Information
and Privacy
Commissioner of
Ontario

Review of the Ontario Institute for Cancer Research in Respect of the Ontario Tumour Bank:

A Prescribed Person under the *Personal Health Information Protection Act*

Ann Cavoukian, Ph.D.
Commissioner
February 2011

Information and Privacy
Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
CANADA

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Review of the Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank:

A Prescribed Person under the *Personal Health Information Protection Act*

The *Personal Health Information Protection Act, 2004* ("the *Act*") is a consent-based statute, meaning that persons or organizations defined as "health information custodians"[1] may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates, subject to limited exceptions where the *Act* permits or requires the collection, use or disclosure to be made without consent.

One such disclosure that is permitted without consent is the disclosure of personal health information to prescribed persons that compile or maintain registries of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances pursuant to subsection 39(1)(c) of the *Act*.

Further, a prescribed entity for the purposes of section 45(1) of the *Act* is permitted to disclose personal health information as if it were a health information custodian to prescribed persons for the purposes of subsection 39(1)(c).

Statutory Provisions Relating to the Disclosure to Prescribed Persons

Subsection 39(1)(c) of the *Act* permits health information custodians to disclose personal health information, without consent, to a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances. The following persons have been prescribed for purposes of subsection 39(1)(c) of the *Act*:

- Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network;
- Cancer Care Ontario in respect of the Colorectal Cancer Screening Registry;
- Cardiac Care Network of Ontario in respect of its registry of cardiac services;

[1] Persons or organizations described in subsection 3(1) of the *Act* that have custody or control of personal health information as a result of or in connection with performing the powers, duties or work of the person or organization.

- INSCYTE Corporation in respect of CytoBase;
- Hamilton Health Sciences Corporation in respect of the Critical Care Information System;
- Children's Hospital of Eastern Ontario in respect of the Ontario Perinatal Surveillance System; and
- Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank.

In order for a health information custodian to be permitted to disclose personal health information to a prescribed person without consent, the prescribed person must have in place practices and procedures approved by the Information and Privacy Commissioner of Ontario ("IPC") to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information pursuant to subsection 13(2) of Regulation 329/04 to the *Act*.

These practices and procedures must also be reviewed by the IPC every three years from the date of their initial approval, pursuant to subsection 13(2) of Regulation 329/04 to the *Act*, in order for a health information custodian to be able to continue to disclose personal health information to a prescribed person without consent, and in order for a prescribed person to be able to continue to collect, use and disclose personal health information without consent as permitted by the *Act*.

Review Process

The *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("*Manual*"), issued by the IPC in 2010, outlines the process that will be followed by the IPC in reviewing the practices and procedures implemented by prescribed persons and prescribed entities to protect the privacy of individuals whose personal information they receive and to maintain the confidentiality of that information. The *Manual* sets out the detailed obligations imposed on prescribed persons and prescribed entities arising from the review and approval process. The *Manual* requires prescribed persons and prescribed entities to have in place practices and procedures to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. At a minimum, the prescribed person or prescribed entity must submit to the IPC the documentation described in Appendix "A" to the *Manual* and the minimum content described in Appendix "B" to the *Manual*.

The Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank submitted the requested documentation on September 17, 2010. Upon receipt, the IPC conducted a detailed review of all the documentation in order to ensure that it complied with the *Manual* requirements. Following the review, on November 12, 2010 a discussion took place with representatives from the Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank to discuss necessary clarifications and minor revisions required by the IPC. Necessary clarifications and revisions were submitted by the prescribed person on November 22, 2010 and on December 16, 2010.

An on-site meeting was held on November 26, 2010 to discuss the practices and procedures implemented by the prescribed person; to provide the IPC with an opportunity to ask questions arising from the documentation provided; and to review the physical, technological and administrative security measures implemented by the prescribed person.

Following the document review and on-site meeting, the Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank was informed of the action that it was required to take prior to the approval of its practices and procedures. Once all necessary action was taken, the IPC prepared a draft report that was submitted to the prescribed person for review and comment.

It must be emphasized that the review by the IPC was limited to personal health information collected, used and disclosed by the prescribed person pursuant to its function as a prescribed person under subsection 39(1)(c) of the *Act* and not with respect to any other role or responsibility that the prescribed person may have.

Description of the Prescribed Person

The Ontario Institute for Cancer Research (OICR) is a federally incorporated not-for-profit corporation funded by the Government of Ontario through the Ministry of Research and Innovation. The OICR is dedicated to research in prevention, early detection, diagnosis and treatment of cancer.

The Ontario Tumour Bank (OTB) is a program of OICR and was established in response to a growing need for a provincial tissue and data bank to support cancer research. The OTB is a multi-centred program which collects blood and tissue samples as well as personal health information from consenting participants and is a source of high quality samples and data for researchers to conduct cancer research.

The OTB coordinates the collection, storage, annotation and distribution of tissue and peripheral blood samples obtained from four Ontario hospitals. The hospitals collect samples from the participants and personal health information from the patient health records. The collection is done with the express written consent of each participant. Each participating hospital maintains a local database of participant personal health information and also stores the locally collected tissue and blood samples.

The participant personal health information collected by the hospitals is subsequently uploaded to the OTB Central Database. Cancer Care Ontario (CCO) hosts and maintains the OTB Central Database for OICR. The software application, TissueMetrix, for the OTB Central Database is provided and supported by the information technology company Artificial Intelligence in Medicine (AIM). Both CCO and AIM provide information technology services to OICR as electronic service providers.

The purpose of the OTB's biospecimen and data collection is to facilitate cancer research through the provision of biospecimens and accompanying clinical data. The samples and de-identified data are disclosed to both academic and industry researchers who conduct research that may result in the development of inventions or discoveries that could provide a foundation for new products, diagnostics, and/or therapeutic agents for cancer patients.

The OTB will continue to obtain express written consent for the provision of samples and personal health information from all new participants. The ability for the OTB to operate as a registry under section 39(1)(c) of the *Act* will permit CCO, and possibly other prescribed entities and persons, to disclose personal health information to the OICR in order to create a more comprehensive and accurate tumour database through data linkages.

Findings of the Review

1. Privacy Documentation

General Privacy Policies, Procedures and Practices

The *OTB Privacy Policy* highlights OICR's policies, procedures and practices with respect to the OTB's collection, use and disclosure of personal health information. It discusses each of the ten principles of the Canadian Standards Association Fair Information Practices as they apply to personal health information in the custody or control of the OTB. OICR is responsible for all data, including personal health information, in its custody or control. The President and Scientific Director of OICR is ultimately accountable for ensuring compliance with the *Act*, its regulation, and the privacy and security policies, procedures and practices implemented. The Privacy Officer and Information Security Officer have been delegated day-to-day authority to manage the privacy program and security program. The *OTB Privacy Policy* states the OICR has administrative, technical and physical safeguards to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. Steps are taken to protect personal health information against theft, loss, unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

The *Development and Management of Policies, Procedures and Guidelines* describes the process for the development of new documents and for the revision of previously issued documents including the document review and approval process. Documents relating to OICR's Privacy and Information Security Program as well as those relevant to OICR prescribed registries, such as the OTB, must be reviewed, at a minimum, on an annual basis.

