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

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

OICR PRIVACY POLICY

Table of Contents

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. OICR is a federally incorporated not-for-profit corporation funded by the Government of Ontario through the Ministry of Research, Innovation and Science.

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 https://oicr.on.ca/website-privacy-statement/.

2.0 Scope

This policy covers the collection, use, disclosure, management, protection, retention and destruction of PHI and PI and is based on the ten 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).

3.0 Definitions

- See Glossary for OICR Privacy Policies and Procedures.

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 VP Corporate Services and Chief Financial Officer, who is responsible for ensuring that OICR meets current legal requirements and adheres to the principles of privacy, confidentiality and security.

The Privacy Officer and the Information Security Officer have been delegated day-to-day authority to manage the privacy and information security program. A matrix reporting structure is in place for both of these positions to report to the VP Corporate Services and Chief Financial Officer for this purpose. Other positions and committees that support the privacy and security programs include the Privacy Leads and Information Governance Committee. The duties and responsibilities of these positions along with the key activities of the privacy and security programs are described in the OICR Privacy and Information Security Accountability Terms of Reference.

4.1.2 Individuals employed or engaged by OICR must comply with this policy for the collection, use, disclosure, management, protection, retention and destruction of PHI and PI. All individuals employed or engaged by OICR must sign the Confidentiality Agreement as a condition of

employment/engagement (refer to policy on Confidentiality of Information) and employees must complete OICR's privacy training and are required to sign the Privacy Training Acknowledgement Form (refer to policy on Confidentiality of Information and Privacy and Information Security Training and Awareness Policy).

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, any executed third party service provider agreement and/or data sharing agreement, and all applicable laws relating to the protection of PI/PHI (refer to policies on Execution of Third Party Service Provider Agreements and Data Sharing Agreements).

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.

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 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 other diseases, and to improved treatment of individuals living with cancer. Restrictions on the use and disclosure of data will be reinforced by OICR's policies governing the same as well as OICR's physical information technology and security 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 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.

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 Health Information Custodians (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 that has been made anonymous will not be updated by OICR.

4.7 Principle 7 – Safeguards

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 description of OICR Information Security Program and related Policy Statements, as well as Facilities Security Policies and Access Card and Key Management 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 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. (For information regarding paper records refer to policies on Retention, Transfer and Disposal of Administrative Records; Retention, Transfer and Disposal of Records Containing Personal Health Information and Confidential/Sensitive Information. For information regarding e-records refer to Policy Statements 3.0 Encryption, 4.0 Secure Electronic Data Retention, Backup, Disposal and Destruction, and 5.0 Data Protection (Encryption, Transmission and Storage).)

4.7.5 Privacy impact assessments (per OICR's 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 description of OICR Information Security Program and Policy Statements.)

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 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.

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

Ontario Institute for Cancer Research
Attn: OICR Privacy Officer
MaRS Centre, South Tower
661 University Avenue, Suite 510
Toronto, Ontario
Canada M5G 0A3
416-977-7599
Questions, concerns and complaints may be addressed to the Information and Privacy Commissioner of Ontario.

Contact Information for the Information and Privacy Commissioner of Ontario:
Information and Privacy Commissioner of Ontario
2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Web: 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 Policy and its Policy and Procedures for Information Security and Privacy Breach Management.

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 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 Policy.

5.0 Related Documents

- Access Card and Key Management Policies and Procedures;
- Confidentiality of Information and OICR Confidentiality Agreement;
- Policy and Procedures for Information Security and Privacy Breach Management;
- Clean Desk Policy;
- Data Use and Disclosure Policy and Project Privacy Evaluation Form;
- Human Resources Privacy Policy;
- OICR Information Security Program Policies and Procedures;
- OICR Policy on Ethics and Integrity of Research;
- Privacy Inquiry Policy and Procedures;
- Privacy Complaint Policy and Procedures;
- Privacy Impact Assessment Policy;
- Retention, Transfer and Disposal of OICR Administrative Records;
- Retention, Transfer and Disposal of Records Containing Personal Health Information and Confidential/Sensitive Information;
- Sending/Receiving Personal Health Information, Personal Information and Confidential/Sensitive Information;
- Facilities Security Policies;
- Privacy and Information Security Training and Awareness Policy;
- Whistle Blower Policy.

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).

Title:	OICR Privacy Policy		
Associated Form(s):			
Document Number:	PR-INS.101.005		
Section:	Privacy & Information Security--Privacy	Pages:	8
Sponsor:	Privacy Officer	Review Cycle:	1 yr.
Content Reviewer(s):	Information Governance Committee	Date of Origin:	November 2, 2009
Issued By:	VP Corporate Services and CFO	Last Modified:	August 15, 2017
Approved By:	Executive Management Team	Review Dates:	January 5, 2010, September 10, 2010, May 15, 2013 July 5, 2016 August 16, 2017