in which the records of personal health information are to be securely disposed of.

In identifying the secure manner in which the records of personal health information will be disposed of, the agreement ensures that the method of secure disposal identified is consistent with the Act and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information; and with the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* implemented by OTB.

The agreement also stipulates the time frame following termination of the agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided to OTB. The agreement further identifies the agent of OTB to whom the certificate of destruction must be provided and must identify the required content of the certificate of destruction. The certificate of destruction is required to identify the records of PHI securely disposed of; to stipulate the date, time and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

Secure Disposal as a Contracted Service

Where the disposal of records of personal health information is the primary service provided to OTB by the third party service provider, in addition to the requirements set out above in relation to secure disposal, the agreement further sets out the responsibilities of the third party service provider in securely disposing of the records of personal health information, including:

- The time frame within which the records are required to be securely disposed of;
- The precise method by which records in paper and/or electronic format must be securely disposed of, including records retained on various media;
- The conditions pursuant to which the records will be securely disposed of;
- The person(s) responsible for ensuring the secure disposal of the records; and
- The agreement also enables OTB, at its discretion, to witness the secure disposal of the records of personal health information subject to such reasonable terms or conditions as may be required in the circumstances.

Implementation of Safeguards

The agreement requires the third party service provider to take steps that are reasonable in the circumstances to ensure that the personal health information accessed and used in the course of providing services pursuant to the agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of PHI subject to the agreement are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be implemented by the third party service provider are detailed in the agreement.

Training of Agents of the Third Party Service Provider

The agreement requires the third party service provider to provide training to its agents on the importance of protecting the privacy of individuals whose personal health information is accessed and

used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations.

The agreement also requires the third party service provider to ensure that its agents who will have access to the records of personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the PHI. The agreement sets out the method by which this will be ensured. This includes requiring agents to sign an acknowledgement, prior to being granted access to the PHI, indicating that they are aware of and agree to comply with the terms and conditions of the agreement.

Subcontracting of the Services

In the event that the agreement permits the third party service provider to subcontract the services provided under the agreement, the third party service provider is required to acknowledge and agree that it will provide OTB with advance notice of its intention to do so, that the third party service provider will enter into a written agreement with the subcontractor on terms consistent with its obligations to OTB and that a copy of the written agreement will be provided to OTB.

Notification

The agreement requires the third party service provider to notify OICR at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if personal health information handled by the third party service provider on behalf of OICR is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. The agreement also identifies whether the notification is verbal, written or both and to whom the notification must be provided. The third party service provider also is required to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance

The agreement outlines the consequences of breach of the agreement. It further indicates that OICR will be auditing compliance with the agreement, the manner in which compliance will be audited, and the notice that will be provided to the third party service provider of the audit.

21. Log of Agreements with Third Privacy Service Providers

OICR, in respect of OTB, maintains a log of executed agreements with third party service providers. The log includes the following:

- The name of the third party service provider;
- The nature of the services provided by the third party service provider that require access to and use of personal health information;
- The date that the agreement with the third party service provider was executed;
- The date that the records of personal health information or access to the records of personal health information, if any, was provided;
- The nature of the personal health information provided or to which access was provided;

- The date of termination of the agreement with the third party service provider;
- Whether the records of personal health information, if any, will be securely returned or will be securely disposed of following the date of termination of the agreement; and
- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to the personal health information was terminated or the date by which the records of personal health information must be returned or disposed of or access terminated.

22. Policy and Procedures for the Linkage of Records of Personal Health Information

Policy and Procedures for Data Linkages – Ontario Tumour Bank has been developed and implemented with respect to linkages of records of personal health information.

The policy and procedures identify that OTB permits the linkage of records of personal health information and the purposes for which and the circumstances in which such linkages are permitted.

In identifying the purposes for which and the circumstances in which the linkage of records of PHI is permitted, regard is had to the sources of the records of PHI that are requested to be linked and the identity of the person or organization that will ultimately make use of the linked records of personal health information, including:

- The linkage of records of PHI solely in the custody of OTB for the exclusive use of the linked records of PHI by OTB;
- The linkage of records of PHI in the custody of OTB with records of PHI to be collected from another person or organization for the exclusive use of the linked records of PHI by OTB;
- The linkage of records of PHI solely in the custody of OTB for purposes of disclosure of the linked records of PHI to another person or organization; and
- The linkage of records of PHI in the custody of OTB with records of PHI to be collected from another person or organization for purposes of disclosure of the linked records of PHI to that other person or organization.

Review and Approval Process

The *Policy and Procedures for Data Linkages - Ontario Tumour Bank* indicate that the OTB Director is responsible for receiving the application and the PO, ISO and the Information Governance Committee are all responsible for reviewing and determining whether to approve or deny the request to link records of PHI and the process that must be followed in this regard. This process includes a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also address the requirements that must be satisfied and the criteria that must be considered by the agents responsible for determining whether to approve or deny the request to link records of personal health information.

The policy and procedures also set out the manner in which the decision approving or denying the request to link records of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on Approval

Where the linked records of PHI will be disclosed by OTB to another person or organization, the policy and procedures require that the disclosure be approved pursuant to the *Policy and Procedures for Data Disclosure – Ontario Tumour Bank*.

Where the linked records of personal health information will be used by OTB, the policy and procedures must require that the use be approved pursuant to the *Policy and Procedures for Data Access and Use – Ontario Tumour Bank*. The policy and procedures further require that the linked records of personal health information be de-identified and/or aggregated as soon as practicable pursuant to the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* and that, to the extent possible, only de-identified and/or aggregate information be used by agents of OTB.

Process for the Linkage of Personal Health Information

The policy and procedures outline the process to be followed in linking records of personal health information, the manner in which the linkage of records of PHI must be conducted, and the agents responsible for linking records of PHI when approved in accordance with this policy and its procedures.

Retention

The policy and procedures require that linked records of personal health information be retained in compliance with the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* until they are de-identified and/or aggregated.

Secure Disposal

The *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* addresses the secure disposal of records of personal health information linked by OTB and, in particular, requires that the records of personal health information be securely disposed of in compliance with this policy.

Compliance, Audit and Enforcement

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer in collaboration with the OTB Director to be responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

Tracking Approved Linkages of Records of Personal Health Information

OICR's policies and procedures require that a log be maintained containing the linkages of records of personal health information approved by OTB. The log of data linkages contains the name of the requester, the date/time the linkage was performed, the name of the individual performing the linkage and the disposition of the linked record set. In circumstances where approved data linkages are performed by on an on-going basis by automated processes, OICR's policies and procedures require that an audit trail be maintained specifying the date and time of each record linkage and its disposition. The policy and procedures address where documentation related to the receipt, review, approval or denial of requests to link records of personal health information will be retained and the agent(s) responsible for retaining this documentation.

23. Log of Approved Linkages of Records of Personal Health Information

OTB's negotiation to create linkages of records of personal health information is ongoing, however, to date, no such linkages have been formed. When such linkages will occur, OTB will maintain a log of linkages of records of personal health information approved by OTB. The log will include the name of the person or organization who requested the linkage; the date that the linkage of records of personal health information was approved or denied; and the nature of the records of personal health information linked, the purpose of the linkage, the frequency of the linkage and a copy of (or reference to) the applicable Data Sharing Agreement governing the linkage.

24. Policy and Procedures with Respect to De-Identification and Aggregation

OTB has developed and implemented policy and procedures with respect to de-identification and aggregation. The policy and procedures require that personal health information not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose.

The *Policy and Procedures for Data Access and Use – Ontario Tumour Bank* articulates that record-level data is considered to be de-identified if the threshold is 0.2, which is equivalent to a cell size of 5. In articulating the policy with respect to cell-sizes of less than five, regard is had to the restrictions related to cell-sizes of less than five contained in Data Sharing Agreements, Research Agreements and written research plans pursuant to which the personal health information was collected by OTB.

The policy and procedures provide a definition of de-identified information and aggregate information that identifies the meaning ascribed to each of these terms. The definitions adopted and the policy of OICR with respect to cell-sizes of less than five have regard to, and are consistent with, the meaning of "identifying information" in subsection 4(2) of the Act.

The information that must be removed, encrypted and/or truncated in order to constitute de-identified information and the manner in which the information must be grouped, collapsed or averaged in order

to constitute aggregate information has also been identified. The policy and procedures also address the agents responsible for de-identifying and/or aggregating information and the procedure to be followed in this regard.

Further, the policy and procedures require de-identified and/or aggregate information, including information of cell-sizes of less than five, to be reviewed prior to use or disclosure in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agents responsible for conducting this review are also identified.

The process to be followed in reviewing the de-identified and/or aggregate information and the criteria to be used in assessing the risk of re-identification is also be set out. In establishing the criteria to be used in assessing the risk of re-identification, OTB has given regard to the type of identifying information available, including information that can be used to identify an individual directly (e.g., name, address, health card number) or indirectly (e.g., date-of-birth, postal code, gender).

OTB also consulted with Dr. Khaled El Emam in order to assist in ensuring that the policy and procedures developed with respect to de-identification and aggregation are based on an assessment of the actual risk of re-identification.

The *Policy and Procedures for Data Disclosure – Ontario Tumour Bank* prohibit agents from using de-identified and/or aggregate information, including information in cell-sizes of less than five, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. The policy and procedures also identify the mechanisms implemented to ensure that the persons or organizations to whom de-identified and/or aggregate information is disclosed will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual.

OTB requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, and sets out the frequency with which the policy and procedures will be audited and identifies the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

25. Privacy Impact Assessment Policy and Procedures

The *Privacy Impact Assessment Policy* has been developed and implemented to identify the circumstances in which privacy impact assessments (PIAs) are required to be conducted. In identifying the circumstances in which PIAs are required to be conducted, the policy and procedures ensure that

OTB conducts PIAs on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated.

The policy also sets out limited and specific circumstances in which PIAs are not required to be conducted on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated. The policy and procedures include a rationale for why PIAs are not required under these limited and specific circumstances. The policy and procedures further identify that the PO in consultation with the IGC is responsible for making this determination and requires the determination and the reasons for the determination to be documented.

The policy and procedures also address the timing of PIAs with respect to proposed data holdings involving personal health information and new, or changes to existing, information systems, technologies or programs involving PHI. The policy and procedures require that PIAs be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage.

With respect to existing data holdings involving personal health information, the policy and procedures require that a timetable be developed to ensure that required PIAs are conducted and the policy and procedures identify the Privacy Officer in consultation with the Information Governance Committee as responsible for developing the timetable.

Once PIAs have been completed, the policy and procedures require that they are reviewed on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the information practices of OICR. The policy and procedures also identify the circumstances in which and the frequency with which PIAs are required to be reviewed.

The policy and procedures also identify the shared responsibility of the Privacy Officer and the Information Security Officer in consultation with the OTB Director as responsible and the process that is followed in identifying when PIAs are required; in identifying when PIAs are required to be reviewed in accordance with the policy and procedures; in ensuring that PIAs are conducted and completed; and in ensuring that privacy impact assessments are reviewed and amended, if necessary.

The identification of a need for a PIA, the conduct of PIAs, the determination that the PIA addresses appropriate regulations, the response to PIA recommendations, the procedures for ongoing review of the PIAs and the implementation of recommendations and/or amendments, are a shared responsibility between the PO and the ISO in consultation with the manager of the program, information system or technology requiring the PIA. The policy and procedures also stipulate the required content of privacy impact assessments, including descriptions of the following:

- The data holding, information system, technology or program at issue;
- The nature and type of personal health information collected, used or disclosed or that is proposed to be collected, used or disclosed;

- The sources of the personal health information;
- The purposes for which the personal health information is collected, used or disclosed or is proposed to be collected, used or disclosed;
- The reason that the personal health information is required for the purposes identified;
- The flows of the personal health information;
- The statutory authority for each collection, use and disclosure of personal health information identified;
- The limitations imposed on the collection, use and disclosure of the personal health information;
- Whether or not the personal health information is or will be linked to other information;
- The retention period for the records of personal health information;
- The secure manner in which the records of personal health information are or will be retained, transferred and disposed of;
- The functionality for logging access, use, modification and disclosure of the personal health information and the functionality to audit logs for unauthorized use or disclosure;
- The risks to the privacy of individuals whose personal health information is or will be part of the data holding, information system, technology or program and an assessment of the risks;
- Recommendations to address and eliminate or reduce the privacy risks identified; and
- The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the personal health information.

The process for addressing the recommendations arising from privacy impact assessments, including the PO and/or ISO as responsible for assigning other agents to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations, is also outlined.

The policy and procedures require that a log be maintained of privacy impact assessments that have been completed; that have been undertaken but that have not been completed; and that have not been undertaken. The policy and procedures also identify that the Privacy Officer is responsible for maintaining such a log.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and procedures will be audited and identify the Privacy Officer as responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

In developing the policy and procedures, the Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act, published by the Information and Privacy Commissioner of Ontario are considered.

26. Log of Privacy Impact Assessments

OICR, in respect of OTB, maintains a log of privacy impact assessments that have been completed and of privacy impact assessments that have been undertaken but that have not been completed. The log describes the data holding, information system, technology, or program involving personal health information that is at issue; the date that the privacy impact assessment was completed or is expected to be completed; the Privacy Officer who is the agent responsible for completing or ensuring the completion of the privacy impact assessment; the recommendations arising from the privacy impact assessment; the Privacy Officer as the agent 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.

OICR, in respect of OTB, also maintains a log of data holdings involving personal health information and of new or changes to existing information systems, technologies or programs involving personal health information for which privacy impact assessments have not been undertaken. For each such data holding, information system, technology or program, the log either sets out the reason that a privacy impact assessment will not be undertaken and the Privacy Officer who is responsible for making this determination or sets out the date that the privacy impact assessment is expected to be completed and the agents responsible for completing or ensuring the completion of the privacy impact assessment.

27. Policy and Procedures in Respect of a Security and a Privacy Audit

OICR's *Policy and Procedures in Respect of a Security and a Privacy Audit* set out the types of privacy audits that are required to be conducted. At a minimum, the audits required to be conducted include audits to assess compliance with the privacy policies, procedures and practices implemented by OTB, and audits of the agents permitted to access and use personal health information pursuant to the *Policy and Procedures for Data Access and Use – Ontario Tumour Bank*.

With respect to each privacy audit that is required to be conducted, the policy and procedures set out the purposes of the privacy audit; the nature and scope of the privacy audit (i.e., document reviews, interviews, site visits, inspections); the agent responsible for conducting the privacy audit; and the frequency with which and the circumstances in which each privacy audit is required to be conducted. In this regard, the policy and procedures set out a privacy audit schedule to be developed and identify the Privacy Officer as the agent responsible for developing the privacy audit schedule.

For each type of privacy audit that is required to be conducted, the policy and procedures also set out the process to be followed in conducting the audit. This includes the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided. The policy and procedures further discuss the documentation that must be completed, provided, and/or

executed in undertaking each privacy audit; the Privacy Officer as the agent responsible for completing, providing, and/or executing the documentation.

The Privacy Officer is identified as having been delegated overall responsibility to manage the privacy program. The Information Security Officer is identified as having been delegated overall responsibility to manage the security program.

The policy and procedures also set out the process that must be followed in addressing the recommendations arising from privacy audits, including the Privacy Officer as responsible for assigning other agents to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations, and for monitoring and ensuring the implementation of the recommendations.

The policy and procedures also set out the nature of the documentation that must be completed, provided, and/or executed at the conclusion of the privacy audit, including the Privacy Officer who is the agent responsible for completing, providing, and/or executing the documentation, the agent(s) to whom the documentation must be provided and the required content of the documentation.

The policy and procedures further address the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of addressing the recommendations, are communicated. This includes a discussion of the Privacy Officer as the agent responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit will be communicated.

The policy and procedures further require that a log be maintained of privacy audits and identifies the Privacy Officer as the agent responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified timeframe. They also set out that the documentation related to privacy audits is retained in OICR's secured central filing system, and that the Privacy Officer is responsible for retaining this documentation.

The policy and procedures also require the Privacy Officer, the agent responsible for conducting the privacy audit, to notify OTB, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management* and of an information security breach or suspected information security breach in accordance with the *Information Security Incident Response*.

28. Log of Privacy Audits

OICR, in respect of OTB, maintains a log of privacy audits that have been completed. The log sets out the nature and type of the privacy audit conducted; the date that the privacy audit was completed; the Privacy Officer as the agent responsible for completing the privacy audit; the recommendations arising from the privacy 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.

29. Policy and Procedures for Information Security and Privacy Breach Management

The *Policy and Procedures for Information Security and Privacy Breach Management*, in conjunction with form F-OTB.POL801-1, have been developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of privacy breaches both at OICR and at Collection Centers.

These documents provide a definition of the term "privacy breach." A privacy breach is defined to include:

- The collection, use and disclosure of personal health information that is not in compliance with the Act or its regulation;
- A contravention of the privacy policies, procedures or practices implemented by OTB;
- A contravention of Data Sharing Agreements, Research Agreements, Confidentiality Agreements and Agreements with Third Party Service Providers retained by OTB; and
- Circumstances where personal health information is stolen, lost or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification or disposal.

The policies and procedures impose a mandatory requirement on agents to notify OICR and/or the Collection Centre Privacy Officer (depending on the location) of a privacy breach or suspected privacy breach.

In this regard, the policies and procedures identify that the Collection Centre Privacy Officer, OTB Privacy Lead and Privacy Officer and/or the Information Security Officer must be notified of the privacy breach or suspected privacy breach and provide contact information for these agents. The policies and procedures further stipulate the time frame within which notification must be provided, whether the notification must be provided verbally and/or in writing and the nature of the information that must be provided upon notification. The policies and procedures also address the documentation that must be completed, provided and/or executed with respect to notification; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

Upon notification, the policies and procedures require a determination to be made of whether a privacy breach has in fact occurred and if so, what, if any, PHI has been breached. The Privacy Officer and Information Security Officer are responsible for making this determination.

The policies and procedures further address when senior management, including the President and Scientific Director, will be notified. This includes a discussion of the agents responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.

The policies and procedures also require that containment be initiated immediately and identify the agent responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the agent responsible for containing the breach and the required content of the documentation.

In undertaking containment, the policies and procedures ensure that reasonable steps are taken in the circumstances to protect personal health information from further theft, loss or unauthorized use or disclosure and to protect records of PHI from further unauthorized copying, modification or disposal. These steps include ensuring that no copies of the records of personal health information have been made and ensuring that the records of PHI are either retrieved or disposed of in a secure manner. Where the records of PHI are securely disposed of, written confirmation should be obtained related to the date, time and method of secure disposal. These steps also include ensuring that additional privacy breaches cannot occur through the same means and determining whether the privacy breach would allow unauthorized access to any other information and, if necessary, taking further action to prevent additional privacy breaches.

The agent responsible and the process to be followed in reviewing the containment measures implemented and determining whether the privacy breach has been effectively contained or whether further containment measures are necessary, is identified in the policies and procedures. The policies and procedures also address the documentation that must be completed, provided and/or executed by the agent responsible for reviewing the containment measures; the agent to whom this documentation must be provided; and the required content of the documentation.

The policies and procedures require the health information custodian or other organization that disclosed the personal health information to OTB to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization.

In particular, the policies and procedures set out that the Privacy Officer is responsible for notifying the health information custodian or other organization, the format of the notification and the nature of the information that must be provided upon notification. The policies and procedures require the health information custodian or other organization to be advised of the extent of the privacy breach, the nature of the personal health information at issue, the measures implemented to contain the privacy breach and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation. As a secondary collector of PHI, OTB does not directly notify the individual to whom the personal health information relates of a privacy breach. The required notification shall be provided by the health information custodian.

The policies and procedures also set out whether any other persons or organizations must be notified of the privacy breach and set out that the Privacy Officer is responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification.

The policies and procedures further identify the Privacy Officer as responsible for investigating the privacy breach, the nature and scope of the investigation (i.e., document reviews, interviews, site visits, and inspections) and the process that must be followed in investigating the privacy breach. This includes a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; and the agents responsible for completing, providing and/or executing the documentation. The Privacy Officer has been delegated the overall responsibility to manage the privacy program and the security program.

The policies and procedures also identify the Privacy Officer as responsible for assigning other agent(s) to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines. The policies and procedures also set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the privacy breach, including the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policies and procedures also address the manner and format in which the findings of the investigation of the privacy breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This includes a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the President and Scientific Director.

In addition, the policies and procedures address whether the process to be followed in identifying, reporting, containing, notifying, investigating and remediating a privacy breach is different where the breach is both a privacy breach or suspected privacy breach, as well as an information security breach or suspected information security breach.

Further, the policies and procedures require that a log be maintained of privacy breaches and identify the agents responsible for maintaining the log and for tracking that the recommendations arising from the investigation of privacy breaches are addressed within the identified timelines. They further address where documentation related to the identification, reporting, containment, notification, investigation and remediation of privacy breaches will be retained and identify the Privacy Officer as responsible for retaining this documentation.

OTB requires agents to comply with these breach management documents and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and procedures will be audited and identify the Privacy Officer as responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures were developed with regard to the guidelines produced by the Information and Privacy Commissioner of Ontario entitled What to do When Faced With a Privacy Breach: Guidelines for the Health Sector.