Transparency

The *OTB Privacy Policy* specifies that the OTB must make information about its policies, procedures and practices related to the management of personal health information readily available on its website and also in printed format upon a request to the OICR Privacy Officer. This information includes the *OTB Privacy Policy*, answers to Frequently Asked Questions, documentation related to the review by the IPC, the *Statement of Purpose for the OTB* and the contact information for the person to whom inquiries, concerns or complaints regarding compliance with the *Act*, its regulation and with the privacy policies, procedures and practices implemented by the OTB can be directed.

The OTB obtains express written consent from the participant donors for the collection of their tissue, blood and personal health information via the four member hospitals where the personal health information and samples are collected. The *OTB Letter of Information and Consent Form* is approved by the Research Ethics Board of each participating hospital.

Collection of Personal Health Information

The *Policies and Procedures for the Collection of Personal Health Information – OTB* states that any collection of personal health information must be consistent with the *Act* and its regulation and the OTB must identify the purpose for which personal health information is collected. The OTB will only collect personal health information that is relevant to its described purpose and will not collect personal health information if other information will serve the purpose and will not collect more personal health information than is reasonably necessary to meet the described purpose. A requestor must submit a request for the collection of personal health information to the OTB Director and the request will be reviewed by the Privacy Officer. If the proposed collection is approved, the OTB Director must ensure that prior to the collection of personal health information, a Data Sharing Agreement or Third Party Services Agreement has been executed between OICR and the applicable organization, a Privacy Impact Assessment has been conducted, and Research Ethics Board approval has been obtained.

The OICR has a *List of OTB Data Holdings* with categories that include the purpose of the data holding/study, the data elements, and who has access to the data. The *Policies and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information* describes the creation, review, amendment and approval of statements of purpose for data holdings containing personal health information.

The *Statement of Purpose for the OTB* describes the OTB and further specifies where the OTB collects personal health information; the type of personal health information the OTB collects; how the OTB uses personal health information; why personal health information is required; to whom the OTB discloses personal health information; how to obtain access to one's own personal health information; and whom to speak to regarding questions, concerns or complaints related to the OTB's information practices and privacy program. The OTB collects tissue and blood samples as well as personal health information from patient health records. Personal health information collected from the patient health record includes demographic information; details of the cancer diagnosis; treatment details; patient and family history of cancer and other risk factors; and outcome information concerning the progression of the disease or the disease-free status. This information is supplemented, with the consent of participants, with data from CCO's data holdings, including the Ontario Cancer Registry, which includes additional outcome, diagnosis and treatment details. The OTB also collects direct identifiers to enable longitudinal and comprehensive data collection. Participant donors are informed that the information collected by OTB will be supplemented with additional information, including identifying information, from other approved organizations, such as CCO. The use, disclosure and retention of data that is collected by the OTB is for maintaining a high quality registry of patient-donated biospecimens and accompanying clinical data for the facilitation of cancer research.

Use of Personal Health Information

The purpose of the *Policy and Procedures for Data Access and Use – OTB* is to ensure that the OTB agents access and use the least identifiable information and minimum amount of identifiable information necessary for carrying out their employment responsibilities. The OTB data consists of records of personal health information from patients who consent to donate tissue samples to the OTB. The OTB is not a research program and internal use of the OTB personal health information and de-identified information for research is not permitted. The only permitted use of the OTB data is for the purpose of carrying out activities related to the OTB operations, e.g. to coordinate distribution of samples and de-identified information to qualified researchers. For most purposes, access to identifying information is not required by the OTB agents. If access is required, the only permitted access to record-level data by OTB agents is read-only access. All access to the OTB data must be approved by the Director, OTB and the Information Security Officer and access is subject to detailed conditions and restrictions. The maximum period for access to the OTB data is one year, users that require ongoing use of the OTB data must again request approval to access the data after the one year expiry date. The *OTB Data Access Log* contains categories including the user name; the data holding; the level/type of access granted to the data holding; the date access was granted/renewed; and the date access to the data holding expires.

Disclosure of Personal Health Information

The *Policy and Procedures for Data Disclosure –OTB* applies to all disclosures of OTB data. The *Policy* states that the OTB is permitted to disclose personal health information for non-research purposes, as permitted by the *Act*. For example, the OTB discloses personal health information to CCO for the purpose of linking the personal health information collected at the participating hospitals to additional information that is in the custody and control of CCO, e.g. data within the provincial cancer registry. The Policy states that this disclosure is permitted under section 49 of the *Act*. The OTB will only disclose personal health information if personal health information is required and de-identified or aggregate data will not serve the purpose; if no more personal health information is being requested than is reasonably necessary to meet the purpose; and if the recipient has in place adequate privacy and security policies and procedures. All disclosures of OTB data for non-research purposes must be reviewed, approved and documented.

The *Policy and Procedures for Data Disclosure – OTB* states that the OTB does not permit personal health information (identifiable record-level data) to be disclosed for research under any circumstances. All data sets disclosed to researchers must be classified as de-identified or aggregate data. In order for de-identified, record-level data to be disclosed, the requestor must submit a request for the data to the OTB Director. The OTB Director will review the request and make a decision to approve or deny it, consulting with the Privacy Officer and Information Security Officer as required. In determining whether to approve the request, the OTB Director must consider whether a data sharing agreement is required, and if so, ensure that one is executed prior to the release of the data. If a data sharing agreement is not required, the OTB Director must ensure that the recipient has acknowledged in writing that they will not use the de-identified data, alone or in combination with any other information including prior knowledge, to attempt to re-identify any individual, link the data to any other data sources, or disclose the data to any third party. The data set must be classified as de-identified record-level data, according to the guidelines set out in the *Re-identification Risk Assessment: The OTB*.

The *Standard Operating Procedure Material and Data Request and Release* describes the processes for ensuring that samples are released from each OTB collection centre along with associated de-identified clinical data from the OTB Central Database only under highly monitored circumstances. With the exception of the *Preliminary Data Report* (which enables the researcher to assess the suitability of each case for their study, and contains a minimal amount of data that has been de-identified), de-identified clinical data will not be disclosed to researchers prior to a *Material Transfer Agreement* being executed and prior to receipt of the Ontario Cancer Research Ethics Board approval. Only the minimum amount of de-identified clinical data required for the research is disclosed. All de-identified clinical data is sent to the researcher from the OICR office, not from the collection centres, through encrypted email. Tissue samples are shipped directly from the collection centres at OICR's request. All documentation pertaining to the release of the de-identified clinical data are securely retained in the OTB offices at OICR.

