ONTARIO TUMOUR BANK PRIVACY POLICY

1.0 Introduction

The Ontario Institute for Cancer Research (OICR) is a centre of excellence in cancer research with a focus on prevention, early detection, diagnosis and treatment of cancer. OICR is a federally incorporated not-for-profit corporation funded by the Government of Ontario.

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 that collects blood and tissue samples as well as personal health information (PHI) from consenting volunteer participants. The OTB is a source of high quality samples and data for 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. Information about the OTB is publicly available on the OTB website at www.ontariotumourbank.ca.

Under section 39(1)(c) of the Personal Health Information Protection Act, 2004 (PHIPA), the Ministry of Health and Long-Term Care has prescribed the OICR in respect of the OTB as a registry of personal health information. In order to fulfill this role, OICR 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 and approval by the Information Privacy Commissioner/Ontario (IPC) every three years.

2.0 Scope

This document highlights OICR's policies, procedures, and practices with respect to OTB's collection, use and disclosure of personal health information as described under PHIPA, and is based on the 10 principles of the Canadian Standards Association Fair Information Practices, which form part of Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA). This document discusses each of these principles individually as they apply to PHI in the custody or control of OTB. OTB collects, uses and discloses PHI to facilitate the conduct of cancer research in accordance with all applicable legislation, including PHIPA and its regulation and is committed to ensuring compliance with PHIPA.

3.0 Definitions

Personal Health Information (PHI): As per Ontario's Personal Health Information Protection Act (PHIPA), 2004, PHI is defined as identifying information about an individual in oral or recorded form. It includes information about an individual's health or history as it:

(a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;
(c) is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual;
(d) relates to payments or eligibility for health care in respect of the individual;
(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;
(f) is the individual's health number; or
(g) identifies an individual's substitute decision maker.

Identifying Information: As per Ontario's Personal Health Information Protection Act (PHIPA), 2004, identifying information means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

4.0 Policy

The following sets out how OICR adheres to these principles with respect to the OTB.

4.1 Principle 1 – Accountability

The OICR has a commitment to comply with the provisions of PHIPA, 2004 and its regulation applicable to prescribed persons (or prescribed Registries). OICR is responsible for all data, including PHI, in its custody or control and designates individuals who are accountable for the organization's compliance with the following principles.

The President and Scientific Director of OICR is ultimately accountable for ensuring compliance with PHIPA, 2004 and its regulation and for ensuring compliance with the privacy and security policies, procedures and practices implemented. The President and Scientific Director has delegated the day-to-day responsibility to the Vice-President, Operations, who is responsible for ensuring that OICR meets its 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 program and security program.

A matrix reporting structure is in place for both of these positions to report to the Vice-President, Operations for this purpose. Other positions and committees that support the privacy and security programs include the OICR Program Privacy Leads and OICR Information Governance Committee. The duties and responsibilities of these positions, along with the key activities of the privacy and security programs, are described in OICR's Privacy and Information Security Accountability Terms of Reference.

4.2 Principle 2 – Identifying Purposes

OTB ensures that any collection of PHI is consistent with the collection of PHI permitted by PHIPA, 2004 and its regulation. OTB identifies the purposes for which PHI is collected.

Specifically, potential tissue and blood donors are informed of the purposes for the collection of their PHI and biospecimens and the potential uses of their data and biospecimens via an informed consent process administered by agents of the hospitals participating in the collection of data and samples for OTB. These hospitals are classified under PHIPA as 'health information custodians' (HICs). In addition, a Statement of Purpose and Frequently Asked Questions document describing the purpose for the data collection are made available on the OTB website, www.ontariotumourbank.ca.

OTB only collects, uses, and discloses personal health information that is relevant to its described purpose, which is to maintain a high quality registry of patient-donated biospecimens and accompanying clinical data for the facilitation of cancer research. PHI that does not meet the specific requirements of OTB, and that it is not reasonably necessary to meet the described purpose, will not be collected.

The purpose of OTB's biospecimen and data collection is to facilitate cancer research through the provision of biospecimens and data in the custody of the OTB to approved researchers. The samples and de-identified data are disclosed to both academic and to 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 types of PHI collected include demographic information (*e.g.*, age, sex), details of the cancer diagnosis (*e.g.*, type of cancer, grade, stage), 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. OTB also collects direct identifiers (*e.g.*, name, date of birth, medical record number) to enable longitudinal and comprehensive data collection.

The information is collected and maintained within the OICR data holding entitled the Ontario Tumour Bank Central Database. An individual may obtain more information about this data holding and the purposes, data elements, and data sources by referring to the Statement of Purpose listed on the OTB website: www.ontariotumourbank.ca.