30. Log of Privacy Breaches

OICR, in respect of OTB, maintains a log of privacy breaches setting out:

- The date of the privacy breach;
- The date that the privacy breach was identified or suspected;
- Whether the privacy breach was internal or external;
- The nature of the personal health information that was the subject matter of the privacy breach and the nature and extent of the privacy breach;
- The date that the privacy breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to OTB was notified;
- The date that the investigation of the privacy breach was completed;
- The agent(s) responsible for conducting the investigation;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

31. Policy and Procedures for Privacy Complaints

OICR, in respect of OTB, has developed and implemented *Privacy Complaint Policy and Procedures* to address the process to be followed in receiving, documenting, tracking, investigating, remediating and responding to privacy complaints. A definition of the term "privacy complaint" is provided that, includes concerns or complaints relating to the privacy policies, procedures and practices implemented by OTB and related to the compliance of OTB with the Act and its regulation.

The policy and procedures identify the information that is communicated to the public relating to the manner in which, to whom and where individuals may direct privacy concerns or complaints. The title, mailing address and contact information of the Privacy Officer to whom concerns or complaints may be directed and information related to the manner in which and format in which privacy concerns or complaints may be directed to OTB is made publicly available. The policy and procedures also advise individuals that they may make a complaint regarding compliance with the Act and its regulation to the Information and Privacy Commissioner of Ontario and provides the mailing address and contact information for the Information and Privacy Commissioner of Ontario.

The policy and procedures establish the process to be followed in receiving privacy complaints. All complaints made in writing and addressed to the Privacy Officer will be received by OICR and referred to the Privacy Officer. Upon receipt of the complaint, the PO will ensure that the following information has been requested from the individual making the privacy complaint:

- the reason for making the complaint;
- a description of the complaint; and
- the name and contact information of the individual making the complaint.

Upon receipt of a privacy complaint, the policy and procedures require a determination to be made of whether or not the privacy complaint will be investigated. The policy states that the Privacy Officer in consultation with the Information Governance Committee will review and evaluate all complaints (determination within 15 business days) and will investigate all complaints that are deemed to be justified. The policy and procedures establish the process that must be followed and the criteria that must be used in making the determination, including any documentation that must be completed, provided and/or executed and the required content of the documentation.

In the event that it is determined that an investigation will not be undertaken, the policy and procedures require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken; advising the individual that he or she may make a complaint to the IPC if there are reasonable grounds to believe that OTB has contravened or is about to contravene the Act or its regulation; and providing contact information for the IPC.

In the event that it is determined that an investigation will be undertaken, the policy and procedures require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; advising that an investigation of the privacy complaint will be undertaken; explaining the privacy complaint investigation procedure; indicating whether the individual will be contacted for further information concerning the privacy complaint; setting out the projected time frame for completion of the investigation; and identifying the nature of the documentation that will be provided to the individual following the investigation.

The policy and procedures identify the Privacy Officer as responsible for sending the above noted letters to the individuals making privacy complaints and the time frame within which the letters will be sent to the individuals.

Where an investigation of a privacy complaint will be undertaken, the policy and procedures identify the Privacy Officer as responsible for investigating the privacy complaint, the nature and scope of the investigation (i.e., document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy complaint. This includes a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The roles of the Privacy Officer and the Information Security Officer that have been delegated day-to-day authority to manage the privacy program and the security program are also identified.

The policy and procedures set out the process for addressing the recommendations arising from the investigation of privacy complaints and indicate the Privacy officer is responsible for assigning other

agent(s) to address the recommendations, for establishing timelines to address the recommendations and for monitoring and ensuring the implementation of the recommendations is also addressed in the policy and procedures. The policy and procedures also set out the nature of the documentation that will be completed, provided and/or executed at the conclusion of the investigation of the privacy complaint, including that the Privacy Officer is responsible for completing, preparing and/or executing the documentation; the IGC to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also address the manner and format in which the findings of the investigation of the privacy complaint, including recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This includes a discussion of the agents responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation are communicated; and to whom the findings are communicated, including the President and Scientific Director.

The policy and procedures further requires the individual making the privacy complaint to be notified, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint. The individual making the privacy complaint is also advised that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the Act or its regulation has been or is about to be contravened. The contact information for the Information and Privacy Commissioner of Ontario is also provided. The Privacy Officer will be responsible for notifying the complainant in writing, of the outcome of the investigation, within 60 days of the outcome.

The policy and procedures also address that the Privacy Officer will be responsible for notifying in writing, of the outcome of the investigation, any/all other organizations and/or persons required to be notified as determined during the formal investigation, within 60 days of the outcome.

Further, the policy and procedures requires that a log be maintained. Specifically, the Privacy Officer will track all privacy-related complaints by:

- Maintaining a log of all complaints, responses and any remedial action including any relevant documentation;
- Monitoring the implementation of the recommendations arising from the investigation of complaints within the identified timelines;
- Storing the log and documentation in a secure location in the SharePoint system; and
- Providing the Vice-President, Corporate Services & Chief Financial Officer with a summary of the log on a twice annual basis.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, and indicates a frequency of two years in which the policy and

procedures will be audited by the Privacy Officer. The relationship between this policy and its procedures and the *Policy and Procedures for Information Security and Privacy Breach Management* is also addressed.

This policy and its associated procedures is a stand-alone document.

32. Log of Privacy Complaints

OICR, in respect of OTB, maintains a log of privacy complaints received that sets out:

- The date the Privacy complaint was received;
- The nature of the complaint;
- Agent addressing the complaint;
- Investigation (yes/no);
- Date of determination;
- Date of letter to complainant to announce investigation or non-investigation;
- Agent conducting investigation;
- Date investigation commenced;
- Date of completion of investigation;
- Recommendations (list);
- Agents addressing recommendation;
- Date recommendation to be addressed;
- Manner each recommendation is/was addressed; and
- Date of letter to complainant describing investigation and response.

33. Policy and Procedures for Privacy Inquiries

OICR, in respect of OTB, has a *Privacy Inquiry Policy and Procedures* to address the process to be followed in receiving, documenting, tracking and responding to privacy inquiries. A definition of the term "privacy inquiry" is provided that includes inquiries relating to the privacy policies, procedures and practices implemented by OTB and related to the compliance of OTB with the Act and its regulation.

The policy and procedures include the information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy inquiries. This includes the title, mailing address and contact information of the Privacy Officer to whom privacy inquiries may be directed; information relating to the manner in which privacy inquiries may be directed to OTB; and information as to where individuals may obtain further information about the privacy policies, procedures and practices implemented by OTB.

The policy and procedures further establish the process to be followed in receiving and responding to privacy inquiries. This information includes the Privacy Officer as responsible for receiving and responding to privacy inquiries; any documentation that must be completed, provided and/or executed; the required content of the documentation; and the format and content of the response to the privacy inquiry. The roles of the Privacy Officer and the Information Security Officer that have been delegated day-to-day authority to manage the privacy program and the security program are also identified.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited every two years in accordance with *the Policy and Procedures in Respect of a Security and a Privacy Audit* and identifies the Privacy Officer as responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Complaints* and the *Policy and Procedures for Information Security and Privacy Breach Management* is also addressed.

PART 2 – SECURITY DOCUMENTATION

1. Information Security Policy

OICR has an overarching *Information Security Program* in place to protect personal health information received by OTB under the Act. The policy requires that reasonable and effective steps are taken under the circumstances to ensure that PHI is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of PHI are protected against unauthorized copying, modification or disposal.

The *Information Security Program* also requires OICR to undertake comprehensive and organization-wide threat and risk assessments of all information security assets, including PHI, as well as appropriate project specific threat and risk assessments. It also establishes and documents a methodology for identifying, assessing and remediating threats and risks and for prioritizing all threats and risks identified for remedial action.

The *Information Security Program* establishes a comprehensive information security program that implements administrative, technical and physical security controls that are consistent with established industry standards and practices. The *Information Security Program* effectively addresses the threats and risks identified and is amenable to independent verification and consistent with established security frameworks and control objectives. The security policies and procedures specify that responsibility for the development and implementation of the security program rests with the Information Security Officer of OICR. The duties and responsibilities of agents in respect of the information security program and in respect of implementation of the administrative, technical and physical safeguards are also addressed.

OICR's security policy requires the *Information Security Program* to consist of the following control objectives and security policies, procedures and practices:

- A security governance framework for the implementation of the information security program, including security training and awareness;
- Policies and procedures for the ongoing review of the security policies, procedures and practices implemented;

- Policies and procedures for ensuring the physical security of the premises;
- Policies and procedures for the secure retention, transfer and disposal of records of personal health information, including policies and procedures related to mobile devices, remote access and security of data at rest;
- Policies and procedures to establish access control and authorization including business requirements, user access management, user responsibilities, network access control, operating system access control and application and information access control;
- Policies and procedures for information systems acquisition, development and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management;
- Policies and procedures for monitoring, including policies and procedures for maintaining and reviewing system control and audit logs and security audits;
- Policies and procedures for network security management, including patch management and change management;
- Policies and procedures related to the acceptable use of information technology;
- Policies and procedures for back-up and recovery;
- Policies and procedures for information security breach management;
- Policies and procedures for a security audit; and
- Policies and procedures to establish protection against malicious and mobile code.

OICR's *Information Security Program* refers to more detailed policies and procedures developed and implemented to address the above-noted matters as follows:

- Policy Statement 1.0 Acceptable Use
- Policy Statement 2.0 Data Classification
- Policy Statement 3.0 Encryption
- Policy Statement 4.0 Secure Electronic Data Retention, Backup, Disposal and Destruction
- Policy Statement 5.0 Data Protection (Encryption, Transmission and Storage)
- Policy Statement 6.0 Access Control, Identification and Authentication
- Policy Statement 7.0 Password Governance
- Policy Statement 8.0 Internet Usage
- Policy Statement 9.0 Access to OICR Systems by Contractors, Consultants & Third Parties
- Policy Statement 10.0 Information Security Incident Response
- Policy Statement 11.0 Risk Assessment Policy and Threat Risk Assessment Guide
- Policy Statement 12.0 Change Controls (OICR Production Servers)
- Policy Statement 13.0 Server Security
- Policy Statement 14.0 Network Security
- Policy Statement 15.0 Workstation Security
- Policy Statement 16.0 Personal Use of OICR Systems
- Policy Statement 17.0 Personal Third Party Devices Interacting with OICR Systems

- Policy Statement 18.0 Electronic Mail Security
- Policy Statement 19.0 Extranet Security
- Policy Statement 20.0 Anti-Virus Administration
- Policy Statement 22.0 Remote Access
- Policy Statement 23.0 Electronic Media Destruction
- Policy Statement 24.0 Declaration and Disposal of Surplus IT Equipment
- Policy Statement 25.0 HelpDesk Services Security
- Policy Statement 26.0 Employees on Temporary (Short or Long-Term) Leave
- Policy Statement 28.0 Mobile Devices Security
- Policy Statement 29.0 Disaster Recovery and Offsite Data Storage
- Policy Statement 30.0 Research Lab Security
- Policy Statement 31.0 Loaner Devices
- Policy Statement 32.0 Restricted or Non-Networked Computer Environments
- Policy Statement 33.0 Patch Management
- Policy Statement 36.0 Mobile Device Allocation
- Policy Statement 38.0 IT Device (Hardware and Software) Allocations

The *Information Security Program* also references the information security infrastructure detailed in other policies and procedures including the transmission of personal health information over authenticated, encrypted and secure connections; the establishment of hardened servers, firewalls, demilitarized zones and other perimeter defences; anti-virus, anti-spam and anti-spyware measures; intrusion detection and prevention systems; privacy and security enhancing technologies; and mandatory system-wide password-protected screen savers after a defined period of inactivity.

OICR's policy and procedures also set out the procedures for day-to-day monitoring of security controls to verify the effectiveness of the security program and to detect and deal with threats and risks to holdings of personal health information.

Compliance with these policies is mandatory for all who come into contact with OICR's secured information assets. It is the responsibility of each agent of OICR to understand his/her role and responsibilities regarding information security issues, and to protect OICR's information assets. As the owner of its information technology resources, OICR reserves the right to audit and monitor all systems' usage and content. Such audits are carried out by the Information Security Officer or designate without prior notice (for security reasons), to support ongoing operations, to demonstrate compliance with regulations, for maintenance and upgrades to technology resources, to support approved investigative activities related to inappropriate conduct or legal issues, and as permitted or required by law. Users must not modify systems in any way which would prevent OICR from auditing and monitoring these systems.

OICR, in respect of OTB, requires agents to comply with these above policies and with all other security policies, procedures, and practices implemented by OICR and addresses how and by whom compliance will be enforced and the consequences of breach. The *Policy and Procedures for Information Security*

and Privacy Breach Management indicates that a breach may result in discipline, up to and including termination of an employee or termination of a relationship with agents who are not OICR employees.

OICR's *Policy and Procedures in Respect of a Security and a Privacy Audit* requires its agents to notify the Information Security Officer, at the first reasonable opportunity, if an agent breaches or believes there may have been a breach of this policy or any of the security policies, procedures and practices.

2. Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices

OICR's *Development and Management of Policies, Procedures and Guidelines* are aimed at ensuring the ongoing review of the security policies, procedures and practices. The purpose of the review is to determine whether amendments are needed or whether new security policies, procedures and practices are required.

Documents relating to OICR's privacy and information security program including those relevant to OTB must be reviewed, at a minimum, on an annual basis by the policy sponsor, including the Privacy Officer and Information Security Officer, and endorsed by the Information Governance Committee prior to being approved by OICR's Senior Management Team and implemented via education and training to affected OICR individuals.

In undertaking the review and determining whether amendments and/or new security policies, procedures and practices are necessary, OICR takes into account any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation; evolving industry security standards and best practices; technological advancements; amendments to the Act and its regulation relevant to OTB; and recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches. It also takes into account whether the security policies, procedures and practices of OICR continue to be consistent with its actual practices and whether there is consistency between and among the security and privacy policies, procedures and practices implemented.

The policy and procedures identify the policy working group/sponsor as responsible for communicating the amended or newly developed security policies, procedures and practices, including the method and nature of the communication. It also provides the procedure to be followed by the communications team in reviewing and amending the communication materials available to the public and other stakeholders as a result of the amended or newly developed security policies, procedures and practices.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The *Information Security Program* stipulates that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit* and sets out the frequency with which the policy and procedures will be audited, identifying the Privacy Officer and Information Security Officer as responsible for ensuring compliance with the policy and its procedures and for conducting the audits.

3. Policy and Procedures for Ensuring Physical Security of Personal Health Information

Policies and procedures have been developed and implemented to address the physical safeguards implemented by OICR, and thus, OTB, to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

The physical safeguards implemented include controlled access to the premises and to locations within the premises where records of personal health information are retained such as locked, alarmed, restricted and/or monitored access.

The premises of the OICR are divided into varying levels of security with each successive level being more secure and restricted to fewer individuals. In order to access locations within the premises where records of personal health information are retained, individuals are required to pass through multiple levels of security.

OICR, in respect of OTB, requires agents to comply with the policies and its procedures and indicate that compliance will be enforced by the Privacy Officer and Information Security Officer and sets out the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the policy on *Logging and Security Audits*. The Information Security Officer will assume primary responsibility in ensuring regular and timely completion of security audits.

Scheduled Audits:

- Quarterly account review of active directory (AD) and lightweight directory access protocol (LDAP): To verify that only active employees have active accounts.
- Quarterly computer domain account (AD) audit: To ensure that only current user's computers are connected to the AD domain.
- Quarterly review Unix server log on failure: To analyze logs and investigate anything unusual.
- Quarterly network port scans: To compare the previous port scan to the current port scan. If new ports are opened further investigation is required.
- Annual inspection: Annual inspection of all workstations to confirm OICR root account is installed and active, and that any machines not owned and managed by OICR are removed from the OICR network.
- Monthly Internet use inspection: Analysis of Websense logs.
- Weekly inspection: No less than weekly, security event logs on the active directory are monitored for log on failures. Further investigation is undertaken should something unusual be noticed.

IT Systems Administrators will be responsible for direct review of relevant logs, conduct of the audits, and documentation of the security audit.

The policy and procedures also require agents to notify OICR at the first reasonable opportunity, in accordance with the *Information Security Program*, if an agent breaches or believes that there may have been a breach of this policy or its associated procedures.

Policy, Procedures and Practices with Respect to Access by Agents

The various levels of access that may be granted to the premises and to locations within the premises where records of personal health information are retained are set out in the policy and procedures.

The *Access Card and Key Management for MaRS Location* identify the agents responsible for receiving, reviewing, granting and terminating access by agents to the premises and to locations within the premises where records of personal health information are retained, including the levels of access that may be granted. The process to be followed and the requirements that must be satisfied are also identified, including any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures address the criteria that must be considered by the agent(s) responsible for approving and determining the appropriate level of access. The criteria are based on the "need to know" principle and ensure that access is only provided to agents who routinely require such access for their employment, contractual or other responsibilities. In the event that an agent only requires such access for a specified period, the policy and procedures establish a process for ensuring that access is permitted only for that specified period.

The policy and procedures also set out the manner in which the determination relating to access and the level of access is documented; to whom this determination will be communicated; any documentation that must be completed, provided and/or executed by the agent(s) responsible for making the determination; and the required content of the documentation. User accounts are created by the IT department at time of hire or engagement, or after a job/role change, or change to the terms of engagement based on the Human Resources-IT workflow process.

The policy and procedures also address the agent(s) responsible and the process to be followed in providing identification cards, access cards and/or keys to the premises and to locations within the premises. This includes a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

Theft, Loss and Misplacement of Identification Cards, Access Cards and Keys

Access Card and Key Management for MaRS Location requires agents to notify OICR at the first reasonable opportunity of the theft, loss or misplacement of identification cards, access cards and/or keys and sets out the process that must be followed in this regard.

This policy identifies the Facilities Manager as the agent to whom the notification must be provided; the nature and format of the notification; the documentation that must be completed, provided and/or

executed; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

The safeguards that are required to be implemented as a result of the theft, loss or misplacement of identification cards, access cards and/or keys and the agent(s) responsible for implementing these safeguards is also outlined in the policies and procedures.

The policy and procedures also address the circumstances in which and the procedure that must be followed in issuing temporary or replacement identification cards, access cards and/or keys and the agent(s) responsible for their issuance. This includes a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom the documentation must be provided; the required content of the documentation; the agent(s) to whom temporary identification cards, access cards and/or keys shall be returned; and the time frame for return.

The process to be followed in the event that temporary identification cards, access cards and/or keys are not returned, including the agent(s) responsible for implementing the process and the time frame within which the process must be implemented, is also addressed. Specifically, notice of any access card determined to be unreturned shall be provided to the Facilities Manager who will immediately void all missing access cards.

Termination of the Employment, Contract or Other Relationship

OICR policy and procedures require agents, as well as their supervisors, to notify the OICR of the termination of their employment, contractual or other relationship with the OICR and to return their identification cards, access cards and/or keys to OICR on or before the date of termination of their employment, contractual or other relationship in accordance with the *Employees Departing OICR* policy and procedures.

The policy and procedures also require that access to the premises be terminated upon the cessation of the employment, contractual or other relationship in accordance with the *Employees Departing OICR* policy and procedures.

Notification When Access is No Longer Required

The *Access Card and Key Management for MaRS Location* policy and procedures requires an agent granted approval to access location(s) where records of personal health information are retained, as well as his or her supervisor, to notify OICR when the agent no longer requires such access.

The policy and procedures also identify the agent(s) to whom the notification must be provided; the nature and format of the notification; the time frame within which the notification must be provided; the process that must be followed in providing the notification; the agent(s) responsible for terminating access; the procedure to be followed in terminating access; the method by which access will be terminated; and the time frame within which access must be terminated.

Audits of Agents with Access to Premises

Audits are conducted of agents with access to the premises of OICR and to locations within the premises where records of personal health information are retained in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*. The purpose of the audit is to ensure that agents granted access to the premises and to locations within the premises where records of PHI are retained continue to have an employment, contractual or other relationship with OTB and continue to require the same level of access.

In this regard, the policies and procedures identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy and its procedures and the frequency with which the audits must be conducted. These audits are conducted daily for temporary cards, quarterly for access cards and annually for keys.

Tracking and Retention of Documentation Related to Access to the Premises

Access Card and Key Management for MaRS Location requires that a log be maintained of agents granted approval to access the premises of OICR and to locations within the premises where records of personal health information are retained and identifies the agents responsible for maintaining such a log. The policy and procedures also address where documentation related to the receipt, review, approval and termination of access to the premises and to locations within the premises where PHI is retained is maintained, and indicates the agents responsible for maintaining this documentation.

Policy, Procedures and Practices with Respect to Access by Visitors

The *Access Card and Key Management for MaRS Location* policy addresses the agents responsible and the process to be followed in identifying, screening and supervising visitors to the premises of OICR. The policy and procedures set out the identification that is required to be worn by visitors; any documentation that must be completed, provided and/or executed by agents responsible for identifying, screening and supervising visitors; and the documentation that must be completed, provided and/or executed by visitors.

The visitors are required to record their name, date and time of arrival, time of departure and the name of the agent(s) with whom the visitors are meeting. The duties of agent(s) responsible for identifying, screening and supervising visitors are also addressed. These duties include ensuring that visitors are accompanied at all times; ensuring that visitors are wearing the identification issued by OICR; ensuring that the identification is returned prior to departure; and ensuring that visitors complete the appropriate documentation upon arrival and departure.

The policy and procedures also address the process to be followed when the visitor does not return the identification provided or does not document his or her date and time of departure and the agent(s) responsible for implementing the identified process.

4. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity

A log is maintained of agents granted approval to access the premises of OICR and the level of access granted. The log includes the name of the agent granted approval to access the premises; the level and

nature of the access granted; the locations within the premises to which access is granted; the date that the access was granted; the date(s) that identification cards, access cards and/or keys were provided to the agent; the identification numbers on the identification cards, access cards and/or keys, if any; the date of the next audit of access; and the date that the identification cards, access cards and/or keys were returned to OICR, if applicable.

5. Policy and Procedures for Secure Retention of Records of Personal Health Information

OICR's *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* policy was developed and implemented with respect to the secure retention of records of personal health information in paper and electronic format.

The policy and procedures identify the retention period for records of personal health information in both paper and electronic format, including various categories thereof. For records of personal health information used for research purposes, OTB ensures that the records of PHI are not being retained for a period longer than that set out in the written research plan approved by a research ethics board.

For records of personal health information collected pursuant to a Data Sharing Agreement, the policy and procedures prohibit the records from being retained for a period longer than that set out in the Data Sharing Agreement. In any event, the policy and procedures mandate that records of PHI be retained for only as long as necessary to fulfill the purposes for which the personal health information was collected.

The policy and procedures also require the records of personal health information to be retained in a secure manner and identifies the agents responsible for ensuring the secure retention of these records. In this regard, the policy and procedures identify the precise methods by which records of PHI in paper and electronic format are to be securely retained, including records retained on various media.

Further, this policy and procedures require agents of OICR to take the necessary steps to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of PHI are protected against unauthorized copying, modification or disposal. The steps that must be taken by agents are also outlined in the policy and procedures.

A third party service provider is contracted to retain records of personal health information on behalf of OICR. As such, the policy and procedures also address the following additional matters.

The policy and procedures address the circumstances in which and the purposes for which records of personal health information will be transferred to the third party service provider for secure retention. They detail the procedure to be followed in securely transferring the records of PHI to the third party service provider and in securely retrieving the records from the third party service provider, including the secure manner in which the records will be transferred and retrieved, the conditions pursuant to which the records will be transferred and retrieved and the agent(s) responsible for ensuring the secure transfer and retrieval of the records. In this regard, the procedures comply with OICR's *Retention,*

Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information.

Further, the policy and procedures address the documentation that is required to be maintained in relation to the transfer of records of personal health information to the third party service provider for secure retention. In particular, the policy and procedures require the agents responsible for ensuring the secure transfer to document the date, time and mode of transfer and to maintain a repository of written confirmations received from the third party service provider upon receipt of the records PHI.

The policy and procedures also require a detailed inventory to be maintained of records of personal health information being securely retained by the third party service provider and of records of PHI retrieved by OTB and identifies the agents responsible for maintaining the detailed inventory.

Further, where a third party service provider is contracted to retain records of personal health information, the policy and procedures require that a written agreement be executed with the third party service provider containing the relevant language from the Third Party Service Provider Agreements template, and identifying the agent responsible for ensuring that the agreement has been executed prior to transferring the records of PHI for secure retention.

OTB requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, setting out the frequency with which the policy and procedures will be audited and identifying the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of the policy or its procedures.

6. Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices

OICR, in respect of OTB, has a policy and procedures that identifies whether and in what circumstances OICR permits personal health information to be retained on a mobile device. In this regard, the policy and procedures provide a definition of “mobile device.”

In drafting the *Mobile Devices Security* policy, OICR had regard to orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-004 and Order HO-007; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices, Fact Sheet 14: Wireless Communication Technologies: Safeguarding Privacy and Security and Safeguarding Privacy in a Mobile Workplace.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and procedures will be audited and identify the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

Where Personal Health Information is not Permitted to be Retained on a Mobile Device

OICR does not permit PHI to be retained on a mobile device, as such, the policy and procedures expressly prohibit the retention of PHI on a mobile device and indicate whether or not personal health information may be accessed remotely through a secure connection or virtual private network.

When OTB permits personal health information to be accessed remotely, the policy and procedures set out the circumstances in which this is permitted.

Approval Process

The *Remote Access* policy and procedures identify that approval is required prior to accessing personal health information remotely through a secure connection or virtual private network.

The policy and procedures identify the process that must be followed and the agent responsible for receiving, reviewing and determining whether to approve or deny a request for remote access to PHI. This includes a discussion of any documentation that must be completed, provided and/or executed; the agents responsible for completing, providing and/or executing the documentation; the agents to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures further address the requirements that must be satisfied and the criteria that must be considered by the agents responsible for determining whether to approve or deny the request for remote access.

Prior to any approval of a request to remotely access personal health information, the policy and procedures require the agents responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more PHI will be accessed than is reasonably necessary to meet the identified purpose.

The policy and procedures also require the agents responsible for determining whether to approve or deny the request to ensure that the use of the personal health information has been approved pursuant to the *Remote Access* policy.

The policy and procedures also set out the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Remote Access to Personal Information

The *Remote Access* policy and procedures identify the conditions or restrictions with which agents granted approval to access personal health information remotely must comply. The agents are prohibited from remotely accessing PHI if other information, such as de-identified and/or aggregate information, will serve the purpose and from remotely accessing more PHI than is reasonably necessary for the identified purpose. The policy and procedures also set out the administrative, technical and physical safeguards that must be implemented by agents in remotely accessing PHI.

Requests for remote access must be submitted to the OICR IT HelpDesk. The HelpDesk will ensure that the request clearly states who requires access, why they require access, and that their manager and/or the data owner has approved this access. If the remote access request is from an OICR employee, the HelpDesk will verify that they are an active employee, who has been fully provisioned and trained on Information Security and Privacy. The HelpDesk will assign any request that does not meet these requirements to the Information Security Officer.

7. Policy and Procedures for Secure Transfer of Records of Personal Health Information

OICR, in respect of OTB, has developed and implemented policies and procedures with respect to the secure transfer of records of personal health information in paper and electronic format.

OICR's *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* requires records of personal health information to be transferred in a secure manner and sets out the secure methods of transferring records of personal health information in paper and electronic format that have been approved by OTB. OICR's policy and procedures require its agents to use the prescribed methods of transferring records of personal health information and prohibit the use of other methods.

The procedures to be followed in transferring records of personal health information through each of the approved methods are outlined. The polices include a discussion of the conditions pursuant to which records of PHI will be transferred; the agent(s) responsible for ensuring the secure transfer; any documentation that is required to be completed, provided and/or executed in relation to the secure transfer; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

The policy and procedures also indicate that the agent transferring records of PHI is required to document the date, time and mode of transfer; the recipient of the records of PHI; and the nature of the records of PHI transferred. Further, the policy and procedures note that written confirmation of receipt of the records of personal health information is required from the recipient, and the manner of

obtaining and recording acknowledgement of receipt of the records of personal health information and the agent(s) responsible for doing so.

Also outlined in the policy and procedure are the administrative, technical and physical safeguards that must be implemented by agents in transferring records of PHI through each of the approved methods in order to ensure that the records of PHI are transferred in a secure manner.

OTB ensures that the approved methods of securely transferring records of personal health information and the procedures and safeguards that are required to be implemented in respect of the secure transfer of records of PHI are consistent with:

- Orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including but not limited to Order HO-004 and Order HO-007;
- Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario, including Privacy Protection Principles for Electronic Mail Systems and Guidelines on Facsimile Transmission Security; and
- Evolving privacy and security standards and best practices.

OTB requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, setting out the frequency with which the policy and procedures will be audited and identifying the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

8. Policy and Procedures for Secure Disposal of Records of Personal Health Information

OICR's *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* policy and procedures with respect to the secure destruction and/or disposal of records of personal health information in paper and electronic format to ensure that such records cannot be reasonably recovered or reconstructed after destruction and disposal.

The policy and procedures require records of personal health information to be disposed of in a secure manner and provide a definition of secure disposal that is consistent with the Act and its regulation. The policy and procedures further identify the precise method by which records of personal health information in paper format are required to be securely disposed of and the precise method by which records of PHI in electronic format, including records retained on various media, are required to be securely disposed of.

In the case of paper records, the policies and procedures state that the personal health information shall be destroyed by cross-cut shredding, pulverization or incineration and further require that printed documents containing personal health information shall not be disposed of in waste baskets, recycling bins, or any other normal waste disposal methods.

All data storage media, (e.g., tapes, hard drives, and CDs) used by OICR and which contain PHI must be physically destroyed in such a manner that data retrieval is not possible, provided that such data storage media meet one of the following criteria:

- It is a backup copy of data that has been stored for more than seven years or the duration specified by the data owner;
- It has reached the end of its life expectancy and requires disposal or recycling;
- It has "failed", as in the case of a hard drive or USB failure, and requires disposal or recycling;
- It has been slated for destruction as per its classification by a data owner.

Physical destruction of all electronic media is documented by a Certificate of Destruction, signed by the systems administrator affecting the process and his or her immediate supervisor. Data that is slated for disposal and destruction is permanently deleted using a minimum of a seven pass deletion method.
In addressing the precise method by which records of personal health information in paper and electronic format must be securely disposed of, OICR ensures that the method of secure disposal adopted is consistent with the Act and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information.

The policy and procedures further address the secure retention of records of personal health information pending their secure disposal in accordance with *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*. The policy and procedures require the physical segregation of records of personal health information intended for secure disposal from other records intended for recycling, require that an area is designated for the secure retention of records of PHI pending their secure disposal and require the records of PHI to be retained in a clearly marked and locked container pending their secure disposal. The policy and procedures also identify the agents responsible for ensuring the secure retention of records of PHI pending their secure disposal.

In the event that records of personal health information or certain categories of records of PHI will be securely disposed of by a designated agent, who is not a third party service provider, the policy and procedures identify the designated agent responsible for securely disposing of the records of PHI; the responsibilities of the designated agent in securely disposing of the records; and the time frame within which, the circumstances in which and the conditions pursuant to which the records of PHI must be securely disposed of. The policy and procedures also require the designated agent to provide a certificate of destruction, which may include:

- Identifying the records of personal health information to be securely disposed of;
- Confirming the secure disposal of the records of personal health information;

- Setting out the date, time and method of secure disposal employed; and
- Bearing the name and signature of the agent(s) who performed the secure disposal.

The time frame within which and the agents to whom certificates of destruction must be provided following the secure disposal of the records of PHI are also addressed in the policy and procedures.

In the event that records of PHI or certain categories of records of PHI will be securely disposed of by an agent that is a third party service provider, the policy and procedures address the following additional matters.

The policy and procedures detail the procedure to be followed by OICR in securely transferring the records of personal health information to the third party service provider for secure disposal. The policy and procedures identify the secure manner in which the records of personal health information will be transferred to the third party service provider, the conditions pursuant to which the records will be transferred and the agents responsible for ensuring the secure transfer of the records. In this regard, the policy and procedures shall comply with the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information*.

The policy and procedures also require the agents responsible for ensuring the secure transfer of records of personal health information to document the date, time and mode of transfer of the records of personal health information and to maintain a repository of written confirmations received from the third party service provider evidencing receipt of the records of personal health information. A detailed inventory related to the records of PHI transferred to the third party service provider for secure disposal must also be maintained and the policy and procedures require maintaining this inventory.

Further, where a third party service provider is retained to securely dispose of records of personal health information, the policy and procedures require that a written agreement be executed with the third party service provider containing the relevant language from the Third Party Service Provider Agreement template, and identify the agent(s) responsible for ensuring that the agreement has been executed prior to the transfer of records of personal health information for secure disposal.

The policy and procedures also outline the procedure to be followed in tracking the dates that records of personal health information are transferred for secure disposal and the dates that certificates of destruction are received, whether from the third party service provider or from the designated agent that is not a third party service provider, and the agent(s) responsible for conducting such tracking. Further, the policy and procedures outline the process to be followed where a certificate of destruction is not received within the time set out in the policy and its procedures or within the time set out in the agreement with the third party service provider and the agent(s) responsible for implementing this process.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and procedures will be

audited and identify the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

9. Policy and Procedures Relating to Passwords

A policy and procedures has been developed and implemented with respect to passwords for authentication and passwords for access to information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by OICR.

OICR's *Password Governance* policy and procedures identify the required minimum and maximum length of the password, the standard mandated for password composition and other restrictions imposed on passwords, such as re-use of prior passwords and the use of passwords that resemble prior passwords. The policy and procedures specify that, at a minimum, passwords must be comprised of a combination of upper and lower case letters as well as numbers and non-alphanumeric characters.

The time frame within which passwords will automatically expire, the frequency with which passwords must be changed, the consequences arising from a defined number of failed log-in attempts and the imposition of a mandatory system-wide password-protected screen saver after a defined period of inactivity are also addressed.

The policy and procedures further identify the administrative, technical and physical safeguards that are implemented by agents in respect of passwords in order to ensure that the personal health information is protected against theft, loss and unauthorized use or disclosure and that the records of personal health information are protected against unauthorized copying, modification or disposal. At a minimum, agents are required to keep their passwords private and secure and are required to change their passwords immediately if they suspect that their password has become known to any other individual, including another agent. Agents also are prohibited from writing down, displaying, concealing, hinting at, providing, sharing or otherwise making their password known to any other individual, including another agent of OTB.

OTB ensures that the policy and procedures are consistent with any orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation; with any guidelines, fact sheets and best practices issued by the IPC; and with evolving privacy and security standards and best practices.

OTB also requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, sets out the frequency with which the policy and procedures will be audited and identifies the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

10. Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs

A policy and procedures have been developed and implemented 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 PHI and with the threats and risks associated with the PHI.

The policy and procedures require OTB to ensure that all information systems, technologies, applications and programs involving personal health information have the functionality to log access, use, modification and disclosure of PHI.

The policy and procedures also set out the types of events that are required to be audited and the nature and scope of the information that must be contained in system control and audit logs. The system control and audit logs set out the date and time that personal health information is accessed; the date and time of the disconnection; the nature of the disconnection; the name of the user accessing personal health information; the network name and identification of the computer through which the connection is made; and the actions that create, amend, delete or retrieve personal health information including the nature of the action, the date and time of the action, the name of the user that performed the action and the changes to values, if any.

The Information Security Officer is responsible for ensuring that the types of events that are required to be audited are in fact audited and that the nature and scope of the information that is required to be contained in system control and audit logs is in fact logged.

The policy and procedures require the system control and audit logs to be immutable, that is, OTB ensures that the system control and audit logs cannot be accessed by unauthorized persons or amended or deleted in any way. The policy sets out the procedures in this regard and the agents responsible for implementing these procedures.

In practice, logs from the TissueMetrix servers are stored locally on OICR servers and are only accessible by authorized users, as well as transmitted in real time over a secure channel via a logging agent to a centralized logging server. Local logs are accessible by authorized OTB staff only, while logs stored on the central logging server are accessible by OICR information security IT staff only. The centralized logging server, known as the Log Correlation Engine (LCE), is a password protected server for the specific purpose of securely storing, archiving, correlating and analyzing log events. The LCE server is only accessible by authorized OICR information security and IT staff, and it is not possible for unauthorized users to access, amend or delete these logs in any way. Should the logging agent be stopped, or should any server log files be deleted or amended by these authorized users, the systems will identify that

either the logs were stopped, or that the log database was manipulated. Further logs will then allow OICR to identify which user was on the logging system at the time the logs were manipulated.

Log events which are sent to the LCE include:

- TissueMetrix database logs of user login/logout;
- TissueMetrix application logs of User activity; and
- Windows Operating System Server "events" (e.g., log in, log out, attempted log in failures, system events, etcetera etc...).

The policy and procedures also identify the length of time that system control and audit logs are required to be retained, that the ISO is responsible for retaining the system control and audit logs and sets out where the system control and audit logs will be retained.

The review of system control and audit logs is also be addressed, including the ISO being responsible for reviewing the system control and audit logs, the frequency with which and the circumstances in which system control and audit logs are required to be reviewed and the process to be followed in conducting the review.

The ISO is required to notify the OTB, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management* and/or of an information security breach or suspected information security breach in accordance with the *Information Security Incident Response*. The relationship between this policy and its procedures and its *Policy and Procedures for Information Security and Privacy Breach Management* is also identified.

Further, the policy and procedures address the findings arising from the review of system control and audit logs, including the agent(s) responsible for assigning other agent(s) to address the findings, for establishing timelines to address the findings, for addressing the findings and for monitoring and ensuring that the findings have been addressed.

The policy and procedures also set out the nature of the documentation, that must be completed, provided and/or executed following the review of system control and audit logs; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; the time frame within which the documentation must be provided; and the required content of the documentation.

The manner and format for communicating the findings of the review and how the findings have been or are being addressed are also outlined. This includes a discussion of the agent(s) responsible for communicating the findings of the review of system control and audit logs; the mechanism and format for communicating the findings of the review; the time frame within which the findings of the review must be communicated; and to whom the findings of the review must be communicated.

Further, the policy and procedures set out the process to be followed in tracking that the findings of the review of system control and audit logs have been addressed within the identified timelines, including the agent(s) responsible for tracking that the findings have been addressed.

OTB requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, sets out the frequency with which the policy and procedures will be audited and identifies the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

11. Policy and Procedures for Patch Management

A policy and procedures have been developed and implemented for patch management.

The *Patch Management* policy and procedures identify the agents responsible for monitoring the availability of patches on behalf of OTB, the frequency with which such monitoring must be conducted and the procedure that must be followed in this regard.

The agents responsible for analyzing the patch and making a determination as to whether or not the patch should be implemented are also be identified. The policy and procedures further discuss the process that must be followed and the criteria that must be considered by the agent(s) responsible for undertaking this analysis and making this determination.

In circumstances where a determination is made that the patch should not be implemented, the policy and procedures require the responsible agents to document the description of the patch; the date that the patch became available; the severity level of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; and the rationale for the determination that the patch should not be implemented.

In circumstances where a determination is made that the patch should be implemented, the policy and procedures identify the agents responsible for determining the time frame for implementation of the patch and the priority of the patch. The policy and procedures also set out the criteria upon which these determinations are to be made, the process by which these determinations are to be made and the documentation that must be completed, provided and/or executed in this regard.

The policy and procedures also set out the process for patch implementation, including the agents responsible for patch implementation and any documentation that must be completed, provided and/or executed by the agent(s) responsible for patch implementation.

The circumstances in which patches must be tested, the time frame within which patches must be tested, the procedure for testing and the agent(s) responsible for testing are also addressed, including

the documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.

The policy and procedures also require documentation to be maintained in respect of patches that have been implemented and identify the agent(s) responsible for maintaining this documentation. The documentation includes a description of the patch; the date that the patch became available; the severity level and priority of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; the date that the patch was implemented; the agent(s) responsible for implementing the patch; the date, if any, when the patch was tested; the agent(s) responsible for testing; and whether or not the testing was successful.

OTB requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, at minimum every 2 years, by the Privacy Officer and Information Security Officer who are responsible for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify Privacy Officer at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

12. Policy and Procedures Related to Change Management

The *Change Controls* policy and procedures is implemented for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment of OTB.

The policy and procedures identify the agents responsible for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment and the process that must be followed and the requirements that must be satisfied in this regard. This includes a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. At a minimum, the documentation shall describe the change requested, the rationale for the change, why the change is necessary and the impact of executing or not executing the change to the operational environment.

The criteria that must be considered by the agents responsible for determining whether to approve or deny a request for a change to the operational environment are also identified.

The policy and procedures also set out the manner in which the decision approving or denying the request for a change to the operational environment and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

If the request for a change to the operational environment is not approved, the policy and procedures require the responsible agents to document the change to the operational environment requested, the name of the agent requesting the change, the date that the change was requested and the rationale for the determination that the change should not be implemented.

If the request for a change to the operational environment is approved, the policy and procedures identify the agent(s) responsible for determining the time frame for implementation of the change and the priority assigned to the change requested. The policy and procedures also set out the criteria upon which these determinations are to be made, the process by which these determinations are to be made and any documentation that must be completed, provided and/or executed in this regard.

The policy and procedures also set out the process for implementation of the change to the operational environment, including the agent(s) responsible for implementation and any documentation that must be completed, provided and/or executed by the agent(s) responsible for implementation.

The circumstances in which changes to the operational environment are tested, the time frame within which changes are tested, the procedure for testing and the agent(s) responsible for testing are also addressed in the policy and procedures, including the documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.

The policy and procedures also require documentation to be maintained of changes that have been implemented and identify the agent(s) responsible for maintaining this documentation. The documentation includes a description of the change requested; the name of the agent requesting the change; the date that the change was requested; the priority assigned to the change; the date that the change was implemented; the agent(s) responsible for implementing the change; the date, if any, when the change was tested; the agent(s) responsible for testing; and whether or not the testing was successful.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, sets out the frequency with which the policy and procedures will be audited and identifies the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

13. Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information

The *Disaster Recovery and Offsite Data Storage* policy and procedures have been implemented for the back-up and recovery of records of personal health information.

The policy and procedures identify the nature and types of back-up storage devices maintained by OICR on behalf of OTB; the frequency with which records of personal health information are backed-up; the agents responsible for the back-up and recovery of records of personal health information; and the process that must be followed and the requirements that must be satisfied in this regard. This includes a discussion of any documentation that must be completed; the agent(s) responsible for completing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures also address testing the procedure for back-up and recovery of records of personal health information, the agents responsible for testing, the frequency with which the procedure is tested and the process that must be followed in conducting such testing. This includes a discussion of any documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.