Data Sharing Agreements

The *Execution of Data Sharing Agreements Policy* outlines the requirements and expectations pertaining to the execution of written data sharing agreements. Other than those involving third party service providers and researchers, data sharing activities involving the collection and/or disclosure of personal health information require the creation of a written data sharing agreement. For example, OICR may enter into a data sharing agreement with a section 45 prescribed entity. The data sharing agreement must identify the purpose(s) for which personal health information is being collected, used and/or disclosed including limitations, conditions and restrictions. No personal health information will be collected or disclosed if other information, namely de-identified and/or aggregate information, will serve the purpose and no more personal health information will be provided than is reasonably necessary to meet the purpose. All parties must act in accordance with the terms specified in the data sharing agreement regarding the secure transfer, retention, return or disposal of personal health information. Violations, including all privacy breaches, will result in termination of the data sharing agreement and all breaches must be reported at the first reasonable opportunity to the OICR contact indicated in the data sharing agreement. OICR maintains a *Log of Data Sharing Agreements*. The *Execution of Data Sharing Agreements Policy* describes the management, tracking and retention of the data sharing agreements and the *Log of Data Sharing Agreements.*

The *Execution of Data Sharing Agreements Policy* requires that all data sharing agreements must, at the minimum, contain the relevant language included in the *Data Sharing Agreement Template*. The *Data Sharing Agreement Template* contains provisions including those related to the collection, use and disclosure of personal health information; technical, administrative and physical safeguards; data breaches; secure transfer, retention, return and disposal of personal health information; training of agents; and protocols for linkage of personal health information. It also contains an acknowledgement form that must be signed by all agents who may be required to access records containing personal health information.

The *Data Sharing Agreement Template* does not set out the specific statutory authority for each collection, use and disclosure contemplated in the data sharing agreement. It is recommended that the *Data Sharing Agreement Template* contain a bracket, e.g. [insert statutory authority for each collection, use and disclosure], to ensure that the specific statutory authority for each collection, use and disclosure is included in all data sharing agreements.

Agreements with Third Party Service Providers

The *Execution of Third Party Service Provider Agreements Policy* requires that a written agreement be entered into with all third party service providers prior to permitting third party service providers access to and use of OICR information assets. The *Policy* requires that no personal health information will be provided to third party service providers if other information, namely de-identified and/or aggregate information will serve the purpose and no more personal health information will be provided than is reasonably necessary to meet the purpose. All parties must act in accordance with the terms specified in the third party service provider agreement regarding the secure transfer, retention, return or disposal of personal health information. Violations, including all privacy breaches, will be subject to termination of the third party service provider agreement and all breaches must be reported at the first reasonable opportunity to the OICR contact indicated in the third party service agreement. OICR maintains a *Log of Third Party Service Agreements*. The *Policy* describes the management, tracking and retention of the third party service agreements and the *Log of Third Party Service Agreements.*

The *Execution of Third Party Service Agreements Policy* requires that all data sharing agreements must, at the minimum, contain the relevant language included in the *Third Party Service Providers Agreement Template*. Schedule C of the *Template* contains provisions related to technical, administrative and physical safeguards. Schedule D of the *Template* contains the varying terms and conditions for the privacy and security of personal health information that must be followed in each of three separate scenarios: when the Third Party Service Provider does not require access to personal health information and is not an agent of OICR; when the Third Party Service Provider requires access to personal health information and is an agent of OICR; and when the Third Party Service Provider requires access to personal health information and is an electronic service provider to OICR. The terms and conditions relate to access, use and disclosure of personal health information; training of personnel; secure transfer, retention, return or disposal of personal health information; data breaches; and privacy audits.

Data Linkage and Data De-identification

The *Policy and Procedures for Data Linkages – OTB* states that the OTB may create data linkages of records of personal health information that are in the custody of the OTB with data from other organizations. The linked data will remain solely in the OTB's custody and control, for exclusive use by OTB. The goal of any data linkage will be to enhance the value of the OTB resource by creating a more comprehensive data set which will be disclosed in a de-identified format to external researchers. A proposal for data linkage must be submitted to OICR's Privacy Officer and Information Security Officer for review. Approval by OICR Senior Management is also required. In order for the linkage to be approved, the source of the data must have the authority to disclose the information to the OTB under the *Act* and its organizational policies; OTB must be authorized to receive the data and create the linkage under the *Act*; the linked data must enhance the value of the OTB as a resource for cancer research; and the least amount of personal health information and the least identifiable personal health information must be used in order to accomplish the linkage. A *Log of OTB Data Linkages* is also maintained.

The *Policy and Procedures for Data Linkages – OTB* describes the procedures for data linkage. The *Policy* states that the minimum amount of personal health information and the least identifiable personal health information will be used to perform linkages and that data will be transferred securely to and from the other organization. The OTB Analyst will coordinate requests for data and will ensure that any files used to facilitate the linkage are securely destroyed once the linkage has been completed. It is recommended that the *Policy and Procedure for Data Linkages - OTB* include more detail as to the specific manner in which the linkage of personal health records must be conducted and include the agent responsible for linking the records.

The *Policy and Procedures for Data Disclosure – OTB* states that all data sets disclosed to researchers must be classified as de-identified or aggregate data and contains a definition of both those terms. The default re-identification risk threshold for de-identified data is 0.2, which is equivalent to a cell size of 5. The OTB Analyst is responsible for ensuring that the data set is classified as de-identified record-level data, according to the guidelines set out in the *Re-identification Risk Assessment – OTB*. The *Re-identification Risk Assessment – OTB* is a detailed report describing a re-identification risk analysis that was performed on the data sets that will be disclosed by the OTB.

Privacy Impact Assessments

The *Privacy Impact Assessment Policy* states that Privacy Impact Assessments (PIAs) will be conducted on existing and proposed data holdings that contain personal health information; when OICR creates a new, or significantly modifies an existing information system, technology or program that involves the collection, use or disclosure of personal health information or otherwise raises privacy issues; when OICR creates or modifies a permanent data linkage that includes personal health information; and as determined by the Privacy Officer in consultation with the Information Governance Committee. The *Policy* also stipulates the minimum required content of PIAs. Once completed, PIAs must be reviewed on an ongoing basis, at a minimum bi-annually, or sooner if privacy risks are identified or if a change is being contemplated. The response to PIA recommendations and the implementation of recommendations and/or amendments are a shared responsibility between the Privacy Officer and the Information Security Officer in consultation with the manager of the program, information system or technology requiring the PIA. The Privacy Officer maintains a *Log of Privacy Impact Assessments* that have been completed; those have been undertaken, but are incomplete; and that have not yet been undertaken.