4.3 Principle 3 – Consent

The OTB obtains express written and knowledgeable consent from the patient donor for the collection of their tissue, blood and personal health information. This is done via the member hospitals (HICs) where the PHI and samples are collected. It is OTB's policy that express consent be provided by the individual donor, and not by their substitute decision maker or next of kin. Additionally, the OTB does not seek consent from individuals who are under 18 years of age (*i.e.*, all donors must be older than 18 years of age). A general description of the potential uses of the samples and data is provided to donors in the consent form.

A donor may revoke his/her consent at any time. Written requests to revoke consent are addressed to the designated HIC where consent was obtained. If the donor does not wish to revoke his/her consent in writing, he/she may contact the designated contact person at the HIC and this information is provided on the consent form. In the event that samples from a donor who has revoked his/her consent have been distributed to a researcher, the de-identified data that accompanied that sample(s) may be used for the approved research and the samples and data already distributed will not be returned. All limitations regarding the withdrawal of consent by a donor are set out in the consent form.

4.4 Principle 4 - Limiting Collection

OTB ensures that any collection of PHI is consistent with the collection of PHI permitted by PHIPA, 2004 and its regulation. OTB has a commitment 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. Refer to Policy and Procedures for the Collection of Personal Health Information - Ontario Tumour Bank which outlines the policies, procedures and practices implemented by the OTB to ensure that both the amount and the type of PHI collected is limited to that which is reasonably necessary for its purposes.

4.5 Principle 5 – Limiting Use, Disclosure and Retention

OTB ensures that any use or disclosure of PHI is consistent with the use or disclosures of PHI permitted by PHIPA, 2004 and its regulation. 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 purpose.

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.

OTB remains responsible for PHI used by its agents. Refer to Policy and Procedures for Data Access and Use - Ontario Tumour Bank, which 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 only discloses de-identified clinical data to researchers for the purposes of research. OTB does not permit PHI (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.

OTB is permitted to disclose PHI for non-research purposes in specified circumstances as permitted by PHIPA, 2004 and its regulation. For example, OTB may disclose PHI to Cancer Care Ontario (CCO) for the purpose of linking the PHI collected at the participating hospitals to additional information that is in the custody and control of CCO (*e.g.*, data within OCRIS, the provincial cancer registry). This disclosure is permitted under s. 49 of the Act. OTB will disclose PHI only if de-identified or aggregate data will not serve the purpose.

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 OICR and 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.

The OTB ensures the secure retention of PHI in both paper and electronic form. PHI is retained by OTB for only as long as necessary for the fulfillment of the identified purposes. PHI that is no longer required for the identified purposes is destroyed in a secure manner to ensure that reconstruction of the PHI is not reasonably foreseeable in the circumstances. The OICR has policies, procedures and practices implemented to govern the secure retention, transfer and disposal of records of PHI.

Refer to OICR's policies on the Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information, Clean Desk Policy, Sending/Receiving Personal Health Information, Personal Information and Confidential/Sensitive Information, Investigation and Reporting of Facilities Security Incidents for MaRS Location, Access Card and Key Management for MaRS Location, Facilities Security Policy for MaRS Location, and the Log of Access to OICR Premises. Also refer to OICR's Policy Statements: 3.0 Encryption, 4.0 Secure Electronic Data Retention, Backup, Disposal and Destruction, 5.0 Data Protection (Encryption, Transmission and Storage), 7.0 Password Governance, 15.0 Workstation Security, 22.0 Remote Access, 23.0 Electronic Media Destruction, 28.0 Mobile Devices Security, 29.0 Disaster Recovery and Offsite Data Storage and the OTB SOP TB312 Material and Data Request and Release.

4.6 Principle 6 – Accuracy

PHI shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. HICs (hospitals) that transfer PHI to OTB are responsible for ensuring the PHI is accurate, complete and up-to-date for the purposes specified. OTB facilitates and conducts training meetings and data quality programs to ensure the quality of PHI in its custody for the intended purposes is accurate, complete and up-to-date. Data within OTB is not intended for the purpose of directing patient care at any time. Donors requesting access to their PHI will be directed to the HIC (hospital) where the original information and biospecimens were collected.

4.7 Principle 7 – Safeguards

OICR considers all PHI in its custody to be highly sensitive and implements appropriate safeguards to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information. Steps are taken to protect PHI against theft, loss and unauthorized use or disclosure and to protect records of PHI against unauthorized copying, modification or disposal.
The safeguards in place include:

- Administrative safeguards: *e.g.*, privacy and information security policies and procedures, privacy and information security training for staff, access to PHI on a "need to know" basis, disclosures of de-identified clinical data only (no PHI) for research purposes;
- Technical safeguards: *e.g.*, firewalls, separation of networks, secure servers, password/account user authentication, data encryption, audit logs, backup and recovery systems; and
- Physical safeguards: *e.g.*, secure facilities with monitored access, secure work areas.