The policy and procedures further identify the agents responsible for ensuring that back-up storage devices containing records of personal health information are retained in a secure manner, the location where they are required to be retained and the length of time that they are required to be retained. In this regard, the policy and procedures requires the backed-up records of PHI to be retained in compliance with the *Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-Identified Health Information* and identify the agent(s) responsible for ensuring that they are retained in a secure manner.

Additionally, if a third party service provider is contracted to retain backed-up records of personal health information, the policy and associated procedures also address the following additional matters.

The policy and procedures require the backed-up records of personal health information to be transferred to and from the third party service provider in a secure manner. They also detail the procedure to be followed in securely transferring the backed-up records of PHI to the third party service provider and in securely retrieving the backed-up records from the third party service provider, including the secure manner in which they will be transferred and retrieved, the conditions pursuant to which they will be transferred and retrieved and the agent(s) responsible for ensuring the secure transfer and retrieval of the backed-up records. In this regard, the procedures comply with the *Sending/Receiving Personal Health Information, Personal Information and Confidential/Sensitive Information*.

Further, the policy and procedures address the documentation that is required to be maintained in relation to the transfer of backed-up records of personal health information to the third party service provider for secure retention. In particular, the policy and procedures require the agents responsible for ensuring the secure transfer to document the date, time and mode of transfer and to maintain a repository of written confirmations received from the third party service provider upon receipt of the backed-up records of PHI.

Also, where a third party service provider is contracted to retain backed-up records of personal health information, the policy and procedures requires that a written agreement be executed with the third

party service provider containing the relevant language from the Third Party Services Agreement template and identify the agent(s) responsible for ensuring that the agreement has been executed prior to transferring the backed-up records of PHI to the third party service provider.

The policy and procedures further address the need for the availability of backed-up records of personal health information, including the circumstances in which the backed-up records are required to be made available.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and procedures will be audited and identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

14. Policy and Procedures on the Acceptable Use of Technology

OICR's *Acceptable Use* policy and procedures has been implemented outlining the acceptable use of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by OTB.

The policy and procedures set out the uses that are prohibited without exception, the uses that are permitted without exception and the uses that are permitted only with prior approval.

For those uses that are permitted only with prior approval, the policy and procedures identify the agents responsible for receiving, reviewing and determining whether to approve or deny the request and the process that must be followed and the requirements that must be satisfied in this regard. This includes a discussion of any documentation that must be completed; the agent(s) responsible for completing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request are also identified.

The policy and procedures also identify the conditions or restrictions with which agents granted approval must comply.

The policy and procedures also set out the manner in which the decision approving or denying the request and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited by the Privacy Officer and Information Security Officer, at

a minimum every 2 years, in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

15. Policy and Procedures in Respect of a Security and a Privacy Audit

OICR, in respect of OTB, requires agents to comply with the policies and its procedures and indicate that compliance will be enforced by the Privacy Officer and Information Security Officer and sets out the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*. The Information Security Officer will assume primary responsibility in ensuring regular and timely completion of security audits.

Scheduled Audits:

- Quarterly account review of active directory (AD) and lightweight directory access protocol (LDAP): To verify that only active employees have active accounts.
- Quarterly computer domain account (AD) audit: To ensure that only current user's computers are connected to the AD domain.
- Quarterly review Unix server log on failure: To analyze logs and investigate anything unusual.
- Quarterly network port scans: To compare the previous port scan to the current port scan. If new ports are opened further investigation is required.
- Annual inspection: Annual inspection of all workstations to confirm OICR root account is installed and active, and that any machines not owned and managed by OICR are removed from the OICR network.
- Monthly Internet use inspection: Analysis of Websense logs.
- Weekly inspection: No less than weekly, security event logs on the active directory are monitored for log on failures. Further investigation is undertaken should something unusual be noticed.

IT Systems Administrators will be responsible for direct review of relevant logs, conduct of the audits, and documentation of the security audit.

The policy and procedures also require agents to notify OICR at the first reasonable opportunity, in accordance with the *Information Security Program*, if an agent breaches or believes that there may have been a breach of this policy or its associated procedures.

OICR's *Policy and Procedures in Respect of a Security and a Privacy Audit* has been implemented that sets out the types of security audits that are required to be conducted. The audits required to be conducted include audits to assess compliance with the security policies, procedures and practices implemented by OTB; threat and risk assessments; security reviews or assessments; vulnerability assessments; penetration testing; ethical hacks and reviews of system control and audit logs.

With respect to each security audit that is required to be conducted, the policy and procedures set out the purposes of the security audit; the nature and scope of the security audit; the agent(s) responsible for conducting the security audit; and the frequency with which and the circumstances in which each security audit is required to be conducted. In this regard, the policy and procedures require a security audit schedule to be developed and identify the agent(s) responsible for developing the security audit schedule.

For each type of security audit that is required to be conducted, the policy and procedures also set out the process to be followed in conducting the audit. This includes the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided. The policy and procedures further discuss the documentation that must be completed, provided and/or executed in undertaking each security audit; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The role of the Privacy Officer and Information Security Officer who have been delegated day-to-day authority to manage the privacy program and the security program are also identified.

The policy and procedures also set out the process that must be followed in addressing the recommendations arising from security audits, including the agents responsible for assigning other agents to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations.

The policy and procedures also set out the nature of the documentation that must be completed at the conclusion of the security audit, including the agents responsible for completing, providing and/or executing, the documentation, the required content of the documentation and the agents to whom the documentation must be provided.

The policy and procedures also address the manner and format in which the findings of security audits, including the recommendations arising from the security audits and the status of addressing the recommendations, are communicated. This includes a discussion of the agent(s) responsible for communicating the findings of the security audit; the mechanism and format for communicating the findings of the security audit; the time frame within which the findings of the security audit must be communicated; and to whom the findings of the security audit will be communicated, including the President and Scientific Director.

The policy and procedures further require that a log be maintained of security audits and identify the agents responsible for maintaining the log and for tracking that the recommendations arising from the security audits are addressed within the identified time frame. They further address where documentation related to security audits will be retained and the agents responsible for retaining this documentation.

The policy and procedures also require the agents responsible for conducting the security audit to notify OICR, at the first reasonable opportunity, of an information security breach or suspected information security breach and of a privacy breach or suspected privacy breach in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*.

16. Log of Security Audits

OICR, in respect of OTB, maintains a log of security audits that have been completed. The log sets out 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.

17. Policy and Procedures for Information Security and Privacy Breach Management

Policy and Procedures in Respect of a Security and a Privacy Audit has been implemented to address the identification, reporting, containment, notification, investigation and remediation of information security breaches and provides a definition of the term “information security breach.” An information security breach is defined to include a contravention of the security policies, procedures or practices implemented by OICR .

The policy and procedures impose a mandatory requirement on agents to notify OTB of an information security breach or suspected information security breach.

In this regard, the policy and procedures identify the agents who must be notified of the information security breach or suspected information security breach and provide contact information for the Privacy Officer and Information Security Officer who must be notified. The policy and procedures further stipulate the time frame within which notification must be provided, whether the notification must be provided verbally and/or in writing and the nature of the information that must be provided upon notification. The policy and procedures also address the documentation that must be completed, provided and/or executed with respect to notification; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

Upon notification, the policy and procedures require a determination to be made of whether an information security breach has in fact occurred, and if so, what personal health information has been breached. A determination shall further be made of the extent of the information security breach and whether the breach is an information security breach or privacy breach or both. The agents responsible for making these determinations are also identified.

The policy and procedures address the process to be followed where the breach is a privacy breach as well as an information security breach and when the breach is reported as an information security breach but is determined to be a privacy breach.

The policy and procedures address when senior management, including the President and Scientific Director, will be notified. This includes a discussion of the agents responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.

The policy and procedures also require that containment be initiated immediately and identify the agents responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach and the required content of the documentation. In undertaking containment, the policy and procedures ensure that reasonable steps are taken in the circumstances to ensure that additional information security beaches cannot occur through the same means.

The agents responsible and the process to be followed in reviewing the containment measures implemented and determining whether the information security breach has been effectively contained or whether further containment measures are necessary are identified in the policy and procedures. The policy and procedures also address any documentation that must be completed, provided and/or executed by the agent(s) responsible for reviewing the containment measures; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures require the health information custodian or other organization that disclosed the personal health information to OTB to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization.

In particular, the policy and procedures establishes that the Privacy Officer is responsible for notifying the health information custodian or other organization, and sets out the format of the notification and the nature of the information that will be provided upon notification. The policy and procedures require the health information custodian or other organization to be advised of the extent of the information security breach; the nature of the personal health information at issue, if any; the measures implemented to contain the information security breach; and further actions that will be undertaken with respect to the information security breach, including investigation and remediation.

The policy and procedures also set out whether any other persons or organizations must be notified of the information security breach and set out the agents responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification.

The policy and procedures further identify the Privacy Officer and Information Security Officer as responsible for investigating the information security breach, the nature and scope of the investigation (i.e., document reviews, interviews, site visits, and inspections) and the process that must be followed in investigating the information security breach. This includes a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for

completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program has also been identified.

The policy and procedures also identify the agents responsible for assigning other agents to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines. The policy and procedures also set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the information security breach, including the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also address the manner and format in which the findings of the investigation of the information security breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This includes a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the President and Scientific Director.

Further, the policy and procedures require that a log be maintained of information security breaches and identify the agents responsible for maintaining the log and for tracking that the recommendations arising from the investigation of information security breaches are addressed within the identified timelines. They further address where documentation related to the identification, reporting, containment, notification, investigation and remediation of information security breaches are retained and the agents responsible for retaining this documentation.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and procedures will be audited and identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

18. Log of Security Breaches

OICR, in respect of OTB, maintains a log of information security breaches setting out:

- The date of the information security breach;
- The date that the information security breach was identified or suspected;
- The nature of the personal health information, if any, that was the subject matter of the information security breach and the nature and extent of the information security breach;

- The date that the information security breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to OICR was notified, if applicable;
- The date that the investigation of the information security breach was completed;
- The agent(s) responsible for conducting the investigation;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

PART 3 – HUMAN RESOURCES DOCUMENTATION

1. Policy and Procedures for Privacy Training and Awareness

OICR has developed and implemented a policy requiring its agents to attend initial privacy and security awareness training upon hiring as well as ongoing privacy awareness training.

OICR's *Privacy and Information Security Training and Awareness Policy* sets out the time frame within which agents must complete the initial privacy orientation as well as address the frequency of ongoing privacy training. The policy and procedures requires all agents newly employed or engaged by OICR, including scientists, adjunct scientists, fellows, students and volunteers, to receive privacy and information security training at the commencement of their employment or prior to being given access to research data, including personal health information and to attend ongoing privacy training provided by OICR on an annual basis.

The OICR's Privacy Officer and Information Security Officer are responsible for preparing and delivering the initial privacy orientation and ongoing privacy training. The policy and procedures further set out the process that must be followed in notifying the Privacy Officer and Information Security Officer the agents responsible for preparing and delivering the initial privacy orientation when an agent has commenced or will commence an employment, contractual or other relationship with OTB. This includes a discussion of the managers responsible for providing notification, the time frame within which notification must be provided and the format of the notification.

The policy and procedures also identify the content of the initial privacy orientation to ensure that it is formalized and standardized. The content of the initial privacy and security orientation includes:

- A description of the status of OTB under the Act and the duties and responsibilities that arise as a result of this status;
- A description of the nature of the personal health information collected and from whom this information is typically collected;
- An explanation of the purposes for which personal health information is collected and used and how this collection and use is permitted by the Act and its regulation;
- Limitations placed on access to and use of personal health information by agents;
- A description of the procedure that must be followed in the event that an agent is requested to disclose personal health information;
- An overview of the privacy policies, procedures and practices that have been implemented by OTB and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the privacy policies, procedures and practices implemented;
- An explanation of the privacy program, including the key activities of the program and the agent(s) that have been delegated day-to-day authority to manage the privacy program;
- The administrative, technical and physical safeguards implemented by OTB to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;

- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by OTB;
- A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute and the key provisions of the Confidentiality Agreement; and
- An explanation of the Policy and Procedures for Information Security and Privacy Breach Management and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches.

The policy and procedures also require the ongoing privacy training to be formalized and standardized: to include role-based training in order to ensure that agents understand how to apply the privacy policies, procedures and practices in their day-to-day employment, contractual or other responsibilities; to address any new privacy policies, procedures and practices and significant amendments to existing privacy policies, procedures and practices; and to have regard to any recommendations with respect to privacy training made in privacy impact assessments, privacy audits and the investigation of privacy breaches and privacy complaints.

The policy and procedures require that a log be maintained to track attendance at the initial privacy orientation as well as the ongoing privacy training and the policy and procedures identify Human Resources as responsible for maintaining such a log and tracking attendance.

The process to be followed in tracking attendance at the initial privacy orientation as well as the ongoing privacy training is also outlined, including the documentation that must be completed to verify attendance; the agents responsible for completing, providing and/or executing the documentation; the agent to whom this documentation must be provided; and the required content of the documentation. The procedure to be followed when HR identifies agents who do not attend the initial privacy orientation or the ongoing privacy training and for ensuring that such agents attend the initial privacy orientation and the ongoing privacy training is also identified, including the time frame following the date of the privacy orientation or the ongoing privacy training within which this procedure must be implemented.

The policy and procedures indicate that documentation related to attendance at the initial privacy orientation and the ongoing privacy training is to be retained by Human Resources.

The policy and procedures also discuss the other mechanisms implemented by OICR to foster a culture of privacy and to raise awareness of the privacy program and the privacy policies, procedures and practices implemented. The policy and procedures also discuss the frequency with which OICR communicates with its agents in relation to privacy, the method and nature of the communication and the agents responsible for the communication.

OICR requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and procedures will be audited and

identify the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

This policy and procedures is combined with the *Privacy and Information Security Training and Awareness*.

2. Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training

OICR, in respect of OTB, maintains a log of the attendance of agents at initial privacy awareness training, ongoing privacy training and special training sessions. The log sets out the name of the agent, the date that the agent attended the initial privacy orientation and the dates that the agent attended ongoing privacy training.

3. Policy and Procedures for Security Training and Awareness

OICR has developed and implemented a policy requiring its agents to attend initial security awareness training upon hiring as well as ongoing security awareness training.

The *Privacy and Information Security Training and Awareness Policy* sets out the time frame within which agents must complete the initial security orientation as well as address the frequency of ongoing security training. The policy and procedures require all agents newly employed or engaged by OICR, including scientists, adjunct scientists, fellows, students and volunteers, to receive security and information security training at the commencement of their employment or prior to being given access to research data, including personal health information and to attend ongoing security training provided by OICR on an annual basis.

The OICR's Privacy Officer and Information Security Officer are responsible for preparing and delivering the initial security orientation and ongoing security training. The policy and procedures further set out the process that must be followed in notifying the Privacy Officer and Information Security Officer, the agents responsible for preparing and delivering the initial security orientation when an agent has commenced or will commence an employment, contractual or other relationship with OTB. This includes a discussion of the managers responsible for providing notification, the time frame within which notification must be provided and the format of the notification.

The policy and procedures also identify the content of the initial security orientation to ensure that it is formalized and standardized. The content of the initial privacy and security orientation includes:

- An overview of the security policies, procedures and practices that have been implemented by OTB and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the security policies, procedures and practices implemented;

- An explanation of the security program, including the key activities of the program and the agent(s) that have been delegated day-to-day authority to manage the security program;
- The administrative, technical and physical safeguards implemented by OTB to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;
- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by OTB; and
- An explanation of the *Policy and Procedures for Information Security and Privacy Breach Management* and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.

The policy and procedures also require the ongoing security training to be formalized and standardized; to include role-based training in order to ensure that agents understand how to apply the security policies, procedures and practices in their day-to-day employment, contractual or other responsibilities; to address any new security policies, procedures and practices and significant amendments to existing security policies, procedures and practices; and to have regard to any recommendations with respect to security training made in privacy impact assessments, the investigation of information security breaches and the conduct of security audits including threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs.

The policy and procedures require that a log be maintained to track attendance at the initial security orientation as well as the ongoing security training and the policy and procedures identify Human Resources as responsible for maintaining such a log and tracking attendance.

The process to be followed in tracking attendance at the initial security orientation as well as the ongoing security training are also be outlined, including the documentation that must be completed, provided and/or executed to verify attendance; the agents responsible for completing, providing and/or executing the documentation; the agent to whom this documentation must be provided; and the required content of the documentation. The procedure to be followed and the agents responsible for identifying agents who do not attend the initial security orientation or the ongoing security training and for ensuring that such agents attend the initial security orientation and the ongoing security training are also be identified, including the time frame following the date of the security orientation or the ongoing security training within which this procedure must be implemented.

The policy and procedures indicate that documentation related to attendance at the initial security orientation and the ongoing security training is to be retained by Human Resources.

The policy and procedures also discuss the other mechanisms implemented by OTB to raise awareness of the security program and the security policies, procedures and practices implemented. The policy and procedures also discuss the frequency with which OICR communicates with its agents in relation to

security, the method and nature of the communication and the agents responsible for the communication.

OICR requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and procedures will be audited and identify the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Information Security Incident Response*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

This policy and procedures is combined with the P*rivacy and Information Security Training and Awareness Policy*.

4. Log of Attendance at Initial Security Orientation and Ongoing Security Training

OICR, in respect of OTB, maintains a log of the attendance of agents at initial security awareness training, ongoing security training and special training sessions. The log sets out the name of the agent, the date that the agent attended the initial security orientation and the dates that the agent attended ongoing security training.

5. Policy and Procedures for the Execution of Confidentiality Agreements by Agents

OICR has a *Confidentiality of Information Policy* and procedures requiring agents to execute a Confidentiality Agreement in accordance with the *Confidentiality of Information Policy* at the commencement of their employment, contractual or other relationship with OTB and prior to being given access to personal health information, and on an annual basis.

The policy and procedures further identify the agents responsible for ensuring that a Confidentiality Agreement is executed with each agent of OTB at the commencement of the employment, contractual or other relationship.

In particular, the policy and procedures outline the process that must be followed in notifying the responsible agents each time an agent has commenced or will commence an employment, contractual or other relationship with OTB. This includes a discussion of the agents responsible for providing notification, the time frame within which notification must be provided and the format of the notification.

The policy and procedures also outline the process that must be followed by the responsible agents in tracking the execution of Confidentiality Agreements, including the process that must be followed

where an executed Confidentiality Agreement is not received within a defined period of time following the commencement of the employment, contractual or other relationship.

The policy and procedures also require that a log be maintained of executed Confidentiality Agreements are maintained by OICR Human Resources for OICR employees and OTB agent agreements are retained by OTB.

OTB requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance with the policy and its procedures and with the Confidentiality Agreement will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, set out the frequency with which the policy and its procedures will be audited and identify the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

6. Template Confidentiality Agreement with Agents

A Confidentiality Agreement must be executed by each agent of OTB in accordance with OICR's *Confidentiality of Information Policy* that addresses the matters set out below.

General Provisions

The OTB Confidentiality Agreement describes the status of OTB under the Act and the duties and responsibilities arising from this status. It also states that individuals executing the agreement are agents of the OTB in respect of personal health information and outlines the responsibilities associated with this status.

The Confidentiality Agreement also requires agents to comply with the provisions of the Act and its regulation relating OTB and with the terms of the Confidentiality Agreement as may be amended from time to time.

Agents are also required to acknowledge that they have read, understood and agree to comply with the privacy and security policies, procedures and practices implemented by OTB and to comply with any privacy and security policies, procedures and practices as may be implemented or amended from time to time following the execution of the Confidentiality Agreement.

The Confidentiality Agreement provides a definition of personal health information and the definition provided is consistent with the Act and its regulation.

Obligations with Respect to Collection, Use and Disclosure of Personal Health Information

The OTB Confidentiality Agreement identifies the purposes for which agents are permitted to collect, use and disclose personal health information on behalf of OICR and any limitations, conditions or restrictions imposed thereon.

In identifying the purposes for which agents are permitted to collect, use or disclose personal health information, OTB ensures that each collection, use or disclosure identified in the Confidentiality Agreement is permitted by the Act and its regulation. In this regard, the Confidentiality Agreement prohibits agents from collecting and using personal health information except as permitted in the Confidentiality Agreement and from disclosing such information except as permitted in the Confidentiality Agreement or as required by law.

Further, the Confidentiality Agreement prohibits agents from collecting, using or disclosing personal health information if other information will serve the purpose and from collecting, using or disclosing more personal health information than is reasonably necessary to meet the purpose.

Termination of the Contractual, Employment or Other Relationship

The OTB Confidentiality Agreement requires agents to securely return all property of OTB, including records of personal health information and all identification cards, access cards and/or keys, on or before the date of termination of the employment, contractual or other relationship in accordance with the policy on *Employees Departing OICR.* The Confidentiality Agreement also stipulates the time frame within which the property of OICR must be securely returned, the secure manner in which the property must be returned and the agent to whom the property must be securely returned.

Notification

The OTB Confidentiality Agreement requires agents to notify OICR at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security and Privacy Breach Management*, if the agent breaches or believes that there may have been a breach of the Confidentiality Agreement or if the agent breaches or believes that there may have been a breach of the privacy or security policies, procedures and practices implemented by OTB.