Privacy Audit Program

The *Policy and Procedures in respect of a Privacy Audit* states that a privacy audit will consist of a review of internal compliance with all relevant privacy polices, procedures and practices to ensure that personal health information is safeguarded against unauthorized access, use and disclosure. The privacy audit will consist of a review of documentation and in person interviews with relevant individuals, including staff. The Privacy Officer assumes primary responsibility for the privacy audit, in collaboration with the Director/Leader of the program/platform. Records of all privacy audits and recommendations arising from the audits are captured in the *Log of*

Privacy Audits and maintained and tracked by the Privacy Officer. The *Policy* states that, at a minimum, the privacy audit will be conducted every two years and more frequently as required. The *Development and Management of Policies, Procedures and Guidelines* further specifies that documents relating to OICR's Privacy and Information Security Program as well as those relevant to OICR prescribed registries must be reviewed, at a minimum, on an annual basis.

The *Third Party Services Agreement Template* states that OICR may assess and review the third party service provider's practices and procedures for reviewing and processing personal health information to ensure that the provider is complying with the privacy and security terms and conditions under the agreement. The *Data Sharing Agreement Template* states that the other party must cooperate with any privacy assessment or audit conducted by OICR or any third party retained by OICR. However, the *Policy and Procedure in respect of a Privacy Audit* only addresses internal compliance with policies, procedures and practices and does not address external audits. According to the *Manual*, with respect to each privacy audit that is required to be conducted, the policy and procedures must set out the purposes of the privacy audit; the nature and scope of the privacy audit; the agent responsible for conducting the privacy audit; and the frequency with which and circumstances in which the privacy audit is required to be conducted. The policy and procedures must require a privacy audit schedule to be developed and must identify the agent responsible for developing the schedule. The policy and procedures must also set out the process to be followed in conducting the audit. The process must include the criteria that must be considered in selecting the subject matter of the audit; whether notification will be provided and, if so, the nature and content of the notification; the documentation that must be completed, provided and/or executed in undertaking the privacy audit and the agent responsible for doing so; the agent to whom this documentation must be provided; and the required content of the documentation. It is recommended that the *Policy and Procedures in respect of a Privacy Audit* be amended to address all the above requirements as related to external audits.

Privacy Breaches, Inquiries and Complaints

The *Policy and Procedures for Privacy Breach Management* outlines the process for managing a breach of privacy or suspected breach of privacy. All individuals employed or engaged by OICR are responsible for reporting privacy breaches, suspected privacy breaches, and/or privacy risks they believe may lead to a privacy breach in the future, to the Privacy Officer and/or the Information Security Officer. The Privacy Officer, Information Security Officer or designate will confirm that the event is a breach and, if so, will assemble the Information Governance Sub-Committee to respond to the breach. The Information Governance Sub-Committee will evaluate the extent of the breach and will evaluate the necessity for further notification and the immediacy of notification. Decisions regarding further notification (e.g. to the President and Scientific Director, Board of Directors, OICR Legal Counsel and/or Ministry of Research and Innovation) will be based on the level of risk of the breach, and on whether the breach is internal or external. The Privacy Officer must ensure that a *General Breach Report/Investigation Form* is completed.

The process of containment is to be initiated by the discoverer of the breach. The Privacy Officer will review the containment measures and determine whether the privacy breach has been effectively contained or whether further containment measures are warranted. The health information custodian or other organization that disclosed personal health information to OICR must be notified at the first reasonable opportunity whenever the personal health information is, or is believed to be, stolen, lost or accessed by unauthorized persons or whenever required pursuant to the agreement with the health information custodian or other organization. In the case of an external breach of personal health information, the IPC will be notified at the first reasonable opportunity. As soon as reasonably possible after becoming aware of the breach an internal investigation will be conducted. At the conclusion of the investigation, a report will be completed by the Privacy Officer and will include a summary of the investigation, and a report on the implementation of the recommendations arising from the investigation. The report will be communicated to the Information Governance Committee and to the OICR Board of Directors in the form of a written report. The *Log of Privacy Breaches* is the responsibility of the Privacy Officer and is used to record all privacy breaches and suspected privacy breaches and to track that all recommendations arising from the investigation are addressed within identified timelines.

The *Policy and Procedures for Privacy Breach Management* provides a definition of the term "privacy breach," however, as per *Manual* requirements, the *Policy* does not define "privacy breach" to include the collection, use or disclosure of personal health information that is not in compliance with the *Act* and its regulations; a contravention of the privacy policies, procedures or practices implemented by the OTB; or a contravention of Data Sharing Agreements, Research Agreements, Confidentiality Agreements and Agreements with Third Party Service Providers retained by the OTB. The definition of "privacy breach" in the *Policy* is also not the same as the definition of "breach of privacy" provided in the *General Breach Report/Investigation Form*. It is recommended that the *Policy and Procedures for Privacy Breach Management* and the *General Breach Report/Investigation Form* be amended to include a complete and consistent definition of the term "privacy breach."

The *Privacy Complaint Policy and Procedures* describes OICR's privacy complaint management process. Information regarding the process for making a privacy complaint is publicly available on OICR's website. The OICR website indicates that complaints regarding OICR's compliance with the *Act* and its regulation can be directed to the IPC. The contact information for the IPC is posted on the OICR website. All written complaints will be referred to the Privacy Officer or designate within 2 business days post receipt. A written response will be sent to the complainant within 30 days of receiving the complaint. In situations where a complaint will not be investigated, the written response will include an acknowledgement of the complaint review; a summary of the outcome of the complaint review; notification that an investigation will not be conducted; information regarding how the complainant may make a complaint to the IPC if there are reasonable grounds to believe that OICR has contravened or is about to contravene the *Act* or its regulation; and the provision of contact information for the IPC. In situations where a complaint will be investigated, the written response will include an acknowledgement of receipt of the complaint; a summary of the outcome of the complaint review and notification that an investigation will be conducted; an explanation of the privacy complaint investigation procedure, indicating whether the complainant will be contacted for further information concerning the privacy complaint; the projected time frame for the completion of the investigation; the nature of the documentation that will be provided to the complainant following the investigation; information regarding how the complainant may make a complaint to the IPC if there are reasonable grounds to believe that OICR has contravened or is about to contravene the *Act* or its regulation; and the provision of contact information for the IPC.

Complaints are classified as either HIGH (i.e. an external complaint related to personal health information or to OICR corporate image or reputation, intellectual property and/or financial matters) or LOW (i.e. internal complaint related to OICR corporate communications, executive and/or employees or related to incorrect process and/or policy interpretation). The Privacy Officer, in consultation with the Information Governance Sub-committee, will review and evaluate all complaints and investigate those that are deemed to be justified (complaints classified as HIGH). A determination as to whether the complaint will be investigated must be made within 15 business days. If a complaint is investigated, the findings of the investigation, including recommendations, the process for implementation, and the recommended timelines for implementation will be included in an investigation report. The Privacy Officer must provide the complainant with written notification of the outcome of the investigation, within 60 days of the outcome. The written notification must include the findings of the investigation; recommended measures (if any) to be taken in response to the privacy complaint; the status of implementation of the recommended measures (if any); information regarding how the complainant may make a complaint to the IPC if there are reasonable grounds to believe that OICR has contravened or is about to contravene the *Act* or its regulation; and the provision of contact information for the IPC. The Privacy Officer maintains a *Log of Privacy Complaints* including investigations occurring as a result of the complaints and remedial action arising from the investigations.

