



August 2009

## GENERAL PRIVACY AND CONFIDENTIALITY POLICY

### 1.0 Introduction

The Ontario Institute for Cancer Research (OICR) is committed to respecting individual privacy, to safeguarding confidential information and to ensuring the security of personal health information (PHI) and personal information (PI) in its custody or under its control.

OICR's Statement of Commitment to Privacy and Confidentiality is publicly available on the OICR website at <http://www.oicr.on.ca/termsandconditions.htm>.

### 2.0 Scope

This policy covers the collection, use, disclosure, management, protection, retention and destruction of PHI and PI. This policy applies to all OICR employees. Although the majority of OICR employees do not access information or data that contains PHI or PI, all employees must be aware of the General OICR Privacy and Confidentiality Policies and Procedures.

OICR Programs which either access or which may have inadvertent access to PHI include the Ontario Tumour Bank (OTB), the Ontario Cancer Research Ethics Board (OCREB), Clinical Trials Program (CTP) and other specific research programs and platforms.

Best practices for privacy in Canada are set out in the privacy principles of Schedule 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA).

### 3.0 Definitions

**Agent:** A person who is authorized by OICR to act on its behalf and not for his/her own purposes, in managing OICR's PI/PHI.

**Collect:** To gather, receive or record personal information from any source and by any method.

**Collection Centre:** An organization that collects tumour, blood samples and PHI and is a public hospital and an HIC for purposes of PHIPA.

**Confidentiality:** The organization's obligation to protect from disclosure the PHI and PI with which it has been entrusted.

**Data linkage:** The process by which information from one data holding is combined with that of another data holding to create new or more complete information. Temporary linkages are created for the purpose of specific research projects. Permanent linkages effectively create new data holdings.

**Data holdings:** A list of all datasets that are maintained on OICR servers and are in the custodianship of OICR.

**Disclose:** To make personal information available or known to individuals outside OICR.

**Express consent:** Any specifically given (whether in writing, in person, electronically, by telephone, by using a check-off box or otherwise) voluntary, knowledgeable indication of an individual's wishes.



August 2009

**Health Information Custodian:** A health information custodian has the meaning set out in PHIPA (section 3). For the purpose of this policy, references to health information custodians (HICs) include public hospitals that act as Collection Centres and are primary data collectors responsible for complying with PHIPA, including ensuring that individuals are aware of the purposes for which their data is being collected, used and disclosed and their right to withdraw consent.

**Individual:** The person, whether living or deceased, whose information is collected, used or disclosed.

**Organization:** A legal person (e.g., a corporation), an association, a partnership, a Health Information Custodian or a trade union.

**Personal Information (PI):** Information about an identifiable individual including personal health information, but does not include the name, title, business address or telephone number of an employee of an organization.

**Personal Health Information (PHI):** As defined by PHIPA 2004 section 4.1, "personal health information", means identifying information about an individual in oral or recorded form, if the information:

- (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 provision 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, or eligibility for coverage 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.

**PHIPA:** The *Personal Health Information Protection Act, 2004* and regulations, as amended from time to time.

**Research:** A systematic investigation designed to develop or establish principles, facts or knowledge that can be generalized, or any combination of the above, and includes the development, testing and evaluation of research.

**Research Ethics Board (REB):** A board composed of qualified persons which can be formally designated by an organization, while maintaining its independent functioning from the organization, which meets for the purpose of conducting ethical reviews of research applications and meets the requirements of applicable provincial and federal legislation and regulations (e.g., PHIPA and the federal *Food and Drugs Act*) and applicable guidelines and policies (e.g., Tri-Council Policy Statement and ICH Good Clinical Practice Guidelines). The REB may approve, reject, propose modifications to, put on hold or terminate research at its sole discretion as well as recommend the suspension of ongoing research.

**Use:** To handle or deal with information, including transferring the information to an agent of OICR, but does not include disclosing the information to someone who is not an agent of OICR.



August 2009

## 4.0 Policy and Procedure

The following sets out how OICR adheres to these principles.

### 4.1 Principle 1 – Accountability

4.1.1 The President and Scientific Director of OICR is accountable for compliance with the applicable federal and Ontario privacy legislation and regulations. The President and Scientific Director has delegated this accountability to the Vice-President, Operations, who is responsible for ensuring that OICR meets current legal requirements and adheres to the principles of privacy, confidentiality and security.

The roles of individuals [Privacy Officer (PO), Information Security Officer (ISO), & Program Privacy Leads] who are responsible for the day-to-day management of PHI and PI are listed in the OICR Information Governance Terms of Reference.

4.1.2 OICR employees must comply with this policy for the collection, use, disclosure, management, protection, retention and destruction of PHI and PI. All employees must sign the Confidentiality Agreement as a condition of employment/engagement and employees must attend and participate in OICR's privacy and confidentiality training and are required to sign the Privacy Training Acknowledgement Form.