Consequences of Breach and Monitoring Compliance

The OTB Confidentiality Agreement outlines the consequences of breach of the agreement and addresses the manner in which compliance with the Confidentiality Agreement will be enforced. The Confidentiality Agreement further stipulates that compliance with the Confidentiality Agreement will be audited and addresses the manner in which compliance will be audited.

7. Log of Executed Confidentiality Agreements with Agents

OICR, in respect of OTB, maintains a log of Confidentiality Agreements that have been executed by agents at the commencement of their employment, contractual or other relationship with OTB and on an annual basis. The log includes the name of the agent, the date of commencement of the employment, contractual or other relationship with OTB and the dates that the Confidentiality Agreements were executed.

8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Policy

A job description for the position of Privacy Officer that has been delegated day-to-day authority to manage the privacy program on behalf of OTB has been developed.

The job description sets out the reporting relationship of the Privacy Officer that has been delegated day-to-day authority to manage the privacy program to the President and Scientific Director. The job description also identifies the responsibilities and obligations of the Privacy Officer in respect of the privacy program. These responsibilities and obligations include:

- Developing, implementing, reviewing and amending privacy policies, procedures and practices;
- Ensuring compliance with the privacy policies, procedures and practices implemented;
- Ensuring transparency of the privacy policies, procedures and practices implemented;
- Facilitating compliance with the Act and its regulation;
- Ensuring agents are aware of the Act and its regulation and their duties thereunder;
- Ensuring agents are aware of the privacy policies, procedures and practices implemented by OICR and are appropriately informed of their duties and obligations thereunder;
- Directing, delivering or ensuring the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy;
- Conducting, reviewing and approving privacy impact assessments;
- Receiving, documenting, tracking, investigating, remediating and responding to privacy complaints pursuant to the *Policy and Procedures for Privacy Complaints*;
- Receiving and responding to privacy inquiries pursuant to the *Policy and Procedures for Privacy Inquiries*;
- Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the *Policy and Procedures for Information Security and Privacy Breach Management;* and
- Conducting privacy audits pursuant to the *Policy and Procedures in Respect of a Security and a Privacy Audit*.

9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program

A job description for the Director IT and Information Security Officer that has been delegated day-to-day authority to manage the security program on behalf of OTB has been developed.

The job description sets out the reporting relationship of the Director IT and Information Security Officer that has been delegated day-to-day authority to manage the security program to the President and Scientific Director. The job description also identifies the responsibilities and obligations of the position in respect of the security program. These responsibilities and obligations include:

- Developing, implementing, reviewing and amending security policies, procedures and practices;
- Ensuring compliance with the security policies, procedures and practices implemented;
- Ensuring agents are aware of the security policies, procedures and practices implemented by OICR and are appropriately informed of their duties and obligations thereunder;
- Directing, delivering or ensuring the delivery of the initial security orientation and the ongoing security training and fostering a culture of information security awareness;

- Receiving, documenting, tracking, investigating and remediating information security breaches or suspected information security breaches pursuant to the Policy and Procedures for Information Security and Privacy Breach Management; and
- Conducting security audits pursuant to the *Policy and Procedures in Respect of a Security and a Privacy Audit*.

10. Policy and Procedures for Termination or Cessation of Employment or Contractual Relationship

The *Termination Policy* in concert with the *Progressive Discipline Policy* and policy and procedures for *Employees Departing OICR* requires agents, as well as their supervisors, to notify OTB of the termination of the employment, contractual or other relationship. The policy and procedures identify the agents to whom notification must be provided, the nature and format of the notification, the time frame within which notification must be provided and the process that must be followed in providing notification.

The policies and its procedures also require agents to securely return all property of OTB on or before the date of termination of the employment, contractual or other relationship. In this regard, a definition of property is provided in the policy and procedures and this definition includes records of personal health information, identification cards, access cards and/or keys.

The policies and procedures identify the agent to whom the property must be securely returned; the secure method by which the property must be returned; the time frame within which the property must be securely returned; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation. The procedures to be followed in the event that the property of OTB is not securely returned upon termination of the employment, contractual or other relationship is also addressed, including the agent(s) responsible for implementing the procedure and the time frame following termination within which the procedure must be implemented.

The policies and procedures also require that access to the premises OICR, to locations within the premises where records of personal health information are retained and to the information technology operational environment, be immediately terminated upon the cessation of the employment, contractual or other relationship. The policy and procedures identify the agent responsible for terminating access; the procedure to be followed in terminating access; the time frame within which access must be terminated; the documentation that must be completed, provided and/or executed and the agents responsible for completing, providing and/or executing the documentation.

OTB requires agents to comply with the policies and procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit*, sets out the frequency with which the policy and procedures will be audited and identifies the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policies and procedures also require agents to notify OTB at the first reasonable opportunity, in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

11. Policy and Procedures for Discipline and Corrective Action

OICR, in respect of OTB, has implemented a policy and associated procedures for discipline and corrective action in respect of personal health information.

The *Progressive Discipline* policy and procedures addresses the investigation of disciplinary matters, including the persons (namely human resources and manager) responsible for conducting the investigation; the procedure that must be followed in undertaking the investigation; any documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the required content of the documentation; and the agent(s) to whom the results of the investigation must be reported.

The types of discipline that may be imposed by OICR and the factors that must be considered in determining the appropriate discipline and corrective action is also set out in the policy and procedures. The agent(s) responsible for determining the appropriate discipline and corrective action, the procedure to be followed in making this determination, the agent(s) that must be consulted in making this determination; and the documentation that must be completed, provided and/or executed, are also identified.

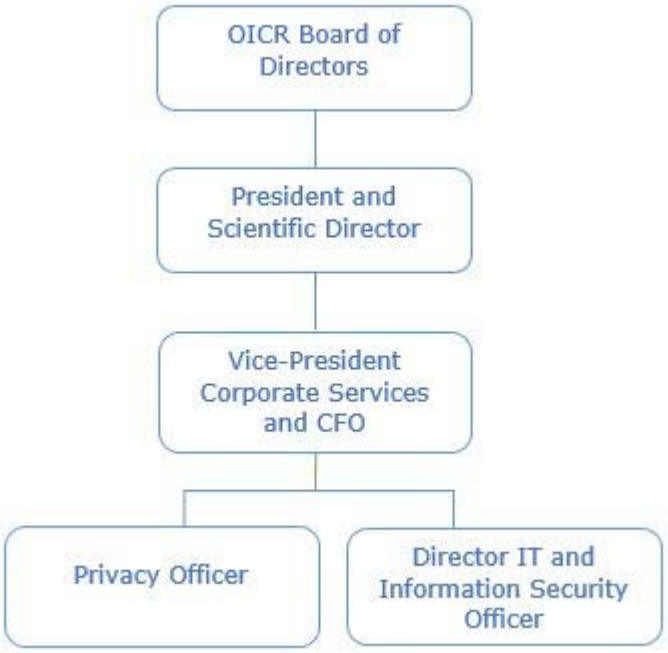
The policy and procedures address the retention of documentation related to the discipline and corrective action taken, including where this documentation will be retained and the agent(s) responsible for retaining the documentation.

PART 4 – ORGANIZATIONAL AND OTHER DOCUMENTATION

1. Privacy Governance and Accountability Framework

A privacy governance and accountability framework for ensuring compliance with the Act and its regulation and for ensuring compliance with the privacy policies, procedures and practices implemented by OICR has been established.

The *OICR Privacy and Information Security Accountability Terms of Reference* stipulates that the President and Scientific Director is ultimately accountable for ensuring that OICR and its agents comply with the Act and its regulation and comply with the privacy policies, procedures and practices implemented.



*Co-Chairs of an Information Governance Committee which has been established to ensure that OICR meets its commitments with respect to privacy and security.

The Privacy Officer and Information Security Officer have been delegated day-to-day authority to manage the privacy program as identified in the OICR Privacy and Information Security Accountability Terms of Reference. This document also describes the nature of the reporting relationship to the President and Scientific Director of OICR. This privacy governance and accountability framework also identifies the other individuals, committees and teams that support the Privacy Officer and Information

Security Officer in managing the privacy program and sets out their roles in respect of the privacy program.

The role of the Board of Directors in respect of the privacy program is also addressed. The privacy governance and accountability framework also sets out the frequency with which and the method and manner by which the Board of Directors is updated with respect to the privacy program, the agents responsible for providing such updates and the matters with respect to which the Board of Directors is required to be updated.

The update provided to the Board of Directors, is done on an "as necessary" basis and addresses the initiatives undertaken by the privacy program including privacy training and the development and implementation of privacy policies, procedures and practices. It also includes a discussion of the privacy audits and privacy impact assessments conducted, including the results of and recommendations arising from the privacy audits and privacy impact assessments and the status of implementation of the recommendations. The Board of Directors is also advised of any privacy breaches and privacy complaints that were investigated, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations.

The privacy governance and accountability framework is accompanied by a privacy governance organizational chart as depicted above.

The privacy governance and accountability framework also sets out the manner in which the privacy governance and accountability framework will be communicated to agents of OTB, the method by which it will be communicated and the agents responsible for this communication.

This privacy governance and accountability framework is combined with the security governance and accountability framework.

2. Security Governance and Accountability Framework

A security governance and accountability framework for ensuring compliance with the Act and its regulation and for ensuring compliance with the security policies, procedures and practices implemented by OTB has been established.

The OICR *Privacy and Information Security Accountability Terms of Reference* stipulates that the President and Scientific Director is ultimately accountable for ensuring the security of personal health information and for ensuring that OICR and its agents comply with the security policies, procedures and practices implemented.

The Director IT and Information Security Officer has been delegated day-to-day authority to manage the security program and has been identified in the security governance and accountability framework. The nature of the reporting relationship to the President and Scientific Director is described. The security governance and accountability framework also sets out the responsibilities and obligations of the positions that have been delegated day-to-day authority to manage the security program and identify

the other individuals, committees and teams that support the positions that have been delegated day-to-day authority to manage the security program and their role in respect of the security program.

The role of the Board of Directors in respect of the security program is also addressed. The security governance and accountability framework also sets out the frequency with which and the method and manner by which the Board of Directors is updated with respect to the security program, the agents responsible for providing such updates and the matters with respect to which the Board of Directors is required to be updated. The Board of Directors is updated as needed.

The update provided to the Board of Directors addresses the initiatives undertaken by the security program including security training and the development and implementation of security policies, procedures and practices. It also includes a discussion of the security audits conducted, including the results of and recommendations arising from the security audits and the status of implementation of the recommendations. The Board of Directors is also advised of any information security breaches investigated, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations. The security governance and accountability framework is combined with the privacy governance and accountability framework as depicted in Part 4, Section 1 above.

The security governance and accountability framework also sets out the manner in which the security governance and accountability framework will be communicated to agents of OTB, the method by which it will be communicated and the agents responsible for this communication.

3. Terms of Reference for Committees with Roles with Respect to the Privacy Policy and/or Security Program

OICR has established a terms of reference for each committee that has a role in respect of the privacy and/or the security program. For each committee, the terms of reference identifies the membership of the committee, the chair of the committee, the mandate and responsibilities of the committee in respect of the privacy and/or the security program and the frequency with which the committee meets. The terms of reference also set out to whom the committee reports; the types of reports produced by the committee, if any; the format of the reports; to whom these reports are presented; and the frequency of these reports.

4. Corporate Risk Management Framework

OICR has developed a comprehensive and integrated corporate risk management framework to identify, assess, mitigate and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

The *OICR Corporate Risk Management Policy* addresses the agents responsible and the process that must be followed in identifying risks that may negatively affect the ability of OICR to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. This includes a discussion of the agents or other persons or organizations that must be

consulted in identifying the risks; the documentation that must be completed, provided and/or executed; the agents responsible for completing, providing and/or executing the documentation; the agents to whom this documentation must be provided; and the required content of the documentation. It also addresses the agents responsible, the process that must be followed and the criteria that must be considered in ranking the risks and assessing the likelihood of the risks occurring and the potential impact if they occur. This includes a discussion of the agents or other persons or organizations that must be consulted in assessing and ranking the risks; the documentation that must be completed in assessing and ranking the risks; the documentation that must be completed in setting out the rationale for the assessment and ranking of the risks; the agents responsible for completing, providing and/or executing the documentation; the agents to whom this documentation must be provided; and the required content of the documentation.

The document also identifies the agents responsible, the process that must be followed and the criteria that must be considered in identifying strategies to mitigate the actual or potential risks to privacy that were identified and assessed, the process for implementing the mitigation strategies and the agents or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies.

This includes identifying the agents responsible for assigning other agents to implement the mitigation strategies, for establishing timelines to implement the mitigation strategies, and for monitoring and ensuring that the mitigation strategies have been implemented. The corporate risk management framework further addresses the documentation that must be completed in identifying, implementing, monitoring and ensuring the implementation of the mitigation strategies; the agents responsible for completing the documentation; the agents to whom this documentation must be provided; and the required content of the documentation.

The document also addresses the manner and format in which the results of the corporate risk management process, including the identification and assessment of risks, the strategies to mitigate actual or potential risks to privacy and the status of implementation of the mitigation strategies, are communicated and reported. This involves identifying the agents responsible for communicating and reporting the results of the corporate risk management process, the nature and format of the communication; and to whom the results will be communicated and reported, including to the President and Scientific Director. Approval and endorsement of the results of the risk management process, including the agents responsible for approval and endorsement, is also outlined.

Further, the document requires that a corporate risk register be maintained and that the corporate risk register be reviewed on an ongoing basis in order to ensure that all the risks that may negatively affect the ability of OICR to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information continue to be identified, assessed and mitigated.

The frequency with which the corporate risk register must be reviewed and the agent(s) responsible and the process that must be followed in reviewing and amending the corporate risk register is also identified.

The manner in which the corporate risk management framework is integrated into the policies, procedures and practices of OICR and into the projects undertaken by OICR and the agents responsible for integration is also addressed.

5. Corporate Risk Register

OICR has a corporate risk register that identifies each risk that may negatively affect the ability of OICR to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. For each risk identified, the corporate risk register includes an assessment of the risk, a ranking of the risk, the mitigation strategy to reduce the likelihood of the risk occurring and/or to reduce the impact of the risk if it does occur, the date that the mitigation strategy was implemented or is required to be implemented, and the agents responsible for implementation of the mitigation strategy.

6. Policy and Procedures for Maintaining a Consolidated Log of Recommendations

OICR, in respect of OTB, has implemented a *Policy and Procedures for Maintaining a Consolidated Log of Recommendations* requiring a consolidated and centralized log to be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits and the investigation of privacy breaches, privacy complaints and security breaches. The consolidated and centralized log also includes recommendations made by the Information and Privacy Commissioner of Ontario that have been addressed by OTB prior to the next review of its practices and procedures.

The *Policy and Procedures for Maintaining a Consolidated Log of Recommendations* sets out the frequency with which and the circumstances in which the consolidated and centralized log must be reviewed, the agents responsible for reviewing and amending the log and the process that must be followed in this regard. The log is updated each time that a privacy impact assessment, privacy audit, security audit, investigation of a privacy breach, investigation of a privacy complaint, investigation of an information security breach or review by the Information and Privacy Commissioner of Ontario is completed and each time that a recommendation has been addressed. The consolidated and centralized log be reviewed on an ongoing basis in order to ensure that the recommendations are addressed in a timely manner.

OICR, in respect of OTB, requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of a Security and a Privacy Audit* and set out the frequency with which the policy and procedures will be audited and the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify OTB at the first reasonable opportunity in accordance with its *Policy and Procedures for Information Security and Privacy Breach Management* if an agent breaches or believes there may have been a breach of this policy or its procedures.

7. Consolidated Log of Recommendations

OICR, in respect of OTB, maintains a consolidated and centralized log of all recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches and reviews by the Information and Privacy Commissioner of Ontario.

In particular, the log sets out the name and date of the document, investigation, audit and/or review from which the recommendation arose. For each recommendation, the log sets out the recommendation made, the manner in which the recommendation was addressed or is proposed to be addressed, the date that the recommendation was addressed or by which it is required to be addressed, and the agent(s) responsible for addressing the recommendation.

8. Business Continuity and Disaster Recovery Plan

A policy and associated procedures has been developed and implemented to protect and ensure the continued availability of the information technology environment of OICR in the event of short and long-term business interruptions and in the event of threats to the operating capabilities of OICR, including natural, human, environmental and technical interruptions and threats.

The *Business Continuity Plan – Ontario Tumour Bank* in concert with the OICR policy on *Disaster Recovery and Offsite Data Storage* (collectively, the "BCP") addresses notification of the interruption or threat, documentation of the interruption or threat, assessment of the severity of the interruption or threat, activation of the business continuity and disaster recovery plan and recovery of personal health information.

In relation to notification of the interruption or threat, the BCP identifies the agents as well as the other persons or organizations that must be notified of short and long-term business interruptions and threats to the operating capabilities of OICR and the agents responsible for providing such notification. The business continuity and disaster recovery plan also addresses the time frame within which notification will be provided, the manner and format of notification, the nature of the information that will be provided upon notification and any documentation that will be completed, provided and/or executed.

In this regard, a contact list has been developed and maintained of all agents, service providers, stakeholders and other persons or organizations that will be notified of business interruptions and threats and the business continuity and disaster recovery plan will identify the agents responsible for creating and maintaining this contact list.

In relation to the assessment of the severity level of the interruption or threat, the business continuity and disaster recovery plan identifies the agents responsible for the assessment, the criteria pursuant to which this assessment is to be made and the agents and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat. It also addresses the

documentation that must be completed, provided and/or executed resulting from or arising out of this assessment; the required content of the documentation; the agents to whom the documentation must be provided; and to whom the results of this assessment must be reported.

In relation to the assessment of the interruption or threat, the BCP sets out the agents responsible and the process that must be followed in conducting an initial impact assessment of the interruption or threat, including its impact on the technical and physical infrastructure and business processes of OICR. This includes the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be utilized in conducting the assessment; the documentation that must be completed, provided and/or executed; the agents responsible for completing, providing and/or executing the documentation; the agents to whom the documentation must be provided; and the agents to whom the results of the initial impact assessment must be communicated.

The BCP further identifies the agents responsible for conducting and preparing a detailed damage assessment in order to evaluate the extent of the damage caused by the threat or interruption and the expected effort required to resume, recover and restore infrastructure elements, information systems and/or services. It further addresses the manner in which the assessment is required to be conducted; the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be considered in undertaking the assessment; the documentation that must be completed, provided and/or executed; the agents responsible for completing, providing and/or executing the documentation; the agents to whom the documentation must be provided; and the agents to whom the results of the assessment must be communicated.

The BCP also identifies the agents responsible for resumption and recovery, the procedure that must be utilized in resumption and recovery for each critical application and business function, the prioritization of resumption and recovery activities, the criteria pursuant to which the prioritization of resumption and recovery activities is determined, and the recovery time objectives for critical applications. This includes a discussion of the agents and other persons or organizations that are required to be consulted with respect to resumption and recovery activities; the documentation that must be completed, provided and/or executed; the required content of the documentation; the agents responsible for completing, providing and/or executing the documentation; the agents to whom the documentation must be provided; and the agents to whom the results of these activities must be communicated.

In this regard, the BCP requires that an inventory be developed and maintained of all critical applications and business functions and of all hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and network settings for firewalls, routers, domain name servers, email servers and the like. The business continuity and disaster recovery plan further identify the agents responsible for developing and maintaining the inventory, the agents and other persons and organizations that must be consulted in developing the inventory, and the criteria upon which the determination of critical applications and business functions must be made.

The procedure by which decisions made and actions taken during business interruptions and threats to the operating capabilities of OICR will be documented and communicated and by whom and to whom they will be communicated must also be discussed.

The BCP also addresses the testing, maintenance and assessment of the business continuity and disaster recovery plan. This includes identifying the frequency of testing; the agents responsible for ensuring that the business continuity and discovery plan is tested, maintained and assessed; the agents responsible for amending the business continuity and discovery plan as a result of the testing; the procedure to be followed in testing, maintaining, assessing and amending the business continuity and discovery plan; and the agents responsible for approving the business continuity and disaster recovery plan and any amendments thereto.

The BCP further addresses the agents responsible and the procedure to be followed in communicating the business continuity and disaster recovery plan to all agents, including any amendments thereto, and the method and nature of the communication. The agents responsible for managing communications in relation to the threat or interruption will also be identified, including the method and nature of the communication.

PRIVACY, SECURITY AND OTHER INDICATORS

Part 1 – Privacy Indicators

Categories	Privacy Indicators	OICR
General Privacy Policies, Procedures and Practices	The dates that the privacy policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.	**OICR Policies: (see Appendix D)** **OTB Policies:** Any changes are communicated in three ways each time: (1) verbal communication that modified policies are being shipped (via teleconference), (2) a physical mail-out of the modified documents along with a table of changes and instructions for removing old policies and inserting the new policies into the policy binder, and (3) the policies are changed on the OTB online "collaboration" website. Agents affected by the policies are further instructed to read the modified policies and log this on their training log. **OTB.POL801 – Ontario Tumour Bank Privacy Policy** 1) Reviewed and amended 2013-10-15 (major change): Added language on breach reporting. Added reference to 2 new forms: F-OTB.POL801-1, Privacy Breach Reporting – Ontario Tumour Bank and FOTB.POL801-2, Privacy Contacts – Ontario Tumour Bank. Updated privacy officer phone number. Implemented and communicated on December 10, 2014. 2) Reviewed and amended 2015-09-04: Re-Formatted Forms to attach as appendices. Separate Forms now obsolete. Updated 'Associated Forms' section of footer. Updated mailing address from 101 College St to new 661 University Ave. Updated Privacy Contacts to reflect changes. Implemented and communicated on December 3, 2015. 3) Reviewed 2016-08-11 (no change). **OTB.POL802 – Policy and Procedures for the Collection of Personal Health Information – Ontario Tumour Bank** 1) Reviewed on 2014-10-21, 2015-10-04 and 2016-08-11 (no change).