The *Privacy Inquiry Policy and Procedures* states that anyone may make an inquiry about OICR's privacy policies, procedures and practices or OICR's compliance with the *Act* and its regulation. Information regarding the process for making a privacy inquiry is publicly available on OICR's website. The Privacy Officer, in collaboration with the Information Governance Sub-Committee and relevant program/platform leaders will determine the nature of the inquiry and the appropriate response. The Privacy Officer or designate will respond to the inquiry in writing, and, where appropriate, will direct the inquirer to the health information custodian that originally collected the personal health information. The *Log of Privacy Complaints* describes the details of the inquiry, OICR's response to the inquiry, and the implementation of recommendations arising from the inquiry.

2. Security Documentation

General Security Policies and Procedures

The *OICR Information Security Program* document is OICR's overarching information security policy. It contains OICR's security principles and security program objectives, including that personal health information must be protected against theft, loss, unauthorized use or disclosure and that records of personal health information must be protected against unauthorized copying, modification or disposal. The *OICR Information Security Program* document also consists of policy statements related to acceptable use; data classification; encryption; secure electronic data retention, backup, disposal and destruction; data protection (encryption, transmission and storage); access control, identification and authentication; password governance; internet usage; access to OICR systems by contractors, consultants and third parties; information security incident response; risk assessment policy and threat risk assessment guide; change controls; server security; network security; workstation security; personal use of OICR systems; personal third party devices interacting with OICR systems; electronic mail security; extranet security; anti-virus administration; remote access; electronic media destruction; declaration and disposal of surplus IT equipment; helpdesk services security; employees on temporary leave; employees departing OICR; mobile devices security; disaster recovery and offsite data storage; research lab security; loaner devices; restricted or non-networked computer environments; patch management; mobile device allocation; and logging and auditing.

The owner of the OICR security program is the OICR executive team. OICR's Information Security Officer is responsible for executing the development, approval, implementation, management, compliance and enforcement of the *OICR Information Security Program* document.

The *Development and Management of Policies, Procedures and Guidelines* describes the process for the development of new documents and for the revision of previously issued documents including the document review and approval process. Documents relating to OICR's Privacy and Information Security Program as well as those relevant to OICR prescribed registries, such as the OTB, must be reviewed, at a minimum, on an annual basis.

Physical Security

The *Facilities Security Policy for MaRS Location* is applicable to all security incidents involving OICR premises and property. As OICR is a tenant in the MaRS Centre, the responsibility for OICR security is shared with the MaRS security team. OICR has a controlled facilities access system in place such that the door from the elevator to the main reception is open only when the reception desk is staffed; doors to offices and laboratories on other floors and entrances to the laboratories and IT server rooms can only be opened with an access card; and offices and/or cabinetry containing personal health information are kept under lock and key. Access cards must be worn visibly while on OICR premises and individuals must report any loss of keys or access cards immediately. Visitors must sign a Visitor's Log, wear a visitor's badge and can only access OICR premises if they are accompanied by an OICR employee. Visitors who require access to OICR premises for an entire day must sign the Day Pass Access Card Log and are then provided with a Day Pass Access Card. Video surveillance is used and OICR premises are regularly patrolled by MaRS Security.

The *Investigation and Reporting of Facilities Security Incidents for MaRS Location* provides guidance on how facilities security incidents will be investigated and reported. An *Incident Report Form* must be completed for incidents related to facilities security, property damage or theft/loss.

The *Access Card and Key Management for MaRS Location* relates to the management of access cards and keys. It describes the process for issuing access cards and keys and identifies the individuals responsible for auditing access privileges. Access cards and keys are issued on a need to know/as needed basis in order that the OICR individual may fulfil employment, contractual or other responsibilities. In order to obtain Level 3 access (special access) to protected areas within OICR premises, a *MaRS Security Access Card Request Form* and/or a *MaRS Security Key Request Form* must be completed. All OICR individuals who have a key or an access card must report any loss or possible theft immediately to the Facilities Manager so that card access can be cancelled and/or door hardware can be changed at the earliest reasonable opportunity. The Facilities Manager must complete a *MaRS Security Access Card Request Form* prior to reissuing a replacement card. Logs are maintained for auditing of access cards, keys and associated access privileges.

Retention, Transfer and Disposal

The *Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information Policy* relates to paper and electronic records. The *Policy* states that records of personal health information may be retained for only as long as necessary to fulfill the purposes for which the personal health information was collected. There is a *Retention Schedule* that specifies the minimum retention periods for personal health information. Personal health information must be stored in a manner that is appropriate to the sensitivity of the information. The method of record disposal may vary depending on the sensitivity of the information and the storage medium. Secure disposal is defined in the *Policy* as to remove, destroy or rid of material in a manner that is free from risk of loss, interception and reconstruction. At OICR, secure disposal of paper records of personal health information occurs only through the use of third party providers. The *Policy* describes the specific provisions that must be in the third party agreement when a third party service provider is contracted to retain or dispose of records of personal health information on behalf of OICR. The third party agreement must include the manner for securely transferring, retrieving and/or disposing the records; the conditions pursuant to which the records will be transferred, retrieved and/or disposed; documentation of the date, time and mode of transfer of the records; maintenance of a detailed inventory of transferred and retrieved records; provision of written confirmation to OICR as to receipt of confidential records; and provision of certificates of destruction immediately following disposal of records confirming the secure disposal of the confidential records, the date, time and method of secure disposal employed, and the name and signature of the agent(s) who performed the secure disposal. Third party service providers engaged to dispose of personal health information (such as shredding of paper records or electronic media) are to be instructed by OICR as to the appropriate standard to be used, and this standard must be documented in the third party service provider agreement (e.g. paper should be cross-cut shred to a standard of 3/8" maximum).

The Sending/Receiving Personal Information, Personal Health Information and Confidential/ Sensitive Information Policy specifies that the preferred method for transmitting de-identified health information is via courier or via encrypted files for electronic transmission. Records containing personal health information must never be transmitted via fax or via scanning from an OICR shared photocopy machine to an email account. The preferred method for transmitting personal health information is via courier. Email may not be used to transmit identifiable personal health information unless approval is granted from the Privacy Officer and/or the Information Security Officer prior to each email transmission. If approval is granted, the email must be encrypted using OICR supplied and supported encryption methodologies and tools.

The *Clean Desk Policy* sets guidelines which reduce the risk of a security breach, fraud and information theft caused by documents being left unattended by OICR individuals. For example, the *Policy* requires personal health information to be locked in a secure location when an employee is away from his or her desk.