4.8 Principle 8 – Openness

OTB makes information about its policies, procedures and practices related to the management and protection of PHI readily available on its website at www.ontariotumourbank.ca and in printed format by direct request to the OICR Privacy Officer.

This information includes:

- OTB privacy policy;
- Answers to Frequently Asked Questions (FAQs) related to the privacy policies, procedures and practices implemented by OTB;
- Documentation related to the review by IPCO of the policies, procedures and practices implemented by OTB to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information;
- Statement of Purpose for OTB; and
- The name and/or title, mailing address and contact information for the person(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with PHIPA and its regulation can be directed.

The FAQs must contain the following minimum content:

- A description of the status of the OTB under PHIPA;
- A description of the duties and responsibilities arising from this status;
- A description of the privacy policies, procedures and practices implemented in respect of PHI including:
    - The types of PHI collected and the persons or organizations from which this PHI is typically collected;
    - The purposes for which PHI is collected;
    - The purposes for which PHI 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 PHI is disclosed and the persons or organizations to which it is typically disclosed.

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

The FAQs should also provide the name and/or title, mailing address and contact information of the person(s) 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 can be directed.

4.9 Principle 9 – Individual Access

Donors requesting access to their PHI will be directed to the HIC (hospital) from whom the PHI was collected.

4.10 Principle 10 – Challenging Compliance

An individual is able to submit an inquiry, concern or complaint related to the privacy policies, procedures and practices of the OTB and/or related to OTB's compliance with PHIPA, 2004 and its regulation. All inquiries, concerns or complaints should be submitted in writing and addressed to the OICR Privacy Officer, as set out below. Inquiries and complaints will be dealt with in accordance with OICR's Privacy Inquiry Policy and Procedures and Privacy Complaint Policy and Procedures, respectively.

Ontario Institute for Cancer Research
Attn: Privacy Officer
Ontario Institute for Cancer Research
MaRS Centre, West Tower
661 University Avenue, Suite 510
Toronto, Ontario
M5G 0A3
Phone: 416-673-6646
Email: privacy@oicr.on.ca

Any complaints regarding OTB's compliance with PHIPA, 2004 and its regulation may be directed to the Information and Privacy Commissioner of Ontario:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
M4W 1A8
Web: www.ipc.on.ca
Phone: 416-326-3333 or 1-800-387-0073

Reporting breaches:
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. A privacy breach includes the following scenarios:

- 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.

5.0 Procedure

None.

6.0 Related Documents

- F-OTB.POL801-1, Privacy Breach Reporting – Ontario Tumour Bank
- F-OTB.POL801-2, Privacy Contacts – Ontario Tumour Bank
- Policy and Procedures for the Collection of Personal Health Information - Ontario Tumour Bank;
- Policy and Procedures for Data Access and Use - Ontario Tumour Bank;
- Policy and Procedures for Data Disclosure - Ontario Tumour Bank;
- Retention, Transfer and Disposal of Records Containing Personal Information and Personal Health Information;
- Clean Desk Policy;
- Sending/Receiving Personal Health Information, Personal Information and Confidential/Sensitive Information;
- Investigation and Reporting of Facilities Security Incidents for MaRS Location;
- Access Card and Key Management for MaRS Location;
- Facilities Security Policy for MaRS Location;
- Log of Access to OICR Premises;
- Privacy Inquiry Policy and Procedures;
- Privacy Complaint Policy and Procedures;
- 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 7.0 Password Governance;
- Policy Statement 15.0 Workstation Security;
- Policy Statement 22.0 Remote Access;
- Policy Statement 23.0 Electronic Media Destruction;
- Policy Statement 28.0 Mobile Devices Security;
- Policy Statement 29.0 Disaster Recovery and Offsite Data Storage;
- OTB SOP TB312 Material and Data Request and Release; and
- OICR's Privacy and Information Security Accountability Terms of Reference.

7.0 References

- Schedule 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA);

- Section 39 (1) (c) Registry status under the Personal Health Information Protection Act, 2004 (PHIPA);
- Long-Term Care Act, 1994; and
- www.ontariotumourbank.ca.

8.0 Revision History

Policy Number	Revision Date (YYYY-MM-DD)	Level of Change	Revision Comments
OTB.POL801.001	Not applicable	No change	New document
OTB.POL801.002	2012-05-11	Minor change	Removal of OCREB and MRI references
OTB.POL801.003	2013-01-22	Minor change	Included reference to MARC in Section 4.5
OTB.POL801.004	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 F-OTB.POL801-2, Privacy Contacts – Ontario Tumour Bank. Updated privacy officer phone number.
OTB.POL801.005	2015-12-03	Minor change	Updated address from 101 College to 661 University. Reformatted to add Forms properly as appendices not separate documents. Updated contact information in appendix B.

