



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de de l'Ontario

VIA ELECTRONIC AND REGULAR MAIL

October 31, 2017

Dr. Michael Sherar
President and CEO
Cancer Care Ontario
620 University Avenue
Toronto, ON M5G 2L7

Dear Dr. Sherar:

RE: Review of the Report on the Practices and Procedures of Cancer Care Ontario

Pursuant to subsections 45(4) of the *Personal Health Information Protection Act* ("the *Act*") and 13(2) of Regulation 329/04 under 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 entity and prescribed person for the purposes of subsection 45(1) and 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 Cancer Care Ontario ("CCO"), a prescribed entity and a prescribed person within the meaning of the *Act*, were last approved on October 31, 2014, 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, 2017.

In accordance with the process set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the *Manual*"), CCO, as a prescribed entity and 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 CCO 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, 2017, I am pleased to advise that the practices and procedures of CCO 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/Télééc: (416) 325-9195
TTY: (416) 325-7539
Web: www.ipc.on.ca

Attached is an Appendix containing recommendations to further enhance the practices and procedures of CCO.

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,

Original signed by:

Brian Beamish
Commissioner

Encl.

cc: Lisa Norton Davies, Manager (Privacy & Compliance)

Appendix

1. It is recommended that CCO's policies and procedures distinguish between the use and disclosure of personal health information for research purposes, and specifically not consider all uses of personal health information for research purposes to be disclosures, within the meaning of those terms under the *Personal Health Information Protection Act* ("the *Act*"), as required by the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the *Manual*"). This recommendation should be addressed as soon as reasonably possible, providing written confirmation to the IPC of this no later than April 1st, 2018.
2. It is recommended that CCO require, at a minimum, the person or organization to which de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, as required by the *Manual*. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. This recommendation should be addressed as soon as reasonably possible, providing written confirmation to the IPC of this no later than April 1st, 2018.
3. It is recommended that CCO ensure that the documents and information it makes available to the public are current and up-to-date, including following amendments to CCO's policies and procedures.
4. It is recommended that CCO review its data holdings to ensure it has correctly identified the legal authority or authorities for the collection of personal health information, and specifically identify whether the personal health information in each data holding is collected pursuant to section 45 of the *Act* and/or pursuant to another authority. It is further recommended that, with respect to each data holding where CCO did not correctly identify the legal authority for the collection of personal health information, CCO review all uses and disclosures in relation to that data holding to ensure they are legally authorized. In particular, this recommendation should be addressed as soon as reasonably possible with respect to those data holdings related to CCO's Brachytherapy Funding, CBCRP, and OOC programs, providing written confirmation to the IPC of this no later than April 1st, 2018. With respect to all other data holdings, this recommendation should be addressed as soon as reasonably possible, providing written confirmation to the IPC of this no later than January 31st, 2020.
5. It is recommended that, at a minimum, all privacy and security policies, procedures, and practices put in place by CCO be reviewed by CCO at least once prior to each scheduled review of these policies, procedures, and practices by the IPC pursuant to section 45(4) of the *Act* and section 13(2)(b) of the Regulation under the *Act*.

6. It is recommended that CCO ensure that its reporting of indicators, especially as related to privacy complaints, are provided in full compliance with the *Manual* at the start of the next review period.
7. It is recommended that CCO ensure that linked records of personal health information are de-identified and/or aggregated as soon as practicable and that, to the extent possible, only de-identified and/or aggregate information is used by CCO's agents, as required by the *Manual*. In particular, CCO should consider the use of meaningless but unique numbers in the place of direct identifiers (e.g., name, address, health card number) when conducting analysis of linked datasets for section 45 purposes. It is further recommended that CCO conduct audits to ensure compliance with these requirements of the *Manual*, pursuant to its *Policy and Procedures in Respect of Privacy Audits*. This recommendation should be addressed as soon as reasonably possible, providing a written progress report to the IPC no later than April 1st, 2018. Further written confirmation of CCO's progress may be requested at the IPC's direction.