Categories	Privacy Indicators	OICR
		OTB.POL803 – Policy and Procedures for Data Access and Use – Ontario Tumour Bank 1) Reviewed on 2014-10-21, 2015-10-04 and 2016-08-11 (no change). **OTB.POL804 – Policy and Procedures for Data Disclosure – Ontario Tumour Bank** 1) Reviewed on 2014-10-21, 2015-10-04 and 2016-08-11 (no change). **OTB.POL805 – Policy and Procedures for Data Linkages – Ontario Tumour Bank** 1) Reviewed on 2014-10-21, 2015-10-04 and 2016-08-11 (no change). **OTB.POL806 – Business Continuity Plan – Ontario Tumour Bank** 1) New policy implemented and communicated on May 19, 2015. 2) Reviewed on 2015-10-04 (minor change): Contact information updated in appendix A. Implemented and communicated on December 3, 2015. 3) Reviewed on 2016-08-15 (minor change): Contact information updated in appendix A. Implemented and communicated on September 14, 2016. **TB312 – Material Request Release** 1) Reviewed on 2014-10-21 (no change). 2) Reviewed and amended on 2015-10-04 (major change): Updated OTB logo, overall grammatical clean-up and formatting. Updated sections 6.3 and 6.7 to remove DM and add SharePoint. Added section 6.8 procedures for customer satisfaction follow-up. Implemented and communicated December 3, 2015. 3) Reviewed on 2016-05-31 (minor change): F-TB312-02 Updated Tom Hudson's name with title "OICR President

Categories	Privacy Indicators	OICR
		and Scientific Director". Implemented and communicated on September 14, 2016. **DM502 – TissueMetrix Access and Configuration** 1) Reviewed on 2014-10-21 and 2015-10-12 (no change). 2) Reviewed and amended on 2016-09-14 (minor change): Updated OTB logo. Updated spelling of Supercedes to Supersedes. Added Form F-DM502-04 OTB Data Access Form – Vendors. Updated Section 6.1 to include staging database. Updated section 6.2.1 to include reference to the new Form F-DM502-04. Performed overall grammatical clean-up. Implemented and communicated on September 16, 2016. **TB311 – Physical Security of OTB Facilities** 1) Reviewed on 2014-10-21, 2015-10-12 and 2016-05-24 (no change).
	Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made	See above
	Whether new privacy policies and procedures were developed and implemented as a result of the	**<u>OICR Policies</u>: (see Appendix D)** **<u>OTB Policies:</u>** One new OTB policy was developed and implemented.

Categories	Privacy Indicators	OICR
	review, and if so, a brief description of each of the policies and procedures developed and implemented.	**OTB.POL806 – Business Continuity Plan – Ontario Tumour Bank** The purpose of this policy is to ensure the continued availability of the information technology environment of Ontario Tumour Bank in the event of short and long-term business interruptions and in the event of threats to the operating capabilities of OTB.
	The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.	**OICR Policies: (see Appendix D)** **OTB Policies:** Amended OTB privacy policies were last communicated to agents via e-mail on September 14, 2016. The 6 policies are also posted on the OTB SharePoint Collaboration website and a hard-copy of each has been distributed to the Collection Centre staff so their SOP and Policy binder can be updated.
	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	**OICR Policies: (see Appendix n/a)** **OTB Policies:** The following public materials were updated as a result of the amendments: 1) OTB Privacy Policy (OTB.POL801) is posted publically on the OTB website: http://www.ontariotumourbank.ca/patients/privacy-documents Updated OICR Privacy Officer mailing address. 2) Answers to Frequently Asked questions related to privacy policies, procedures and practices

Categories	Privacy Indicators	OICR
		http://www.ontariotumourbank.ca/patients/patient-faqs Updated OICR Privacy Officer mailing address. 3) Statement of Purpose http://www.ontariotumourbank.ca/patients/statement-purpose Updated OICR Privacy Officer mailing address.
Collection	The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.	One data holding containing PHI (TissueMetrix2)
	The number of statements of purpose developed for data holdings containing personal health information	One statement of purpose: http://www.ontariotumourbank.ca/patients/statement-purpose
	The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the Information and Privacy	One statement of purpose was reviewed (see statement above).

Categories	Privacy Indicators	OICR
	Commissioner of Ontario	
	Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made.	One change was made to the statement of purpose to update the OICR Privacy Officer mailing address.
Use	The number of agents granted approval to access and use personal health information for purposes other than research.	9 – Collection Centre staff 4 – OICR staff 3 – AIM staff
	The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy	None

Categories	Privacy Indicators	OICR
	Commissioner of Ontario.	
	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 by the Information and Privacy Commissioner of Ontario.	None
Disclosure	The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario.	None
	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 by the	None

Categories	Privacy Indicators	OICR
	Information and Privacy Commissioner of Ontario.	
	The number of requests received for the disclosure of personal health information for research purposes since the prior review by the Information and Privacy Commissioner of Ontario.	None
	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 by the Information and Privacy Commissioner of Ontario.	None
	The number of Research Agreements executed with researchers to whom personal health information was disclosed since	None

Categories	Privacy Indicators	OICR
	the prior review by the Information and Privacy Commissioner of Ontario.	
	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 by the Information and Privacy Commissioner of Ontario.	Aggregate inventory reports are provided to Collection Centres on a monthly basis (36 reports sent via email from November 2013 – October 2016). Number of requests for de-identified data sets for researchers = 39 (November 1, 2013 – October 31, 2016)
	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 by the Information and Privacy Commissioner of Ontario.	Number of Material Transfer Agreements signed and fulfilled = 30 (November 1, 2013 – October 31, 2016) (+4 Pending MTAs to be signed and executed, +5 MTAs were unfulfilled). Unfulfilled MTAs are due to the clients wishing to no longer move forward with their transaction. OTB does not release de-identified data without a signed MTA. Per OTB procedures (see SOP TB312 sec. 6.2), a preliminary data report (see F-TB312-07) may be shared without an MTA to help potential researchers in the selection of appropriate cases for their study.
Data Sharing Agreements	The number of Data Sharing Agreements	4 data sharing agreements (one for each Collection Centre)

Categories	Privacy Indicators	OICR
	executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	
	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 by the Information and Privacy Commissioner of Ontario.	None
Agreements with Third Party Service Providers	The number of agreements executed with third party service providers with access to personal health information since the prior review by the Information and Privacy	One – AIM last renewed on January 26, 2012 (automatic annual renewal)

Categories	Privacy Indicators	OICR
	Commissioner of Ontario.	
Data Linkage	The number and a list of data linkages of PHI approved since the prior review by the Information and Privacy Commissioner of Ontario.	None
Privacy Impact Assessments	The number and a list of privacy impact assessments completed since the prior review by the Information and Privacy Commissioner of Ontario 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	None

Categories	Privacy Indicators	OICR
	was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	
	The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion.	None
	The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion.	None
	The number of determinations made since the prior review by the	None

Categories	Privacy Indicators	OICR
	Information and Privacy Commissioner of Ontario 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.	
	The number and a list of privacy impact assessments reviewed since the prior review by the Information and Privacy Commissioner and a brief description of any amendments made.	None
Privacy Audit Program	The dates of audits of agents granted approval to access and use personal health information since the prior review by the Information and	See "Security Audit Program" indicator on p. 122 below for details. Privacy and Security parameters are audited together in a single audit.

Categories	Privacy Indicators	OICR
	Privacy Commissioner of Ontario and for each audit conducted: – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	
	The number and a list of all other privacy 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,	Freezer and Operational Audit is performed on an annual basis and a Privacy checklist is reviewed (see recommendations and details in Appendix B). See Appendix G on p. 166 for a copy of the Privacy checklist. 15 Annual Freezer and Operational Audits completed since the prior review (conducted at each Collection Centre and at OICR): • March 4, 2014 – KGH • March 11, 2014 – SJHH • March 20, 2014 – LHSC • March 25, 2014 – TOH • May 1, 2014 – OICR • February 9, 2015 – KGH • February 10, 2015 – LHSC • February 18, 2015 – SJHH

Categories	Privacy Indicators	OICR
	– 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.	• February 17, 2015 – TOH • March 11, 2015 – OICR • February 24, 2016 – KGH • April 22, 2016 – LHSC • March 1, 2016 – OICR • February 23, 2016 – SJHH • February 26, 2016 – TOH Annual Privacy Training (no recommendations made) Confidentiality Agreement (no recommendations made)
Privacy Breaches	The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	Zero privacy breaches; one breach investigation report (See Appendix E)
	With respect to each privacy breach or	See Appendix E and:

Categories	Privacy Indicators	OICR
	suspected privacy breach: – The date that the notification was received, – The extent of the privacy breach or suspected privacy breach, – Whether it was internal or external, – The nature and extent of personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the health information custodians or any other organizations,	An investigation of a suspected privacy breach undertaken on August 25, 2015. The result was that no PHI was disclosed. – Notification: August 25, 2015. – Extent: minor incident where one internal OTB staff member was able to temporarily see information about a donor within OTB's database that should not have been readable for that individual's location (i.e., information from one location was readable at another location). – Internal vs. External: Information was available internally – Nature: The information contained no direct patient identifiers, only de-identified sample information. – Senior Management Notified: August 25, 2015. – Containment: affected query was modified to remove comments, user privileges to edit/create queries temporarily removed. This was completed August 25, 2015. – The date(s) that notification was provided to the health information custodians or any other organizations: Not provided as no PHI was disclosed. – The date that the investigation was commenced: August 25, 2015. – The date that the investigation was completed: October 7, 2015. – A brief description of each recommendation made: 1) AIM will update TissueMetrix2 with a patch that will correct the privileges for View/Edit Query SQL Code 2) AIM to address comments nullifying security. – The date each recommendation was addressed: 1) September 23, 2015; 2) patch released January 7, 2016. – The manner in which each recommendation was addressed: The software was updated with a patch to ensure that SQL queries will not be edited with comments to nullify the security.

Categories	Privacy Indicators	OICR
	– 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	The number of privacy complaints received since the prior review by the Information and Privacy Commissioner of Ontario.	None
	Of the privacy complaints received, the number of privacy complaints investigated since the prior review by	None

Categories	Privacy Indicators	OICR
	the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint investigated: – The date that the privacy complaint was received, – The nature of the privacy complaint, – The date that the investigation was commenced, – The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation, – The date that the investigation was completed, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed,	

Categories	Privacy Indicators	OICR
	– 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.	
	Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint not investigated: – The date that the privacy complaint was received,	None

Categories	Privacy Indicators	OICR
	– The nature of the privacy complaint, and – The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.	

Part 2 – Security Indicators

Categories	Security Indicators	OICR
General Security Policies and Procedures	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.	See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices (which includes reference to Appendix D). Privacy and security policies and procedures are reviewed together.
	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.	See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices
	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.	See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices
	The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.	See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices

Categories	Security Indicators	OICR
	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.	See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices
Physical Security	The dates of audits of agents granted approved 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.	Temporary access card audits – daily. Access card audits - quarterly • December 22, 2014 • April 23, 2015 • August 13, 2015 • December 19, 2015 • June 1, 2016 • September 1, 2016 • December 16, 2016 • June 1, 2017 Key audit – annually • August 25, 2014 • September 25, 2015 • October 18, 2016 OTB Physical Security Audit June 27, 2016. There were no recommendations arising from the audit. It should be noted, however, that the June date does not reflect the overall frequency with which OICR conducts its physical security audits. The audit of June 2016 was OTB-specific. In fact, as stated herein, physical security audits

Categories	Security Indicators	OICR
		are conducted daily for temporary cards, quarterly for access cards and annually for keys. Audits can also be performed as related to operational, programmatic and personnel activities. All such audits are conducted in accordance with OICR's policy and procedures *on Access Card And Key Management For Mars Location*.
Security Audit Program	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.	OTB IT audits: April 1, 2014; October 1, 2014; April 1, 2015; October 1, 2015; April 1, 2016; and October 1, 2016. (See Appendix C on p. 139 for descriptions)
	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,	6 OTB IT audits conducted since November 1, 2013. (See Appendix C on p. 139 for descriptions) For more information: refer to OTB.POL803 section 5.4

Categories	Security Indicators	OICR
	– The date of completion of the audit, – A brief description of each recommendation made, – The date that each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is expected to be addressed	
Information Security Breaches	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.	No known information security breaches
	With respect to each information security breach or suspected information security breach: – 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,	No known information security breaches

Categories	Security Indicators	OICR
	– 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

Categories	Human Resources Indicator	OICR
Privacy Training and Awareness	The number of agents who have received and who have not received initial privacy orientation since the prior review by the Information and Privacy Commissioner of Ontario.	11 agents (6 Collection Centre staff and 5 OICR staff) have received their initial privacy training between November 1, 2013 and October 31, 2016. - November 1, 2013 - October 31, 2014: 3 Collection Centre staff and 2 OICR staff - November 1, 2014- October 31, 2015: 3 Collection Centre staff and 2 OICR staff - November 1, 2015- October 31, 2016: 0 Collection Centre staff and 1 OICR staff All agents having access to PHI or daily involvement with OTB have received the training. Zero agents have not received initial privacy training since the prior review.
	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.	None
	The number of agents who have attended and who have not attended ongoing privacy training each year since the	All 14 agents (6 Collection Centre staff and 5 OICR staff)

Categories	Human Resources Indicator	OICR
	prior review by the Information and Privacy Commissioner of Ontario.	have received ongoing privacy training between November 1, 2013 and October 31, 2016. 3 AIM staff have signed attestations of completing ongoing privacy and security awareness training. - November 1, 2013 - October 31, 2014: 8 Collection Centre staff, 4 OICR staff and 3 AIM staff - November 1, 2014- October 31, 2015: 9 Collection Centre staff, 4 OICR staff and 3 AIM staff - November 1, 2015- October 31, 2016: 12 Collection Centre staff, 4 OICR staff and 3 AIM staff Zero agents have not received ongoing privacy training since the prior review.
	The dates and number of communications to agents by the prescribed person or prescribed entity in relation to privacy since the prior review by the Information and Privacy Commissioner of Ontario and a brief description of each communication.	OTB: 1) Annual Privacy and Information Security training is available online (online training completed in December 2014, December 2015, and the next training is scheduled for December 2016)

Categories	Human Resources Indicator	OICR
		2) Collection Centre staff monthly teleconference (Quiz related to Privacy Policy OTB/POL801 conducted on October 15, 2013, November 19, 2014 and November 18, 2015) 3) Annual Operation Audit (conducted at each institution) where a Privacy checklist is reviewed. See Appendix G on p. 166 for a copy of the Privacy checklist: March 4, 2014 – KGH March 11, 2014 – SJHH March 20, 2014 – LHSC March 25, 2014 – TOH May 1, 2014 – OICR February 9, 2015 – KGH February 10, 2015 – LHSC February 18, 2015 – SJHH February 17, 2015 – TOH March 11, 2015 – OICR February 24, 2016 – KGH April 22, 2016 – LHSC March 1, 2016 – OICR February 23, 2016 – SJHH February 26, 2016 – TOH
Security Training and Awareness	The number of agents who have received and who have not received initial security	Same as above. 11 agents (6 Collection Centre staff and 5 OICR staff) have received their

Categories	Human Resources Indicator	OICR
	orientation since the prior review by the Information and Privacy Commissioner of Ontario.	initial security training between November 1, 2013 and October 31, 2016. - November 1, 2013 - October 31, 2014: 3 Collection Centre staff and 2 OICR staff - November 1, 2014- October 31, 2015: 3 Collection Centre staff and 2 OICR staff - November 1, 2015- October 31, 2016: 0 Collection Centre staff and 1 OICR staff All agents having access to PHI or daily involvement with OTB have received the training. Zero agents have not received initial security training since the prior review.
	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.	None
	The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the Information	All 14 agents (6 Collection Centre staff and 5 OICR staff) have received ongoing privacy training between November 1, 2013 and October 31, 2016.

Categories	Human Resources Indicator	OICR
	and Privacy Commissioner of Ontario.	3 AIM staff have signed attestations of completing ongoing privacy and security awareness training. - November 1, 2013 - October 31, 2014: 8 Collection Centre staff, 4 OICR staff and 3 AIM staff - November 1, 2014- October 31, 2015: 9 Collection Centre staff, 4 OICR staff and 3 AIM staff - November 1, 2015- October 31, 2016: 12 Collection Centre staff, 4 OICR staff and 3 AIM staff Zero agents have not received ongoing security training since the prior review.
	The dates and number of communications to agents by the prescribed person or prescribed entity to agents in relation to information security since the prior review by the Information and Privacy Commissioner of Ontario.	Same as above.
Confidentiality Agreements	The number of agents who have executed and who have not executed Confidentiality Agreements each year since the prior review by the Information	5 – OICR staff signed the OICR Confidentiality Agreement. 9 – Collection Centre staff have signed confidentiality agreements between each

Categories	Human Resources Indicator	OICR
	and Privacy Commissioner of Ontario.	agent and their employer, and OTB maintains a record of such. 3 – AIM staff signed a Confidentiality and Non-Disclosure Agreements with OTB. All agents who have regular involvement in the program or who have access to data have signed confidentiality agreements.
	The date of commencement of the employment, contractual or other relationship for agents that have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.	None
Termination or Cessation	The number of notifications received from agents since the prior review by the Information and Privacy Commissioner of Ontario related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.	10 agents: 8 terminations 2 maternity leave

Part 4 – Organizational Indicators

Categories	Organizational Indicators	OICR
Risk Management	The dates that the corporate risk register was reviewed by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	The Enterprise Risk Management Committee ("Risk Management Committee") reviewed the Privacy Register as follows: June 25, 2015. October 6, 2016, January 23, 2017 June 22, 2017. Note: OICR's Corporate Risk Management Policy was only approved by the Board of Directors in January, 2014. The risk register has been reviewed at least annually since that time.
	Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.	No amendments.
Business Continuity and Disaster Recovery	The dates that the business continuity and disaster recovery plan was tested since the prior review by the Information and Privacy Commissioner of Ontario.	Business Continuity and Disaster Recovery plan was communicated on May 19, 2015. Annual testing of this plan was completed on July 8, 2016.
	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 amendments.

Appendix A: Status of the OICR 2014 Prescribed Registry Triennial Review Recommendations

2014 IPC Compliance Recommendation	OICR Response	Status (Complete/In Progress)	Expected Date of Complete
1. It is recommended that OICR ensure that a review of its policies and procedures are conducted, at a minimum, on an annual basis, as required by the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the *Manual*").	Since the 2014 Triennial Review Report, OICR has gone through significant leadership changes, As such organizational structures have been in state of transition. OICR was able to complete one review of all policy and procedures only. However it has developed a plan to help ensure the annual review requirement shall be met moving forward.	In Progress.	Ongoing as of October 31, 2016.
2. It is recommended that OICR ensure confidentiality agreements are executed by all agents on an annual basis, as required by the *Manual*.	OTB Specific Confidentiality Agreements are signed annually by all OTB staff (including those located at Collection Centres) and tracked in the Log of Executed Confidentiality Agreements.	Complete	Ongoing as of October 30, 2013.

3. It is recommended that OICR combine the *Policy and Procedures in Respect of a Security and a Privacy Audit* with the *Policy Statement 37.0, Logging and Security Audit* to create a stand-alone document entitled *Policy and Procedures in Respect of a Security and a Privacy Audit*. This will better align with the policy structure and naming conventions in the *Manual* and thereby facilitate locating relevant content in any future review or IPC audit.	Policies have been merged.	Reviewed/Approved September 13, 2016 and posted January 2017.	September 2016
4. It is recommended that OICR combine the *Policy and Procedures in Respect of a Privacy Breach Management* with the *Policy Statement 10.0 Information Security Incident Response* to create a stand-alone document entitled *Policy and Procedures for Information Security and Privacy Breach Management*. This will better align with the policy structure and naming conventions in the *Manual* and thereby facilitate locating relevant content in any future review or IPC audit.	Policies have been merged.	Reviewed/Approved September 13, 2016 and posted January 2017.	September 2016

Appendix B: Privacy Recommendations from the OTB's annual Freezer and Operational Audit

Date of Audit	Recommendation	Date Addressed	Response
March 4, 2014	KGH: look into modifying the blood retrieval form to reduce the amount of PHI fields which are unnecessary.	March 6, 2014	JS has modified the blood retrieval form to reduce the amount of PHI fields
March 4, 2014	KGH: JS to obtain second monitor so information does not need to be printed from TM.	March 6, 2014	Office now located in separate area. Recommendation no longer applicable.
March 4, 2014	KGH: Printing out the query results are not required as the same list exists in TM.	March 6, 2014	The employee has retired and a new employee has since started in her place. This new employee has an office in a separate area, so this is no longer applicable.
March 20, 2014	LHSC: Donor information sheets should be shredded as there is no need to keep these documents since the same information is in TM.	March 31, 2014	Going forward we will not keep the donor information sheets on file.
March 11, 2014	SJHH: Purge confidential waste daily or store in a locked cabinet until it can be disposed of confidentially.	April 25, 2014	Confidential waste is now stored in a locked cabinet within our room and only Anbreen and I have access to the key.
February 9, 2015	KGH: Obtain a second computer monitor for Tumour Bank staff to reduce need to print information sheets from TM.	March 17, 2015	A second monitor was obtained and installed.
March 11, 2015	OICR: Suggested that the -80 shared freezer should be locked. Both parties to maintain keys.	March 24, 2015	MM now shares keys with IL (Transformative Pathology program)
February 17, 2015	TOH: Confirm with IT group that MS access has been removed from V drive (TissueMetrix folder).	March 30, 2015	V drive/TissueMetrix folder access by MS has been removed. TOH-IT email confirmation is available.
February 17, 2015	TOH: Enable V drive (TissueMetrix folder) access to for PG.	March 30, 2015	TOH-IT V drive/Tissue Metrix folder access provided for PG.