APPENDIX A: OTB PRIVACY BREACH REPORTING

All individuals employed or engaged by OTB are responsible for reporting privacy breaches, suspected privacy breaches and/or privacy risks they believe may lead to a privacy breach in the future. Such individuals should implement the following procedures noting that some steps may be executed concurrently (*e.g.*, notification and containment).

Situation #1: When the breach occurs at the Hospital

1. Take all steps necessary and reasonable in the circumstances to contain the breach, theft, loss, misuse or unauthorized access or disclosure (*e.g.*, if a fax has gone to the wrong number, contact the recipient and ask that it not be read but shredded and that the recipient confirm by email that it has been shredded).

2. Immediately notify the OTB Director and the Hospital's Privacy Officer (*i.e.*, the Privacy Officer at the hospital where the Data originated) (see F-OTB.POL806-2 for current list of contacts) by telephone followed by written notice (*e.g.*, by email).

3. Abide by all remedial actions and recommendations mandated by the Hospital's Privacy Officer and/or the OTB Director.

4. The Hospital's Privacy Officer and /or the OTB Director shall notify the OICR Privacy Officer (see F-OTB.POL806-2) by telephone at the first reasonable opportunity, followed by written notice.

5. In accordance with Hospital policies, depending on the nature of the breach, the Hospital shall contact the individual whose Data was stolen, lost, misused, disclosed, disposed of or accessed in an unauthorized manner.

6. OICR may investigate a Hospital in which a privacy breach occurs.

7. The Hospital shall have established in its policies and procedures, the penalties for employees who willfully commit a privacy breach and re-training for individuals who accidentally commit a privacy breach.

8. The Hospital Privacy Officer and the OICR Privacy Officer shall review any privacy breach and discuss measures to prevent further occurrences.

9. The Hospital Privacy Officer and the OICR Privacy Officer shall collaborate to maintain a log of all privacy breaches, including all processes related to the breach to be reviewed at least annually.

Situation #2: When the breach occurs at OICR

1. When an OICR employee becomes aware or has reason to believe that Data has been or may have been stolen, lost, misused, disposed of or disclosed contrary to OTB/OICR policies, or a person has obtained unauthorized access to the Data, or Data has been used, disclosed or disposed of other than permitted by its agreements with the participating hospitals, the employee shall follow the SOPs and policies and procedures of the OICR, including OICR's "Policy and Procedures for Privacy Breach Management", and shall:

    a. take all steps necessary and reasonable in the circumstances to contain the breach, theft, loss, misuse or unauthorized access or disclosure;

    b. at the first reasonable opportunity notify the OTB Director and OICR's Privacy Officer (see F-OTB.POL806-2) by telephone at the first reasonable opportunity, followed by written notice; and

    c. abide by all remedial actions and recommendations mandated by OICR's Privacy Officer.

2. Depending upon the nature of the breach, the OICR's Privacy Officer shall notify the Hospital's Privacy Officer (see F-OTB.POL806-2) by telephone at the first reasonable opportunity, followed by written notice.

3. Depending upon the nature of the breach, the Hospital Privacy Officer and the OICR Privacy Officer may work together to require additional containment and investigation.

4. In accordance with Hospital policies, depending on the nature of the breach, the Hospital shall contact the individual whose Data was stolen, lost, misused, disclosed, disposed of or accessed in an unauthorized manner.

5. Depending upon the nature of the breach, the Hospital Privacy Officer and the OICR Privacy Officer may review any privacy breach and discuss measures to prevent further reoccurrence.

6. Depending upon the nature of the breach, the Hospital Privacy Officer and the OICR Privacy Officer may collaborate to maintain a log of all privacy breaches, including all processes related to the breach to be reviewed at least annually.

APPENDIX B: OTB PRIVACY CONTACTS

Institution	Contact	Role	Telephone	Email
OICR	Olusola Dokun	OTB Manager	416-697-6656	Sola.Dokun@oicr.on.ca
OICR	Howard Simkevitz	OICR Privacy Officer	416-697-6646	Howard.Simkevitz@oicr.on.ca; privacy@oicr.on.ca
LHSC	Privacy Office	NA	519-685-8500 ext. 32996	privacy@lhsc.on.ca
KGH	Privacy Office	NA	613-549-6666 ext. 2567	privacy@kgh.kari.net
TOH	Privacy Office	NA	613-739-6668	privacy@toh.on.ca
SJH	Marnie Fletcher	SJH Privacy Officer	905-522-1155 ext. 35088	privacy@stjoes.ca