4.1.3 OICR is responsible for protecting the confidentiality of all PHI and/or PI that is transferred to third party service providers or agents acting on behalf of OICR. OICR ensures that adequate processes are in place to protect the confidentiality of any PI/PHI that is transferred to any third party before the information is transferred. Third parties requesting access to PI/PHI from OICR must adhere to this policy and all applicable laws relating to the protection of PI/PHI.

4.1.4 This policy is evaluated on an ongoing basis to ensure that it reflects current legislation and guidelines and that it reflects practices at OICR.

4.1.5 Breaches of the provisions of this policy may result in disciplinary action up to and including termination of the employee.

4.1.6 OICR has procedures in place to receive and to respond to inquiries and complaints.

### 4.2 Principle 2 – Identifying Purposes

4.2.1 Prior to the collection or receipt of any PI/PHI, OICR must identify the purpose for its collection, use or disclosure. Collection of PI//PHI is limited to the information necessary to meet the identified and, if required, ethically approved research purposes.

4.2.2 OICR employees must be aware of the purpose for which PI/PHI may be collected for the data holding(s) in their area.



August 2009

- 4.2.3 When PI/PHI that was previously collected is to be used or disclosed for a purpose not previously identified, the PI/PHI may only be used or disclosed after the new purpose has been identified and if required (for research data) REB approval has been given.

#### **4.3 Principle 3 – Knowledge and Consent**

- 4.3.1 The collection, use and disclosure of PI/PHI are based on knowledgeable consent with respect to research data and knowledgeable consent for other personally identifiable information or without consent in areas where permitted or required by law.
- 4.3.2 For data collection in the OTB program, collection centres [all of which are hospitals and therefore health information custodians (HIC)] act as primary data collectors of PI/PHI and are responsible for complying with all applicable legislation, and for ensuring that individuals are aware of the purposes for which PI/PHI is being collected, used and disclosed.
- 4.3.3 Where express consent **is required** for the collection, use, and disclosure of PI/PHI, OICR will ensure that consent has been obtained

#### **4.4 Principle 4 – Limiting Collection of Data**

- 4.4.1 OICR will only collect data for research and other purposes within its mandate and for its affiliated programs.
- 4.4.2 OICR will not collect PI/PHI indiscriminately. Both the amount and the type of information collected will be limited to what is necessary to fulfill the purposes identified.
- 4.4.3 PI/PHI will be collected directly from the individual unless otherwise permitted or required by law.
- 4.4.4 Any PI/PHI collected that does not fall within the scope identified, must be returned and/or the data will be destroyed.

#### **4.5 Principle 5 – Limiting Use, Disclosure and Retention**

- 4.5.1 Research data collected by OICR will be used for research purposes that contribute to an improved understanding of cancer and to improved treatment of individuals living with cancer. Restrictions on the use and disclosure of data will be reinforced by OICR's information technology architecture. All other data will be used, disclosed and retained for identified purposes.
- 4.5.2 Only authorized and designated OICR personnel, who have signed OICR's Confidentiality Agreement and received appropriate Privacy and Confidentiality Training, will be allowed access to PHI/PI. Access will be authorized on a need-to-know basis for performing OICR duties. No OICR employee may access PI/PHI unless required to do so for the purposes of his/her employment.



---

**August 2009**

- 4.5.3 OICR will take appropriate steps to protect against any risk of unauthorized disclosure of PI/PHI. OICR employees engaged in research must work with HICs, researchers and/or external parties to develop strategies for preparing data sets so that there is no potential risk of residual disclosure while meeting the analysis requirements for the approved research protocol. OICR will develop and maintain standards and guidelines for unauthorized disclosure avoidance and will make HICs, researchers and external parties aware of these standards and guidelines. If unauthorized disclosure issues cannot be resolved to OICR's satisfaction, OICR will not disclose biological samples, or related data.
- 4.5.4 OICR may participate in data linkage with external data sources for specific analyses or for other cancer research purposes, in accordance with applicable laws and/or regulations. All linked data sets will be subject to OICR's policy and procedures which govern the collection, use and disclosure of PI/PHI.
- 4.5.5 OICR has procedures and guidelines for the secure retention of PI/PHI and will not keep the data beyond the designated retention period set out in its data retention policy which is in compliance with applicable legislation.
- 4.5.6 PI/PHI that is no longer required to fulfill its identified purposes will be securely destroyed after the applicable retention period has expired.

**4.6 Principle 6 – Accuracy of PI /PHI**

- 4.6.1 OICR will require that the PI/PHI it receives is accurate, complete and up-to-date at the time of collection, as verified by the individual or organization collecting the data.
- 4.6.2 OICR will not update the PI/PHI it collects unless it is necessary to fulfill the purposes for which the PI/PHI was collected. Data which has been made anonymous will not be updated by OICR.