Policy Statement 4.0, Secure Electronic Data Retention, Backup, Disposal and Destruction, in the *OICR Information Security Program* document provides requirements related to electronic records retained, received or created by OICR. For example, the *Policy Statement* specifies that all personal health information must be saved on OICR file servers and classified by data owners and all data destruction processes involving personal health information are to be documented by a certificate of destruction. Data that is slated for disposal and destruction is permanently deleted using a minimum of a seven pass deletion method.

Policy Statement 3.0, Encryption, in the OICR Information Security Program document describes the encryption standards required by OICR technology users. *Policy Statement 5.0, Data Protection (Encryption, Transmission and Storage)*, further specifies that the primary storage of Level 4 data (such as personal health information) must be on OICR file servers and it must be strongly encrypted during both storage and transmission. *Policy Statement 22.0, Remote Access*, describes standards and procedures required for remote access to OICR resources. Only OICR-approved remote access hardware and software can be used to access OICR networks remotely. Personal health information accessed via remote access must never be saved locally on non-OICR hardware, hard drives or servers.

Policy Statement 28.0, Mobile Devices Security, in the OICR Information Security Program document, states that personal health information must not be stored on mobile devices and defines mobile devices as Blackberry and Apple iPad only. However, *Policy Statement 3.0, Encryption*, states that the use of removable media, such as USB keys, storing data classified as Level Three and Level Four (which includes personal health information) is prohibited *unless* approval is provided by the Information Security Officer and Privacy Officer. The Office of the Information and Privacy Commissioner considers removable media, such as USB keys, to be mobile devices. Since, according to *Policy Statement 3.0*, there is a possibility that personal health information could be stored on USB keys, it is recommended that *Policy Statement 3.0, Encryption* be revised to include the additional requirements specified in the *Manual* regarding storing personal health information on mobile devices, as described below.

Policy Statement 3.0 must identify the process that must be followed for receiving, reviewing and determining whether to approve or deny a request for the retention of personal health information on a mobile device including any documentation that must be completed, provided and/or executed; the agent 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.

Policy Statement 3.0 must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for the retention of personal health information on a mobile device. At a minimum, prior to any approval of a request to retain personal health information on a mobile device, the *Policy* must require the agent(s) 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; that no more personal health information will be retained on the mobile device than is reasonably necessary to meet the identified purpose; and that the use of personal health information has been approved pursuant to the *Policy and Procedures for Data Access and Use –OTB*. The *Policy* should 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.

Policy Statement 3.0 must identify the conditions or restrictions with which agents granted approval to retain personal health information on a mobile device must comply. At a minimum, the agents must be prohibited from retaining personal health information on a mobile device if other information, such as de-identified and/or aggregate information will serve the purpose; de-identify the personal health information to the fullest extent possible; be prohibited from retaining more personal health information on a mobile device than is reasonably necessary for the identified purpose; be prohibited from retaining personal health information on a mobile device for longer than necessary to meet the identified purpose; and ensure that the strong and complex password for the mobile device is different from the strong and complex passwords for the files containing the personal health information and that the password is supported by "defence in depth" measures.

Policy Statement 3.0 must also detail the steps that must be taken by agents to protect the personal health information retained on a mobile device against theft, loss and unauthorized use or disclosure and to protect the records of personal health information retained on a mobile device against unauthorized copying, modification or disposal. *Policy Statement 3.0* must also require agents to retain the personal health information on a mobile device in compliance with the *Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information Policy* and to securely delete personal health information retained on a mobile device in accordance with the process and in compliance with the time frame outlined in the *Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information Policy*.

Information Security

Policy Statement 1.0, Acceptable Use, in the *OICR Information Security Program* document specifies the acceptable and appropriate use of OICR's information technology and assets. The Director, IT must review and approve requests for exceptions to acceptable use. *Policy Statement 8.0, Internet Usage*, states that OICR reserves the right to monitor all communications technologies within OICR and describes prohibited internet usage as well as procedures for wireless access to the OICR network. *Policy Statement 16.0, Personal Use of OICR's Systems*, specifies the standards that must be followed when stakeholders are using the OICR network/internet access for personal use. *Policy Statement 17.0, Personal/Third Party Devices Interacting with OICR Systems*, describes the standards that are required when devices not owned by OICR are used to access OICR's information technology resources. For example, non-OICR mobile devices may not be used for storing or accessing level 4 data such as personal health information. *Policy Statement 18.0, Electronic Mail Security*, outlines the required standards for using OICR-managed email, including those related to approved email access technologies; forwarding emails; prohibited content in email messages; remote access to email; management of email messages; email monitoring/audits; and SPAM filtering.

Policy Statement 7.0, Password Governance, in the *OICR Information Security Program* document describes standards and procedures relating to password definition, password storage and protection and password expiry. *Policy Statement 15.0, Workstation Security* states that all on-site workstations must have a time-delineated password-protected screensaver that locks screen access within 20 minutes of inactivity and all users must lock their computer screens in a password-protected manner when they are away from their desks.

Policy Statement 12.0, Change Controls (OICR Production Servers), in the OICR Information Security Program document, requires all changes to applications, operating systems or services at any level on any OICR production servers to proceed through a change control procedure. It specifies the required procedures related to change request submission, review, implementation, completion and enforcement. *Policy Statement 33.0, Patch Management*, requires all OICR managed computer equipment to have up-to-date security-related patches. It specifies standards and procedures related to subscribing to security alert services, obtaining technical approval for patches, and testing and implementing the patches.

Policy Statement 29.0, Disaster Recovery and Offsite Data Storage, in the OICR Information Security Program document states that all data stored on OICR's network file servers is backed up to tape and stored both on-site and off-site. Almost all system administration work can be done remotely and critical systems can continue to function during major power failures for up to seven days. Every week a copy of the backup tapes is sent to Iron Mountain, an off-site storage facility. The tapes are transported in a secure manner, for the retention period defined by the data owner, after which time they are recalled to OICR for destruction.

Policy Statement 29.0, Disaster Recovery and Offsite Data Storage, does not specify that a written agreement must be executed with a third party service provider (e.g. Iron Mountain) containing language from the *Third Party Services Agreement Template* and identifying the agent responsible for ensuring the agreement has been executed prior to transferring the backed-up records of personal health information to the third party service provider. According to OICR, revisions to the existing agreement with Iron Mountain are currently being reviewed to include the requirements of a third party service provider agreement. It is recommended that the agreement with Iron Mountain be revised and *Policy Statement 29.0, Disaster Recovery and Offsite Data Storage* be amended accordingly.

Policy Statement 29.0, Disaster Recovery and Offsite Data Storage, also does not address the agent responsible for testing the procedure for backup and recovery of records of personal health information, the process that must be followed in conducting such testing, and any documentation that must be completed, provided and/or executed by the agent responsible for testing. According to OICR, there is no specific policy for testing the procedure for backup and recovery of records of personal health information at this time however this will be implemented prior to moving the hosting of the OTB servers from CCO to OICR. It is recommended that *Policy Statement 29.0, Disaster Recovery and Offsite Data Storage* be amended to address testing the procedure for backup and recovery of records of personal health information.