Date of Audit	Recommendation	Date Addressed	Response
February 17, 2015	TOH: NR to remove identifying donor information from the histology and patient follow up list once follow up is complete.	March 30, 2015	Recommendation completed by NR.
February 23, 2016	SJHH: OICR to investigate adding a field for tracking appointment dates in TissueMetrix so this information can be stored within the application instead of encrypted spreadsheet.	In progress	Request has been submitted to vendor but not yet implemented. Expected completion is summer 2017.

Appendix C: Ontario Tumour Bank Security IT Audit Summary

	Type of Audit							
Audit Date	OICR VPN Access[1]	R Drive Access[2]	OTB Inbox Access[3]	TMx – Application[4]	TMx – Oracle[5]	OTB Scan Folder[6]	SSLVPN (AIM access)[7]	OTB SharePoint[8]
01-Apr-14	No issues	One change: Removal of the following user: sstasi *Completed on June 6, 2014*	Removal of sstasi from OTB mailbox access *Completed on May 30, 2014*	Removed: ELIZABETH *Completed January 31, 2014*	Drop the following user: JENN	Removal of sstasi from OTB scan folder access. *Completed on May 30, 2014*	No issues	N/A
01-Oct-14	No issues New users: mmoore, cweir, epoupard Removed: jwoo	No issues New users: mmoore, cweir, epoupard Removed: jwoo	New users: mmoore, cweir, epoupard	**Removed:** MARTA (TOH) *Completed November 3, 2015* JENNIFER (OICR). *Completed June 30, 2015* NANCY (OICR). *Completed September 26, 2014* **New users:** MELISSA (OICR).	Removed: Nancy, Jenn New users: ELISE	No issues	No issues	N/A

	Type of Audit							
Audit Date	OICR VPN Access[1]	R Drive Access[2]	OTB Inbox Access[3]	TMx – Application[4]	TMx – Oracle[5]	OTB Scan Folder[6]	SSLVPN (AIM access) [7]	OTB SharePoint[8]
				Completed July 30, 2015 CEOLA (OICR). *Completed September 3, 2014*				
01-Apr-15	No issues/ changes	No issues/ changes	Removed: Jwoo	No issues **Removed:** JAMES1 and JAMES2 (LHSC and CVH accounts). *Completed December 5, 2014* **New users:** ELISE (OICR). *Completed November 13, 2014* *PANA (TOH).*	No issues/ changes	No issues/ changes	No issues	N/A

	Type of Audit							
Audit Date	OICR VPN Access[1]	R Drive Access[2]	OTB Inbox Access[3]	TMx – Application[4]	TMx – Oracle[5]	OTB Scan Folder[6]	SSLVPN (AIM access) [7]	OTB SharePoint[8]
				Completed December 16, 2014 CAROLYN1 and CAROLYN2 (LHSC and CVH accounts). *Completed January 29, 2015*				
01-Oct-15	No issues **Removed:** Monique Albert **Added:** Sola Dokun	No issues **Removed:** Monique Albert **Added:** Sola Dokun	No issues **Removed:** Monique Albert **Added:** Sola Dokun	No issues **Removed:** JOANNE CAROLYN1 CAROLYN2 MONIQUE **Added:** KATIE JAMES1 JAMES2	No issues **Locked:** MONIQUE (2015-09-08) **Added:** SOLA (2015-09-08)	No issues **Removed:** Monique Albert **Added:** Sola Dokun	No issues	**Removed:** Monique Albert

	Type of Audit							
Audit Date	OICR VPN Access[1]	R Drive Access[2]	OTB Inbox Access[3]	TMx – Application[4]	TMx – Oracle[5]	OTB Scan Folder[6]	SSLVPN (AIM access) [7]	OTB SharePoint[8]
01-Apr-16	No issues **Removed:** Melissa Moore	No issues **Removed:** Melissa Moore	No issues **Removed:** Melissa Moore	No issues **Removed:** MELISSA **Added:** CAROLYN1 CAROLYN2	No issues	No issues **Removed:** Melissa Moore	No issues	No issues **Removed:** Melissa Moore
01-Oct-16	No issues **Added:** Rachel Kelly	No issues **Added:** Rachel Kelly	No issues **Added:** Rachel Kelly	**Removed:** JAMES1 JAMES2 JULIE PANA **Added:** MARTA RACHEL	No issues	No issues **Added:** Rachel Kelly	No issues	No issues **Removed:** Julie HolidayJames Sinfield Pana Giannakouros **Added:** Rachel Kelly

[1] Audits users that currently have access to OICR's VPN/who have been provided RSA keyfobs
[2] Audits users who have access to the OTB folder on FS10: R:\H-Tumour Bank
[3] Audits active users who have access to the shared OTB Inbox on Exchange
[4] Audits (i) active TissueMetrix Accounts in Production; (ii) Audit TissueMetrix account login
[5] Audits list of users with Oracle Production DB Accounts
[6] Audits read/write access to the OTB scan folder
[7] Audits: (i) shell account logs (username, date/time logged in, date/time logged off); and (ii) active CCO VPN accounts
[8] Audits: (i) owners of all OTB program files; (ii) OTB SharePoint user groups; and (iii) OTB Collaboration access

Appendix D: OICR Policy Amendments

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Access Card and Key Management for MaRS Location	Log of Access to OICR Premises—OICR Access Cards (F-AD-SEC.504-01); Log of Access to OICR Premises—OICR Keys (F-AD-SEC.504-02); Day Pass Access Card Log (F-AD-SEC.504-03); MaRS Access Cards Request Form for OICR (F-AD-SEC.504-04); MaRS Key Request form (F-AD-SEC.504-05); MaRS Authorization to Issue Transfer Key (F-AD-SEC.504-06); OICR Incident Report Form (F-AD-SEC.502-03)	AD-SEC.504.003	Administrative—Facilities Security	Facilities Manager		Vice President, Corporate Services and Chief Financial Officer	Corporate Management	30-Aug-16	05-Oct-15 (currently in review process, 10-16)	**AD-SEC.502.003** • Updated as per IPCO feedback Nov 1 2010; • Updated template to reflect new OICR logo; • Sec 5.1.1 #6 – Revised process; • Sec. 5.4.2 – revised process; • Updated Appendices: A, C, D.
Clean Desk Policy		AD-GEN.104.003	Administrative—General Administration and Risk Management	Vice President, Corporate Services and Chief Financial Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	05-Oct-16	11-Oct-16	**AD-GEN.104.003** • Updated IP definition • Updated position and committee titles
Confidentiality of Information	Log of Confidentiality Agreements (F-PR-INS.102-01); OICR Confidentiality Agreement (F-PR-INS.102-02)	PR-INS.102.002	Privacy and Information Security – Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	08-Jun-16	17-Nov-15 (additional sponsor and issuing authority review 3-Aug-16)	**PR-INS.102.002** • Update to Table 5.0, consolidated responsibilities of Commercialization and Grants and Awards group and renamed group to Scientific Secretariat • Updated titles and committee names where necessary • Updated references to a newly integrated policy in sections 2.0, 4.3, 4.6, 5.1 and 6.0.
Data Use and Disclosure Policy	Project Privacy Evaluation Form (F-PR-INS.201-01)	PR-INS.201.004	Privacy & Information Security--Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	14-Jun-16	17-Nov-15 (additional sponsor and issuing authority review 3-Aug-16)	**PR-INS.201.004** • Updated committee and position titles • Updated reference to newly integrated policy in section 4.5 and 6.0
Development and Management of Policies, Procedures and Guidelines	Template for Development of Policies and Procedures (F-AD-GEN.101-01);Approval / Change Request Form for Policies, Procedures and Guidelines (F-AD-GEN.101-02)	AD-GEN.101.002	General Administration and Risk Management	Vice President, Corporate Services and Chief Financial Officer		Vice President, Corporate Services and Chief Financial Officer	Corporate Management	11-Oct-16	12-Oct-16	**AD-GEN.101.003** • Updated references, position and committee titles
Execution of Data Sharing Agreements	Data Sharing Agreement Log (F-PR-INS.205-01), Data Sharing Agreement Template (F-PR-INS.205-02)	PR-INS.205.002	Privacy and Information Security – Privacy -- Data Management	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	14-Jun-16	17-Nov-15 (additional sponsor and issuing authority review 3-Aug-16)	**PR-INS.205.002** • Defined content in table 5.1: updated designated office for Commercialization and industrial partnership to FACIT • Updated organization and position titles • Updated references to a newly integrated policy in sections 2.0, 4.5 and 6.0.

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Execution of Third Party Service Provider Agreements	Third Party Services Agreement (Template) (F-AD-GEN.105-01), Log of Third Party Service Agreements (F-AD-GEN.105-02)	AD-GEN.105.002	Administration—General Administration and Risk Management	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	08-Jun-16;	17-Nov-15 (additional sponsor and issuing authority review 3-Aug-16)	**AD-GEN.105.002** • Updated position and organization titles • Updated references to newly integrated policies in sections 2.0, 4.4, 4.5 and 6.0.
Facilities Security Policy	Visitor Log (F-AD-SEC.502-01); Day Pass Access Card Log (F-AD-SEC.504-03); Lost and Found Log (F-AD-SEC.502-02); OICR Incident Report Form (F-AD-SEC.502-03)	AD-SEC.502.002	Administrative—Facilities Security	Facilities Manager		Vice President, Corporate Services and Chief Financial Officer	Corporate Management	30-Aug-16	5-Oct-15 (currently in review process Oct-16)	**AD-SEC.502.002** • Added Sec 4.6.1 – Video Surveillance Policy
General Breach Report / Investigation Form		F-PR-INS.301-01	Privacy & Information Security--Privacy						21-Oct-16 (Sponsor only, no changes)	**F-PR-INS.301-01** • New document **F-PR-INS.301-01** • Revised document; • Definition of breach revised as per IPC review; • Removed references to "prescribed entities" under definition of breach of privacy – as per feedback from IPCO August 31 2011.
Glossary for Privacy Policies and Procedures		D-PR-INS.102	Privacy & Information Security--Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	02-Jun-16	08-Jun-16	**D-PR-INS.102** • Formatting • Updated position and committee titles
Investigation and Reporting of Suspected Theft for MaRS Location	OICR Incident Report Form (F-AD-SEC.502-03)	AD-SEC.506.002	Administrative—Facilities Security	Facilities Manager		Vice President, Corporate Services and Chief Financial Officer	Corporate Management	30-Aug-16	14-Aug-15; (currently in review process Oct-16)	**AD-SEC.506.002** • Modified Facilities Manager contact information
OICR Incident Report Form	Facilities Security; Investigation and Reporting of Facilities Security Incidents; Accident Reporting and Investigation	F-AD-SEC.502-03	Administration—Facilities Management; Health and Safety	Facilities Manager; Health and Safety Officer	Facilities Manager; Health and Safety Officer	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	18-Oct-11;	24-Oct-16 (Sponsor only, no changes)	

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
OICR Information Security Program		PR-INS.800.005	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	12-Oct-16	12-Oct-16	**PR-INS.800.005** • Updated position and committee titles; • Formatting.
OICR Privacy and Information Security Accountability Terms of Reference		PR-INS.103.002	Privacy and Information Security – General Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	16-Aug-16	11-Oct-16	**PR-INS.103.002** • Update position and committee titles. • Rolled up Information Sub Committee and its responsibilities into the Information Governance Committee
OICR Privacy Policy		PR-INS.101.004	Privacy & Information Security--Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	02-Jun-16	05-Jul-16	**PR-INS.101.004** • Formatting and copy-edit • Updated position and committee titles. • Updated references to a newly integrated policy in sections 4.10.2 and 5.0.
Personal Information Guideline			Privacy and Information Security—OICR Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	07-Jul-16	13-Sep-16	
Policies and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information		PR-INS.206.002	Privacy & Information Security -- Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	02-Jun-16	05-Jul-16	**PR-INS.206.002** • Formatting and copy-edit; • Updated position and committee titles; • Update references to newly integrated policies in sections 4.3 and 5.0.
Policy and Procedures for Maintaining a Consolidated Log of Recommendations	OICR's Consolidated Log of Privacy and Information Security Recommendations (F-PR-INS.104-01)	PR-INS.104.002	Privacy & Information Security— General Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	08-Jun-16	17-Nov-15 (additional sponsor and issuing authority review 3-Aug-16)	**PR-INS.104.002** • Update to acronyms and committee and position titles; • Update references to newly integrated policies in sections 5.2 and 6.0.
Policy and Procedures for Information Security and Privacy Breach Management	Breach Investigation Form (F-PR-INS.301-01), Log of Privacy Breaches (F-PR-INS.301-02)	PR-INS.301.001	Privacy & Information Security— Privacy – Breach Management	Privacy Officer and Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	13-Jul-16	13-Sep-16	**PR-INS.301.001** • Merging of Security Incident Response Policy with Policy and Procedures for Privacy Breach Management per IPC recommendation.
Policy and Procedures in Respect of a Security or a Privacy Audit	Privacy Audit Report Template (F-PR-INS.204-01), Privacy Audit Log (F-PR-INS.204-02),	PR-INS.204.001	Privacy & Information Security—Data Management	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	23-Jul-16	13-Sep-16	**PR-INS.204.001** • Merging of Policy and Procedures in Respect of a Privacy Audit with Logging and Security Audits per IPC recommendation.

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Policy Statement 1.0 Acceptable Use		AD-INT.201.004	Administrative—Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	08-Jun-16	08-Mar-16	**AD-INT.201.004** • Changed text in second paragraph to infer all passwords must not be disclosed • Updated committee and position titles
Policy Statement 11.0 IT Risk Assessment Policy and Threat Risk Assessment Guide		PR-INS.811.002	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	05-Aug-16	11-Oct-16	**PR-INS.811.002** • Formatting; • Removed Level 2 data from the scope of this policy; • Updated position and committee titles.
Policy Statement 12.0 Change Controls (OICR Production Servers)		PR-INS.812.004	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	15-Jun-16	05-Jul-16	**PR-INS.812.004** • Updated Statement on Change Control • Updated Standards section, including review requirements, frequency of IT CRB reviews and when both major and minor changes will be scheduled • Added CRB to approval required for emergency changes • Updated committee and position titles
Policy Statement 13.0 Server Security		PR-INS.813.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Security Officer	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	28-Jun-16	05-Jul-16	**PR-INS.813.003** • Copy-edit and updated position and committee titles
Policy Statement 14.0 Network Security		PR-INS.814.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	21-Jun-16	05-Jul-16	**PR-INS.814.003** • Updated position and committee titles
Policy Statement 15.0 Workstation Security		AD-INT.215.003	Administrative--Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	05-Aug-16	12-Oct-16	**AD-INT.215.003** • Changed auto lockscreen timeout to 10 minutes • Removed Section 2.3 • Updated procedure in Section 3.1. • Updated position and committee titles.
Policy Statement 16.0 Personal Use of OICR Systems		AD-INT.216.004	Administrative--Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	05-Aug-16	11-Oct-16	**AD-INT.216.004** • Removed paragraph on exceptions to Section 1; • Removed example of personal use in Section 1; • Removed Section 3 on Procedures; • Updated billable charges in Section 2; • Updated position and committee titles.
Policy Statement 17.0 Personal/Third Party Devices Interacting with OICR Systems		AD-INT.217.003	Administrative--Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	04-Oct-16	11-Oct-16	**AD-INT.217.003** • Updated references, position and committee titles • Updated practice to 2.1 and removed section 2.3

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Policy Statement 18.0 Electronic Mail Security		AD-INT.218.005	Administrative—Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	15-Jun-16	05-Jul-16	**AD-INT.218.005** • Section 2.4: Removed Entourage from OICR approved technologies list. • Updated section 2.5 relating to requirements for forwarding emails internally. • Added section 2.6 on the use of auto-responses when an employee leaves OICR. • Updated section 2.14 on email archiving where email messages can be automatically archived after a year. • Updated committee and position titles.
Policy Statement 19.0 Extranet Security		PR-INS.819.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	29-Sep-16	11-Oct-16	**PR-INS.819.003** • Updated committee and position titles.
Policy Statement 2.0 Data Classification		PR-INS.802.004	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	14-Jun-16	08-Mar-16	**PR-INS.802.004** * Added wording for Data Owners to provide direction for data encryption; * Updated Type of data/examples for level one, two, three and four; * Updated committee and position titles.
Policy Statement 20.0 Anti-Virus Administration		PR-INS.820.003	Privacy & Information Security—IT Information Security	Privacy & Information Security—IT Information Security	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	02-Jun-16	08-Jun-16	**PR-INS.820.003** • Apple and Windows computers treated the same – both must have antivirus software • Clarification on use of portable media on Lab computers • Updated position and committee titles
Policy Statement 22.0 Remote Access		PR-INS.822.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Security Officer	Vice President, Corporate Services and Chief Financial Officer	Vice President, Corporate Services and Chief Financial Officer	04-Oct-16	11-Oct-16	**PR-INS.822.003** • Update references, position and committee titles; • Removed sections 2.3.1.1 and 2.4.1.1 to sections 2.3 and 2.4
Policy Statement 23.0 Electronic Media Destruction		PR-INS.823.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	13-Sep-16	12-Oct-16	**PR-INS.823.003** • Included examples of destruction methods (S. 2.1) • Updated position and committee titles
Policy Statement 24.0 Declaration and Disposal of Surplus IT Equipment		PR-INS.824.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	02-Jun-16	08-Jun-16	**PR-INS.824.003** • Minor formatting and copy-edit • Updated position and committee titles
Policy Statement 25.0 HelpDesk Services Security		PR-INS.825.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	29-Sep-16	11-Oct-16	**PR-INS.825.003** • Update position and committee titles • Update terminology to IT HelpDesk • Section 3.1: clarify who HelpDesk staff need to ensure the request came from • Section 3.5: Update to process for updating lost or forgotten passwords

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Policy Statement 26.0 Employees on Temporary (Short or Long-Term) Leave		AD-INT.226.004	Administrative--Information Technology	Information Security Officer	Information Governance Committee; Manager, Human Resources	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	29-Sep-16	11-Oct-16	**AD-INT.226.004** • Update to committee and position titles. • Sections 2.1 and 2.2: Update "auto-forwarded" to "made accessible". Removed Section 2.3: Exceptions
Policy Statement 27.0 Employees Departing OICR		AD-INT.227.003	Administrative--Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	05-Oct-16	11-Oct-16	**AD-INT.227.003** • S. 3.6 – Added procedure for preservation of user data • S. 3.7 – Added procedure for transfer of data ownership. Update position and committee titles
Policy Statement 28.0 Mobile Devices Security		AD-INT.228.005	Administrative—Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	20-Sep-16	11-Oct-16	**AD-INT.228.005** • Updated committee and position titles; • Removed Section 3.1 Tunneling Internet Traffic to/from Mobile Devices; • Updated terminology.
Policy Statement 29.0 Disaster Recovery and Offsite Data Storage		PR-INS.829.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	09-Sep-16	12-Oct-16	**PR-INS.829.003** • Removed details on disaster recovery plan for JD Edwards financial data. JD Edwards software now runs on a virtual machine, and is recovered like other Windows servers. • Due to volume and amount of churn, it's not feasible to backup all data on the Isilon file servers. Some protection is provided by automatic daily snapshots.
Policy Statement 3.0 Encryption		PR-INS.803.004	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee; Information Security Officer;	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	28-Jun-16	05-Jul-16	**PR-INS.803.004** • Update 128 to 256 in Section 2.1; • Send passwords using whisper.oicr.on.ca; • Removed reference to specific vendor; • Updated committee and position titles; • Updated references to newly integrated policies in Sections 3.3 and 4.
Policy Statement 30.0 Research Lab Security		PR-INS.830.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	12-Oct-16	12-Oct-16	**PR-INS.830.003** • Added paragraphs to section 1, 3.2 and 3.3; • Formatting; • Updated position and committee titles.
Policy Statement 31.0 Loaner Devices		AD-INT.231.003	Administrative—Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	30-Sep-16	11-Oct-16	**AD-INT.231.003** • Update to committee and position titles. • Add two week restriction to loaner devices. • Clarify where loaner devices are allowed.