**4.7 Principle 7 – Safeguards (anonymization of data and process for the disposal or destruction of PI/PHI)**

- 4.7.1 OICR has security safeguards to protect against the loss, theft, unauthorized access, disclosure, copy, use, modification or disposal of PI/PHI.

Physical Safeguards

- 4.7.2 OICR provides a secure physical environment for the equipment and facilities where PI/PHI is stored and for the employees who use this information. (Refer to OICR Information Technology and Information Security Policies.)

Administrative Safeguards

- 4.7.3 All OICR employees must sign a Confidentiality Agreement. PI/PHI may only be accessed by designated employees on a need-to-know basis and



August 2009

is protected by data-sharing agreements as required. OICR makes all employees aware of the importance of maintaining the privacy and confidentiality of all PI/PHI.

- 4.7.4 OICR has policies and procedures in place pertaining to the disposal or destruction of PI/PHI to prevent unauthorised parties from gaining access to the information.
- 4.7.5 Privacy impact assessments (per OICR Privacy Impact Assessment Policy), including, as appropriate, security analyses and threat risk assessments, are completed on data holdings and organizational practices to ensure that privacy issues are identified and resolved or mitigating strategies, with follow-up plans are in place.

#### Technological Safeguards

- 4.7.6 OICR adopts industry standards and regularly tests its systems to ensure security of its data storage equipment and communication systems. (Refer to OICR Information Technology and Information Security Policies.)

#### **4.8 Principle 8 – Openness**

- 4.8.1 OICR makes information available about its policies and practices relating to the management of PI including PHI as well as the management of biological samples. The policies and practices governing these activities are readily available on the OICR intranet and selected policies on the internet including a Statement of Information Practices.

#### **4.9 Principle 9 – Individual Access to PI/PHI**

- 4.9.1 OICR is not a Health Information Custodian and does not hold health records for individuals for the purpose of providing health care. OICR does not update individual records to ensure that data are current or accurate with respect to the individual. Individuals requesting access to records about themselves that they believe to be held by OICR will be directed to contact the Health Information Custodians that collected or created the information about them. This includes those cases where the HICs collect information for the purpose of research on behalf of OICR or for projects sponsored by OICR.
- 4.9.2 Individuals have a right of access to the information as collected by OICR, but not a right of access to information from researchers.

#### **4.10 Principle 10 – Challenging Compliance**

- 4.10.1 Questions, concerns and complaints about OICR's Privacy and Confidentiality Policy are to be addressed to OICR's Privacy Officer (PO) as set out below. All concerns and questions will be dealt with in a timely fashion and if a complaint is found to be justified, OICR will take appropriate measures including, as necessary, changes to its policies and procedures.



**August 2009**

For more information about the privacy protection practices of the OICR, see the OICR's website at [www.oicr.on.ca](http://www.oicr.on.ca) or contact:

**Ontario Institute for Cancer Research**

Attn: Alison van Nie, Ethics and Privacy Officer  
MaRS Centre, South Tower  
101 College Street, Suite 800  
Toronto, Ontario  
Canada M5G 0A3  
416-673-8574

Questions, concerns and complaints may be addressed to the Information and Privacy Commissioner/Ontario.

Contact Information for the Information and Privacy Commissioner/Ontario:

**Information and Privacy Commissioner/Ontario**

2 Bloor Street East  
Suite 1400  
Toronto, Ontario  
M4W 1A8  
Web: [www.ipc.on.ca](http://www.ipc.on.ca)  
Telephone: 416-326-3333  
Long Distance: 1-800-387-0073 (within Ontario)

- 4.10.2 A privacy breach is the misuse, improper or unauthorized disclosure of PI/PHI/PI in the custody and control of OICR. Privacy breaches include uses or disclosures of PI/PHI/PI that contravene applicable legislation or OICR's Privacy and Confidentiality Policy and its Privacy Breach Policy and Procedure.
- 4.10.3 OICR extends whistleblower protection to any employee who reports a breach or a potential contravention of applicable legislation, or of OICR's Privacy and Confidentiality Policy (refer to Whistle Blower Policy). This protection also extends to those who refuse to perform a transaction that they believe to be in contravention of applicable legislation or OICR's Privacy and Confidentiality Policy.

**5.0 Related Documents**

- Statement of Information Practices at the Ontario Institute for Cancer Research
- OICR Breach of Privacy Policy and Procedure
- OICR Privacy Enquiry Policy and Procedure
- OICR Privacy Complaint Procedure



---

**August 2009**

## **6.0 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)

© Ontario Institute for Cancer Research (OICR). All Rights Reserved. This document is specific to OICR internal activities. OICR does not accept responsibility for use of this material by any person or organization not associated with OICR. No part of this document should be used for publication without permission and acknowledgement. A printed copy of this document may not reflect the current electronic version on the OICR Intranet.