Security Audit Program

Policy Statement 37.0, Logging and Security Audits, in the OICR Information Security Program document states that system security events are logged to a centralized logging server and copied to a secure logging server. The *Policy Statement* describes the scheduled weekly, quarterly, monthly and annual audits. Scheduled audits include a quarterly review of the active directory to verify that only active employees have active accounts; a quarterly computer domain account audit to ensure that only current user's computers are connected to the domain account; a quarterly review of Unix server log on failure to analyze logs and investigate anything unusual; quarterly network port scans; annual inspection of all workstations to confirm the 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; and, no less than weekly, monitoring security event logs on the active directory for log on failures. Unscheduled audits are also performed and can consist of the same audits as the scheduled audits as well as forensic analysis of computers; deep packet analysis; extensive analysis of logs; computer memory, disk logs, caches or events; network monitoring; and firewall log auditing. The Information Security Officer assumes primary responsibility in ensuring regular and timely completion of security audits and has additional responsibilities including assigning IT team members to address the recommendations arising from a security audit; establishing timelines to address the recommendations; and ensuring that communication of the relevant findings and recommendations are disseminated to the Information Governance Committee and the OICR Board of Directors in the form of a summary report. At a minimum, a summary report will be provided on an annual basis.

Policy Statement 37.0, Logging and Security Audits, does not specify that system control and audit logs must be immutable and does not set out the procedures that must be implemented in this regard and the agent(s) responsible for implementing these procedures. According to OICR, logs are not fully immutable, but OICR is working on making them immutable for systems that deal with personal health information. It is recommended that OICR revise its practices to ensure that logs are immutable and amend *Policy Statement 37.0, Logging and Security Audits*, accordingly.

Policy Statement 11.0, Risk Assessment and Threat Risk Assessment, in the *OICR Information Security Program* document, states that OICR performs Threat Risk Assessments every other year or prior to introducing new systems housing personal health information. As well, internal vulnerability audits or scans take place on an ongoing basis, overseen by internal IT Security Administrators. These audits consist primarily of scanning for open ports and ensuring ports that should not be open are closed. Third party personnel are also retained annually to audit systems for vulnerabilities. *Policy Statement 20.0, Anti-Virus Administration*, states all OICR computers with Windows operating systems are actively scanned, in real-time, for viruses.

The ***Policy and Procedures for Data Access and Use – OTB***, describes additional scheduled audits that take place to review active accounts and access to the OTB Central Database. The OTB Analyst is responsible for performing these audits, maintaining related documentation, notifying the Information Security Officer of the audit findings, and reporting any suspected breaches. The Privacy Officer and Information Security Officer are responsible for conducting audits every two years to assess compliance with respect to privacy and information security related policies and procedures.

Information Security Breaches

Policy Statement 10.0, Information Security Incident Response, in the OICR Information Security Program document, requires that all information security incidents, regardless of scope or perceived scope, must be reported to the IT Help Desk or to the Information Security Officer immediately. Any information security incident found to involve personal health information, including any contravention of OICR's security policies, procedures or practices involving personal health information, will constitute an information security breach. For these events the Information Security Officer will initiate a parallel investigation with the Privacy Officer as per OICR's *Policy and Procedures for Privacy Breach Management* to determine if the information security breach resulted in a breach of privacy. Notification to any organization whose information is deemed to have been breached will be in accordance with the *Policy and Procedures for Privacy Breach Management*. The *Policy Statement* describes the required steps to be taken in response to an information security incident, including steps related to incident detection and recording; incident ownership, monitoring, tracking and communication; classification; containment; notification; resolution and recovery; documentation; evidence preservation; and incident closure. Information documented includes the name of the individual who discovered the incident, and that person's contact details; the date and time the incident was reported; the nature of the incident including how and when the incident was detected; the OICR systems administrator or persons involved; the name of the system being targeted, along with the operating system, IP address, and location of the system; any information about the origin of the attack, including IP addresses if applicable; the severity or impact of the incident; the category of the incident; how the incident occurred; other information related to a potential attacker; the response plan that was developed; what was done to respond to the incident, including the containment measures implemented; and the effectiveness of the response.

3. Human Resources Documentation

Privacy and Security Training and Awareness

The *Privacy and Information Security Training and Awareness Policy* requires all individuals newly employed or engaged by OICR to receive privacy and information security training at the commencement of their employment/engagement, and/or prior to being given access to research data including personal health information. Both the OICR Privacy Officer and Information Security Officer are responsible for preparing and delivering privacy and information security training to all OICR individuals. Training and education for individuals who require access to data that may contain personal health information, for example employees within the OTB, will be more specialized and extensive to meet the needs of these individuals (e.g. role-based training). An acknowledgement of completion of training and of compliance with all OICR privacy and information security policies and procedures will be documented by signing the *Privacy and Information Security Attestation Form* (*Attestation Form*). Training will be renewed on an annual basis for all OICR individuals, and/or more frequently as required, to address all new privacy and information security policies and/or significant amendments made thereto. The *Attestation Form* must be re-signed every year. OICR also designates a month each year to the topic of privacy awareness, during which communication tools are used to help foster a culture of privacy and information security. Electronic logs of privacy and information security training are completed, maintained and retained by OICR's Human Resources to track all individuals who have undergone initial and ongoing training and who have signed the *Attestation Form* (annually) and the *Confidentiality Agreements*.

Confidentiality Agreements

The *Confidentiality of Information Policy* outlines the requirements and expectations when handling confidential information (including personal information, personal health information, corporate information or proprietary information) to ensure that confidential information is protected and preserved. All employees, students, volunteers, consultants, contractors or other associates or workers of OICR are required to read and sign the OICR *Confidentiality Agreement* prior to commencing work. *Confidentiality Agreements* must be signed by all OICR individuals on an annual basis. A *Log of Executed Confidentiality Agreements* is maintained. The *Policy* contains a chart outlining the management and retention of the *Log of Executed Confidentiality Agreements* as well of the signed *Confidentiality Agreements*.

The OICR *Confidentiality Agreement* requires the signee to comply with OICR's policies as well as with the *Act* and its regulation. The signee is prohibited from collecting and using personal health information except as permitted by the *Confidentiality Agreement*; from disclosing such information except as permitted by the *Confidentiality Agreement* or as required by law; 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. On cessation of the signee's relationship with OICR, or as requested by OICR, whichever is earliest, the signee must immediately cease the use of any and all information, return all information and copies to OICR or destroy such information in accordance with the written direction of OICR, and return all other property to OICR at the first reasonable opportunity. The signee must immediately report any privacy breaches or suspected privacy breaches relating to personal health information to the Privacy Lead or manager and to the Privacy Officer or the Information Security Officer.