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Policy Statement 32.0 Restricted or Non-Networked Computing Environments		PR-INS.832.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	12-Oct-16	12-Oct-16	**PR-INS.832.003** • Updated position and committee titles
Policy Statement 33.0 Patch Management		PR-INS.833.005	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	12-Oct-16	12-Oct-16	**PR-INS.833.005** • Updated position and committee titles
Policy Statement 36.0 Mobile Device Allocation		AD-INT.236.005	Administrative--Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	12-Oct-16	12-Oct-16	**AD-INT.236.005** • S. 2.0 – Added Apple iPhone as eligible device • S. 3.6 – Added wording to remove any apps that can lock the mobile device. • Updated position and committee titles. • Formatting.
Policy Statement 38.0 IT Device (Hardware and Software) Allocations	Mobile Devices User Agreement (F-AD-INT.238-02)	AD-INT.238.001	Administrative—Information Technology	Director, IT; Director, Finance	Manager, Procurement	Corporate Management	Corporate Management	30-09-16	11-Oct-16	**AD-INT.238.002** • Updated committee and position titles. • Updated messaging in Section 4.3.
Policy Statement 4.0 Secure Electronic Data Retention, Backup, Disposal and Destruction		PR-INS.804.004	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	22-Jun-16	22-Jun-16	**PR-INS.804.004** • Updated 5.4 • Updated position and committee titles
Policy Statement 5.0 Data Protection (Encryption, Transmission and Storage)		PR-INS.805.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	02-Jun-16	08-Jun-16	**PR-INS.805.003** • Updated references; • Updated position and committee titles.
Policy Statement 6.0 Access Control, Identification and Authentication		PR-INS.806.002	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	14-Jun-16	08-Mar-16	**PR-INS.806.003** • Updated terminology; • Clarified where two factor authentication is required; • Updated committee and position titles; • Updated with SSH keys.

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Policy Statement 7.0 Password Governance		AD-INT.207.003	Administrative—Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	23-Sep-15	23-Sep-15	**AD-INT.207.003** • Section 6.0 - Added new paragraph to address Compliance, Audit and Enforcement. • Changes made to keep OICR at industry standard for password strength. • Password minimum increased from 6 to 8 characters; auto lock after failed attempts changed from 10 to 20; grammatical corrections; reference to OTB TM password expiry being 90 days; must not contain a "single dictionary word by itself"; 3 char types vs 2
Policy Statement 8.0 Internet Usage		AD-INT.208.005	Administrative—Information Technology	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	08-Jun-16	09-Mar-16	**AD-INT.208.005** Changes to align with new issues: • Added to section 2. the prohibited use of identity-masking Internet services and the use of peer-to-peer (P2P) file sharing software (torrents and similar); • Added to section 2., all commercial software must be pre-approved by the IT Department via the Helpdesk prior to purchase or installation; • Added to section 3., security of ANY information transmitted on the Internet cannot be guaranteed by OICR; • Removed "OICR Research" wireless access from section 4.2; • Added details to the OICR – Personal Wi-Fi in section 4.2; • Updated committee and position titles
Policy Statement 9.0 Access to OICR Systems by Contractors, Consultants & Third Parties		PR-INS.809.003	Privacy & Information Security—IT Information Security	Information Security Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	16-Jun-16	08-Mar-16	**PR-INS.809.003** • Update to committee and position titles. • Added messaging about requirements for portable media.
Privacy and Information Security Training and Awareness Policy	Privacy and Information Security Attestation (F-PR-INS.601-01); Privacy and Information Security Attestation—Specialized Role-Based Training for Ontario Tumour Bank (F-PR-INS.601-02); Log of Privacy and Information Security Training (L-PR-INS.601-03)	PR-INS.601.003	Privacy & Information Security--Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	07-Jul-16	13-Sep-16	**PR-INS.601.003** • Updated committee and position titles; • Updated reference to newly integrated policy in section 4.3 and 6.0.
Privacy Complaint Policy and Procedure	Privacy Complaint Log (F-PR-INS.702-01)	PR-INS.702.003	Privacy & Information Security—Privacy -- Privacy Information for the Public	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	08-Jun-16	17-Nov-15 (additional sponsor and issuing authority review Aug 3)	**PR-INS.702.003** • Modified content 5.2.1; • Changed IGSC to IGC in entire document; • Included complete link in 5.1.1 & removed DM System in 5.1.8; • Updated references to related policy documents;. • Updated committee and position titles.

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Privacy Impact Assessment Policy	Log of Privacy PIA (F-PR-INS.501-01)	PR-INS.501.002	Privacy & Information Security--Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	07-Jul-16	11-Oct-16	**PR-INS.501.002** • Updated committee and position titles • Updated reference to newly integrated policy in Sections 4.4 and 6.0
Privacy Inquiry Policy and Procedure	Log of Privacy Inquiries (F-PR-INS.701-01)	PR-INS.701.003	Privacy & Information Security--Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	22-Jun-16	05-Feb-16; 05-Jul-16	**PR-INS.701.002** • Modified scope in section 4.0 to address "anyone" rather than "any member of the public"; • Added section 4.1; • Added additional references to OICR Privacy Policy and OICR Privacy and Information Security Accountability Terms of Reference. **PR-INS.701.003** • Sec. 5.0 – IGC committee name updated – no longer Information Sub Governance Committee • Updates to position and committee titles • Updated references to newly integrated policies in Sections 4.1 and 6.0.
Progressive Discipline Policy		AD-HRE.612.002	Administrative – Human Resources – Employment	Human Resources Manager		Vice President, Corporate Services and Chief Financial Officer	Corporate Management	17-Jun-16	05-Jul-16	**AD-HRE.612.002** • Updated in Sections: 3.0, 5.1, 5.2, 6.0; • Updated position and committee titles; • Updated references to newly consolidated policies in Sections 5.4, 6.0.
Retention and Disposal of Administrative Records		PR-INS.203.003	Privacy & Information Security—Data Management	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	28-Jul-16	11-Oct-16	**PR-INS.203.003** • Defined content in scope, sec 2.0; • Updated position and committee titles; • Updated related policy title.
Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information			Privacy & Information Security—Data Management	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	23-Jun-16	25-Jun-16	**PR-INS.201.004** • Updated position and committee titles; • Updated references to newly integrated policies in Sections 5.1, 5.3, 5.4 and 6.0.
Sending / Receiving Personal Information, Personal Health Information and Confidential/Sensitive Information		PR-INS.401.003	Privacy & Information Security--Privacy	Privacy Officer	Information Governance Committee	Vice President, Corporate Services and Chief Financial Officer	Corporate Management	23-Jun-16	05-Jul-16	**PR-INS.401.003** • Formatting; • Updated committee and position titles; • Updated references to newly integrated policies in Sections 4.5 and 6.0.

Policy Title	Associated Form(s)	Policy Number	Section	Sponsor	Content Reviewer(s)	Issued By	Approved By	Last Modified	Review Dates	Revision Comments
Termination Policy	Termination Checklist: Receipt of OICR Property and Assets (F-AD-HRE.611-01); Termination Checklist: Termination / Suspension of Access to OICR Electronic Resources (F-AD-HRE.611-02)	AD-HRE.611.003	Administrative – Human Resources – Employment	Human Resources Manager		Vice President, Corporate Services and Chief Financial Officer	Corporate Management	17-Jun-16	05-Jul-16	**AD-HRE.611.003** • HR reviewed and reorganized wording in the policy and procedure sections. Other minor tweaks to wording; • Updated position and committee titles; • Updated references to newly integrated policies is Sections 5.7, 6.0.

Appendix E: OTB Suspected Breach Investigation Report

OICR
Ontario Institute for Cancer Research

MaRS Centre
661 University Avenue
Suite 510
Toronto, Ontario
Canada M5G 0A3

Telephone 416-977-7599
Toll-free 1-866-678-6427
www.oicr.on.ca

Valid only on date printed: 07/10/2015 9:40:00 AM. Discard immediately after use!

GENERAL BREACH REPORT/INVESTIGATION FORM

NOTE: Following notification of a breach or a suspected breach, the PO or the ISO or designate will complete this form.
TYPE OF BREACH: This form is to be used for PRIVACY breaches of personal information (including personal health information), and for CONFIDENTIALITY breaches including the breach, misuse or loss of confidential and/or sensitive information (e.g., intellectual property, research protocols, Human Resources documents, financial documents)

Definitions

Breach of Privacy:

- The collection, use, and disclosure of personal health information that is not in compliance with the Act or its regulation;
- A contravention of the privacy policies, procedures or practices implemented by a prescribed person;
- A contravention of Data Sharing Agreements, Research Agreements, Confidentiality Agreements and Agreements with Third Party Service Providers retained by the prescribed person; and
- Circumstances where personal health information is stolen, lost or subject to unauthorized use of disclosure or where records of personal health information are subject to unauthorized copying modification, or disposal.

Breach of Confidentiality: The unauthorized use or disclosure of confidential or sensitive information in the custody and control of OICR by OICR or its agents.

Report Information

1. Notification:

Name of Person who reported the breach/suspected breach: Gino Celebre

Job title and contact information: Pathologists' Assistant, Ontario Tumour Bank
905-522-1155 x32856
gcelebre@stjosham.on.ca

Name of manager/supervisor (if applicable):

Date of discovery: August 25, 2015

Time of discovery: 3:00PM

Date of notification: August 25, 2015

FOR USE BY MANAGER, POLICIES FOR DOCUMENTATION CONTROL			
Form Title and Number:	General Breach/Report Investigation Form (F-PR-INS.301-01)		
Associated Policy Title and Number:	Policy and Procedures for Privacy Breach Management (PR-INS.301)		
Section Name:	Privacy & Information Security--Privacy	Template Created On:	March 22, 2011

MaRS Centre
661 University Avenue
Suite 510
Toronto, Ontario
Canada M5G 0A3

Telephone 416-977-7599
Toll-free 1-866-678-6427
www.oicr.on.ca

Time of notification: 3:03PM

2. Containment:

TissueMetrix2 (TMx) users' privileges to edit/create queries using the query wizard and SQL were removed as soon as the incident was reported and will be restored once the issue has been addressed (see s.5 on remediation).

3. Reporting:

Gino Celebre is an OTB staff member located at St. Joseph's Healthcare Hamilton. He has been assigned the permission level of *CC USER* in TMx which does not permit 'View records across institutions' or 'View PHI from other institutions'. On August 25, 2015, Gino ran the query: "*Blood-Only Cases excl PROS (> 2 months)*" in TissueMetrix2. Upon running the query, he noticed the result output contained two cases from another site, specifically, London Health Sciences Centre (LHSC). While no personal health information was visible, Gino was able to identify the institutional source of the information by the first two letters of the Donor Number.

Gino immediately notified Elise Poupard (OTB Sr Analyst) and Sola Dokun (OTB Manager) of the incident via email at 3:03pm on that same day.

As mentioned earlier, the results did not display PHI but included:

- Donor Number (unique donor identifier generated by TMx)
- Event Date (date in which event was added to TMx, not a clinical date)
- Sample Numbers (unique patient identifier generated by TMx)
- Sample Type (plasma, buffy, etc.) and Prep (fresh frozen, FFPE, etc.)

Gino confirmed this was the first time he'd been able to see the results of another Collection Centre when running the query *Blood-Only Cases excl PROS (> 2 months)*. He also confirmed this issue had not occurred in any other TMx query.

Upon receipt of notification from Gino, Elise logged into TissueMetrix2 to view the query, which was written using SQL. She compared it with "typical" queries and noted that this SQL query had contained a comment starting with "--"denoting additional – non SQL – details on the query (i.e., "--The purpose of this query is ..."). She wondered whether the comment in the query may have had an impact on user rights.

Elise contacted AIM (the TMx vendor) to explain her theory. AIM confirmed that adding comments to the end of a query had the unintended effect of nullifying the security coding / user permission. The comments from the query *Blood-Only Cases*

OICR
Ontario Institute for Cancer Research

MaRS Centre
661 University Avenue
Suite 510
Toronto, Ontario
Canada M5G 0A3

Telephone 416.977.7599
Toll-free 1-866-678-6427
www.oicr.on.ca

excl PROS (> 2 months) were immediately removed. Elise reviewed all other existing TMx queries to verify no other comments were embedded.

4. Investigation:

OTB notified OICR privacy personnel, namely the Privacy Officer (Howard Simkevitz), Information Security Officer (David Sutton), and Vice-President, Operations (Jane van Alphen) were all on vacation at this time.

Elise and Sola reached David Sutton on his personal phone at approximately 5:00pm. After briefing David on the incident, David advised OTB to:

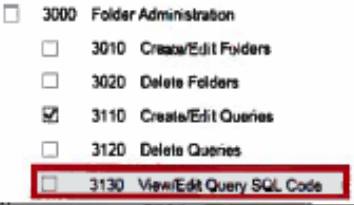
1. Send email to privacy@oicr.on.ca containing information on incident for to create a record (for Howard's review upon his return on Monday, August 30, 2015)
2. Notify LHSC privacy office of incident
    - Note: there was no mention at this point of notifying SJHH privacy office

The above recommendations were completed on August 25, 2015.

Howard responded by way of email and asked for confirmation as to whether PHI was disclosed. Sola confirmed that no PHI was disclosed.

During investigation between OTB and AIM, it was identified that:

1. In the current version of TMx, comments can be added to TMx SQL queries using /* ... */ without security being nullified (verified by QA)
2. Only a TMx administrator (i.e. OTB Sr Analyst) should be able to edit SQL queries (this was a recommendation identified in the OTB Threat Risk Assessment).
3. However, the User Roles in TMx were not properly restricting permissions for Create/Edit Queries vs. View/Edit Query SQL Code (i.e., even though the proper User Role selections were made, all users were able to View/Edit SQL Code)



FOR USE BY MANAGER, POLICIES FOR DOCUMENTATION CONTROL			
Form Title and Number:	General Breach/Report Investigation Form (F-PR-INS.301-01)		
Associated Policy Title and Number:	Policy and Procedures for Privacy Breach Management (PR-INS.301)		
Section Name:	Privacy & Information Security–Privacy	Template Created On:	March 22, 2011

OICR
Ontario Institute for Cancer Research

MaRS Centre
661 University Avenue
Suite 510
Toronto, Ontario
Canada M5G 0A3

Telephone 416-977-7599
Toll-free 1-866-678-6427
www.oicr.on.ca

- This security issue was reported to AIM to be fixed
- In the meantime, since all users are currently able to edit SQL code, there is potential for any user to add comments to a query and see query results from other Collection Centres
- Until such a time that the above is corrected in TMx, the Create/Edit Queries privilege has been removed from all User Roles (except OTB Sr Analyst). This means users are currently unable to create/edit queries using either the query wizard or SQL statements

5. Remediation:

No PHI was disclosed and no harm occurred from this limited incident. However, several steps should be taken to prevent such an incident from occurring in the future.

OTB has taken the following action:

1. Removed comments from *Blood-Only Cases excl PROS (> 2 months)* query
2. Reviewed all existing queries to verify no comments exist
3. Temporarily restricted User Roles so OTB Sr Analyst is the only TMx user able to edit queries (both SQL and query wizard)

On September 10, 2015, AIM fixed the role privilege issue i.e. users can only create/edit query using the query wizard – thereby removing the ability to comment. Elise verified the fix and tested it in the demo and stage environments.

On September 22, 2015, Sola and Elise had a meeting with Howard Simkevitz, and it was decided to

Deploy fix 1, a security patch for privileges 3130 View/Edit Query SQL Code, which was corrected by AIM into production on September 23,2015 but users will receive their privilege to Create/Edit Queries (using the query wizard) once it is released by Elise.

The second fix required from AIM is to ensure that comments indicated with "—" in SQL code will not nullify security

- Work with AIM to identify a timeline on delivery of this fix
- In the meantime, Elise will:
  - i. Not write any queries that contain --
  - ii. Test all new SQL queries in the staging environment to check for any potential security breaches before releasing to production.

FOR USE BY MANAGER, POLICIES FOR DOCUMENTATION CONTROL			
Form Title and Number:	General Breach/Report Investigation Form (F-PR-INS.301-01)		
Associated Policy Title and Number:	Policy and Procedures for Privacy Breach Management (PR-INS.301)		
Section Name:	Privacy & Information Security–Privacy	Template Created On:	March 22, 2011

OICR
Ontario Institute for Cancer Research

MaRS Centre
661 University Avenue
Suite 510
Toronto, Ontario
Canada M5G 0A3

Telephone 416-977-7599
Toll-free 1-866-678-6427
www.oicr.on.ca

Related issues:

As this related to an issue with TMx, a previous privacy breach reported by OTB on May 2, 2013, which also involved TMx, was reviewed looking for commonality. It was found to have a different root cause than the current issue.

Other project information: (if applicable)

Other general notes: (if applicable)

Reporting of Breach – Internal Notification

Individual Notified	Notified by:	Date	Time
Privacy Officer	Email	August 25, 2015	8:57 PM
Vice-President, Operations	Email	August 25, 2015	8:57 PM
Information Security Officer	Voice	August 25, 2015	5:00pm.
Other(s):			

External Notification (if required and as necessary):

Individual Notified	Notified by:	Date	Time
Other (describe): Privacy Officer at London Health Sciences Centre	Email	August 25, 2015	9:05 PM

Form completed by: Howard Simkevitz **Signature:**

Date: October 7, 2015

FOR USE BY MANAGER, POLICIES FOR DOCUMENTATION CONTROL			
Form Title and Number:	General Breach/Report Investigation Form (F-PR-INS.301-01)		
Associated Policy Title and Number:	Policy and Procedures for Privacy Breach Management (PR-INS.301)		
Section Name:	Privacy & Information Security–Privacy	Template Created On:	March 22, 2011

MaRS Centre
661 University Avenue
Suite 510
Toronto, Ontario
Canada M5G 0A3

Telephone 416-977-7599
Toll-free 1-866-678-6427
www.oicr.on.ca

Revision History

Document Number	Revision Date (YYYY-MM-DD)	Level of Change	Revision Comments
F-PR-INS.301-01	Not applicable	No Change	New document
F-PR-INS.301-01	2010-09-10	Minor	Revised document
	2011-03-22	Minor	Definition of breach revised as per IPC review
	2011-09-22	Minor	Removed references to "prescribed entities" under definition of breach of privacy – as per feedback from IPCO August 31 2011.

FOR USE BY MANAGER, POLICIES FOR DOCUMENTATION CONTROL			
Form Title and Number:	General Breach/Report Investigation Form (F-PR-INS.301-01)		
Associated Policy Title and Number:	Policy and Procedures for Privacy Breach Management (PR-INS.301)		
Section Name:	Privacy & Information Security–Privacy	Template Created On:	March 22, 2011

Appendix F: Items in Progress from 2014

Item	Status	Actual Completion Date
From 2011 IPC Compliance Recommendation Iron Mountain Agreement: Revise the existing agreement with Iron Mountain to include the requirements of a third party service provider agreement and amend Policy Statement 29.0, Disaster Recovery and Data Storage, in the OICR Information Security Program document accordingly	Contract negotiations are complete.	September 1, 2014
From 2011 IPC Compliance Recommendation Iron Mountain Agreement Develop and implement a written policy and procedures with respect to business continuity and disaster recovery.	Complete	May 19, 2015
The Corporate Risk Register is in draft– requires input from Risk Management Committee and executive approval.	See Part 4 – Organizational Indicators on p. 132 (under "Risk Management")	See Part 4 – Organizational Indicators on p. 132 (under "Risk Management")
Recommendation from PIA Development of Online Privacy Training Mechanism by which Privacy training is delivered (PPT, in-person) should be re-evaluated given logistical challenges in delivering training to many	Complete	First use December 2014

geographically-dispersed individuals (i.e. consider user-led e-training) annually.		
Recommendation from PIA OICR should ensure that any relevant policies from the broader OICR policy framework apply to third-parties as well (i.e., identified in agreements). Contract with AIM should be modified to include clause indicating which policies are applicable to them. This is to be revisited upon contract renewal.	Contract is auto-renewal, however, current contract includes substantive provisions around privacy practices that are in line with the relevant policies from the broader OICR policy framework.	

Appendix G: OTB Privacy Checklist

The following is an excerpt from *F-QA604-01 – Collection Centre Freezer and Operational Audit Agenda* under Section 5. Privacy & Information Security.

5. PRIVACY & INFORMATION SECURITY

	Staff 1	Staff 2
Have both CC staff completed OICR privacy and information security training within the past year? When?		
When do you log out of TissueMetrix? Do you lock your workstation when you leave? Does your screensaver lock automatically with a required password to unlock? (check screensaver setting and report lockout time) Does anyone else (OTB or other) have access to your workstation?		
Do you share your password? Do you write down or store your passwords anywhere? Do you use known words, *etc.*?		
Do you email screenshots (*i.e.*, to AIM or OICR for troubleshooting)? What method do you use to take screenshot? Do you review the screenshot to ensure it does not have any patient identifying information? How do you edit the image to remove PHI?		
Do you use a USB key or laptop? If yes, are they encrypted?		

Can you provide a hypothetical example of a privacy or information security breach? What would you do?		
Have there been any privacy/information security breaches within the last year? Were they reported? To whom?		
Are consent forms kept in a locked cabinet? If yes, who has keys?		
Who has access to the sample storage equipment (*i.e.*, freezer, slide and block cabinets, dry shippers)? Are they locked? If yes, who has keys?		
What other paper documents are retained for the program? Do any contain patient (identifying) information and why is it necessary? Are any printed from TM? How are the documents stored, for how long, and who has access?		
What other electronic files (*i.e.*, spreadsheets) are maintained for the program? Do any contain patient (identifying) information and why is it necessary? Where are the files stored and who can access them (*i.e.*, secure drive)?		
Is any information circulated to other groups (*i.e.*, LMC or surgeons)?		

Describe the detail included.	
Where is your confidential waste bin (for shredding) located? Do you ever place lists/TM printouts within recycling?	

Additional Comments:

Click here to enter text.