



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

October 31, 2014

VIA ELECTRONIC AND REGULAR MAIL

Dr. Thomas Hudson, President and Scientific Director
Ontario Institute for Cancer Research
MaRS Centre, South Tower
101 College Street, Suite 800
Toronto, Ontario
M5G 0A3

Dear Dr. Hudson:

RE: Review of the Report on the Policies and Procedures of the Ontario Institute for Cancer Research in Respect of the Ontario Tumour Bank

Pursuant to subsection 13(2) of Regulation 329/04 of the *Personal Health Information Protection Act, 2004* ("the *Act*"), the Office of the Information and Privacy Commissioner of Ontario (IPC) is responsible for reviewing the practices and procedures implemented by an organization that has been designated as a prescribed person for the purposes of subsection 39(1)(c) of the *Act*, to protect the privacy of individuals whose personal health information it receives, and to protect the confidentiality of that information.

Given the practices and procedures of the Ontario Institute for Cancer Research (OICR), a prescribed person within the meaning of the *Act*, were last approved on October 31, 2011, the IPC was again required to review these practices and procedures and advise whether they continue to meet the requirements of the *Act* on or before October 31, 2014.

In accordance with the process set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the *Manual*"), OICR, as a prescribed person seeking the continued approval of its practices and procedures, submitted a detailed written report and sworn affidavit to the IPC. These documents were to conform to the requirements set out in the *Manual*.

The IPC has now completed its review of your report and affidavit. Based on this review, I am satisfied that OICR continues to have in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives, that sufficiently maintain the confidentiality of that information and that continue to meet the requirements of the *Act*.

Accordingly, effective October 31, 2014, I am pleased to advise that the practices and procedures of OICR in respect of the Ontario Tumour Bank continue to be approved for a further three-year period.

.../2



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

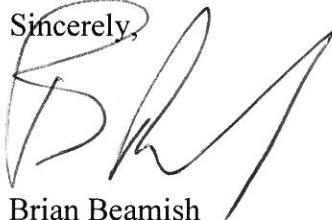
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

Attached is an Appendix containing recommendations to further enhance the practices and procedures of OICR, which must be implemented prior to the next legislated review.

I would like to extend my gratitude to you and your staff for your cooperation provided during the course of the review, including your diligence and timeliness in submitting the requested documentation, in responding to requests by my office for further information, and in making the amendments requested.

Sincerely,

A handwritten signature in black ink, appearing to read 'B Beamish', written over the word 'Sincerely,'.

Brian Beamish
Commissioner (Acting)

Attach.

cc:

Jane van Alphen, VP Operations
Monique Albert, Manager, Ontario Tumour Bank
Howard Simkevitz, General Counsel and Privacy Officer

Appendix

1. It is recommended that OICR ensure that a review of its policies and procedures are conducted, at a minimum, on an annual basis, as required by the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the Manual").
2. It is recommended that OICR ensure confidentiality agreements are executed by all agents on an annual basis, as required by the *Manual*.
3. It is recommended that OICR combine the *Policy and Procedures in Respect of a Privacy Audit* with the *Policy Statement 37.0, Logging and Security Audit* to create a stand-alone document entitled *Policy and Procedures in Respect of Security Audits*. This will better align with the policy structure and naming conventions in the *Manual* and thereby facilitate locating relevant content in any future review or IPC audit.
4. It is recommended that OICR combine the *Policy and Procedures for Privacy Breach Management* with the *Policy Statement 10.0, Information Security Incident Response* to create a stand-alone document entitled *Policy and Procedures for Information Security Breach Management*. This will better align with the policy structure and naming conventions in the *Manual* and thereby facilitate locating relevant content in any future review or IPC audit.

General Note to All Prescribed Persons and Prescribed Entities

The IPC wishes to clarify its expectations regarding the process for the three-year review and approval of prescribed entities and prescribed persons. For future reviews, the IPC will require that you provide your reports for the period spanning from one year prior to the previous approval up to and including October 31st of the year prior to the next expected approval date. Therefore, for the next expected approval date (October 31, 2017), the IPC requires that your reports, especially with regard to your indicators, cover the period from November 1, 2013 up to and including October 31, 2016.

If, at the time of delivering your report, some of the indicators for more recent months are not yet compiled, you will be expected to provide amendments to include the missing data within a reasonable time period after the initial submission of your report. For those prescribed entities and prescribed persons which have provided indicators beyond October 31, 2013 for the current approval, the IPC requires you to simply resubmit, on October 31, 2016, those portions of your indicators which went beyond October 31, 2013 along with new, previously unreported data, as required.