Responsibility for Privacy and Security

According to the OICR *Privacy and Information Security Accountability Terms of Reference*, the Privacy Officer is responsible for the day to day operations of the privacy program within OICR and for compliance with OICR privacy and data access policies. Responsibilities of the Privacy Officer include developing, implementing, reviewing and amending privacy policies, procedures and practices; ensuring the transparency of, and compliance with the privacy policies, procedures and practices; and facilitating compliance with the *Act* and its regulation. The Information Security Officer is responsible for the day to day management of the security program including providing assurance that the technical and administrative safeguards for OICR data assets are adequate to meet policy and regulatory requirements. Responsibilities of the Information Security Officer include developing, implementing, reviewing and amending security policies, procedures and practices and ensuring compliance with the security policies, procedures and practices implemented. The Privacy Officer and the Information Security Officer both report to the Vice-President Operations.

Termination of Relationship

The *Termination Policy* states that as of the effective date of resignation, retirement, contract or employment termination or dismissal, all access to OICR's electronic resources and access to office premises will be immediately terminated by IT and Facilities as appropriate. As of the effective date, all OICR property, including IT assets, files and data, equipment, access cards, keys and employee ID cards, must also be immediately returned to the employee's manager. The manager will sign-off on receipt of all returned property by filling in the *Termination Checklist: Receipt of Property and Assets*. Termination of electronic access will be confirmed and signed off by filling in the *Termination Checklist: Termination/Suspension of Access* to OICR Electronic Resources. Where an employee fails to return any OICR property, the employee's manager will be responsible for devising and implementing further action as required.

Discipline

The *Progressive Discipline Policy* states that a decision to take any progressive disciplinary action against an employee must be discussed between the employee's manager and Human Resources prior to being implemented. The manager must ensure that confidentiality is protected at all times. When a concern regarding an employee's conduct is raised with a manager, the manager will conduct a preliminary investigation. The course of progressive discipline depends on factors including the nature of the misconduct, the employee's disciplinary history, and other factors such as outcomes resulting from the investigation into the alleged misconduct. Following the investigation, a typical progression of discipline for each act of misconduct would be verbal warning(s), written warning(s), paid suspension, and termination. OICR may skip or accelerate steps of discipline that support a more serious response based on the employee's conduct and/or employment record. Where there is evidence that a fundamental breach of the employee relationship has occurred, including breaches of privacy, and the continuation of the employee relationship is no longer viable, OICR reserves the right to impose immediate dismissal.

4. Organizational and Other Documentation

Governance

The OICR *Privacy and Information Security Accountability Terms of Reference* states that OICR's Privacy and Information Security Program is managed by the Vice-President, Operations and is supported by individuals and groups including the Privacy Officer, the Information Security Officer, Program Privacy Leads (each program/group at OICR has a designated Privacy Lead), the Information Governance Committee, and the Information Governance Sub-Committee. The Information Governance Committee acts in a high level advisory role to support the privacy and security programs in addressing significant information management issues including privacy, security, and data access. The Information Governance Sub-Committee acts in a hands-on advisory role to support privacy and security audit, inquiry, complaint, breach management and incident issues. The *Terms of Reference* describes the responsibilities, membership, meetings and reporting requirements for the Information Governance Committee, the Information Governance Sub-Committee and the Privacy Leads. The Privacy Officer and Information Security Officer submit quarterly reports to the Information Governance Committee and to the senior management team. Noteworthy items in the quarterly reports are summarized in an annual report for senior management, and senior management then shares the annual report with the Board of Directors.

Risk Management

The *Policy and Procedures for Maintaining a Consolidated Log of Recommendations* requires the Privacy Officer to update OICR's *Consolidated Log of Privacy and Information Security Recommendations (Log*) each time that a privacy impact assessment, privacy or security audit, investigation of a privacy breach, security breach or privacy complaint, or a review by the IPC has been completed, and from which recommendations were identified. The Privacy Officer must also update the *Log* once a recommendation has been addressed. To ensure recommendations are being implemented as per the agreed upon implementation date, the Privacy Officer will review the *Log* twice annually, and will connect with the appropriate individual designated responsible for the implementation of the recommendation, as required.

OICR's *Corporate Risk Management Policy* contains definitions of terms such as risk evaluation, risk identification and risk management. The *Policy* includes methods to determine risk rating, risk response, and risk monitoring and identifies sources of risk and areas of impact. Risk responses, including assessment of the risk and mitigation plan(s), will be recorded by the affected individual to whose area of responsibility the risk directly relates in the OICR *Corporate Risk Register*. The *Policy* specifies who is responsible for risk management, for example, the OICR Director, OTB is responsible for ensuring that the OTB identifies and addresses any privacy risks related to the operation of the OTB as a prescribed entity under the *Act*.

Business Continuity and Disaster Recovery

OICR did not provide the IPC with a policy and procedures related to business continuity and disaster recovery. It is recommended that OICR develop and implement a policy and associated procedures to protect and ensure the continued availability of the information technology environment of the OTB in the event of short and long-term business interruptions, and in the event of threats to the operating capabilities of the OTB, including natural, human, environmental and technical interruptions and threats.

Summary of Recommendations

It is recommended that OICR in respect of the OTB address the recommendations detailed in this report prior to the next review of its practices and procedures. In summary, it is recommended that OICR in respect of the OTB:

1. Amend the *Data Sharing Agreement Template* to set out the specific statutory authority for each contemplated collection, use and disclosure.
2. Amend the *Policy and Procedures for Data Linkages – OTB* to provide more detail as to the specific manner in which the linkage of personal health records must be conducted and the agent responsible for linking the records.
3. Amend the *Policy and Procedures in respect of a Privacy Audit* to address requirements related to external audits.
4. Amend the *Policy and Procedures for Privacy Breach Management* and *the General Breach Report/Investigation Form* to include a complete definition of the term "privacy breach."
5. Amend *Policy Statement 3.0, Encryption*, in the *OICR Information Security Program* document, to include all the requirements pertaining to retaining personal health information on a mobile device.
6. 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.
7. Amend *Policy Statement 29.0, Disaster Recovery and Offsite Data Storage*, in the *OICR Information Security Program* document, to address testing the procedure for back-up and recovery of records of personal health information.
8. Develop immutable system control and audit logs and amend *Policy Statement 37.0, Logging and Security Audits*, in the *OICR Information Security Program* document accordingly.

9. Develop and implement a written policy and procedures with respect to business continuity and disaster recovery.
10. Ensure that initial and ongoing privacy and security training addresses the new privacy and security policies, procedures and practices implemented by OICR and the significant amendments to existing privacy policies, procedures and practices.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that OICR in respect of the OTB has in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. According, effective February 15, 2011, the practices and procedures of OICR with respect to the OTB have been approved by the IPC.

In order to synchronize the timing of the IPC's review of OICR in respect of the OTB with the reviews of other prescribed persons, this approval will remain effective until October 30, 2011. Prior to September 1, 2011, OICR should submit to the IPC a letter describing the steps taken to address the recommendations outlined in this report so that the IPC may review and approve these practices and procedures effective October 31, 2011 for a further period of three years.

Information and Privacy
Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca