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

VIA ELECTRONIC MAIL

October 30, 2020

Mr. David O'Toole
President and CEO
Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, ON K2A 4H6

Dear Mr. O'Toole:

RE: Review of the Report on the Practices and Procedures of the Canadian Institute for Health Information

Pursuant to subsection 45(4) 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 and approving, every three years, the practices and procedures implemented by each prescribed entity. Such practices and procedures are required for the purposes of protecting the privacy of individuals whose personal health information such organizations receive, and maintaining the confidentiality of that information.

Given the practices and procedures of the Canadian Institute for Health Information (CIHI) were last approved on October 31, 2017, the IPC was required to review these practices and procedures again and advise whether they continue to meet the requirements of the *Act* on or before October 31, 2020.

In accordance with the process set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the *Manual*"), CIHI, as a prescribed entity 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 CIHI continues to have in place practices and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information in accordance with the requirements of the *Act*.

Accordingly, effective October 31, 2020, I hereby advise that the practices and procedures of CIHI continue to be approved for a further three-year period.

Attached is an Appendix containing recommendations to enhance the practices and procedures of CIHI. My staff will continue to actively monitor CIHI's progress towards implementing these recommendations. Please be advised that these recommendations

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

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

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

are to be addressed prior to the next cyclical review of the practices and procedures of CIHI, or sooner, if and as indicated in the attached Appendix.

I would like to extend my gratitude to you and your staff for your cooperation 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.

Yours sincerely,

Patricia Kosseim
Commissioner

Cc Ms. Rhonda Wing, Chief Privacy Officer and General Counsel
Mr. Cal Marcoux, Chief Information Security Officer

Appendix

1. It is recommended that CIHI develop and implement distinct policies and procedures in accordance with the policy structure and naming conventions set out in appendix A of the *Manual*. Doing so will better align CIHI's policies with the expectations set out in the *Manual* and thereby facilitate locating relevant content in any future review.

2. It is recommended that in developing distinct policies and procedures described above, CIHI ensure that each policy and procedure address compliance, audit, and enforcement as required under the *Manual*.

3. It is recommended that CIHI amend its Privacy Policy to include a list of data holdings of personal health information it maintains and identify where an individual may obtain further information in relation to the purposes, data elements and data sources for each data holding of personal health information; and that the *Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information* be amended to address each requirement set out in the *Manual*.

4. It is recommended that CIHI amend its Privacy Policy to clearly distinguish between the use of personal health information and the use of de-identified and/or aggregate information, and to clearly distinguish between the use of personal health information for the purposes of section 45 of the *Act* and the use of personal health information for research purposes.

5. It is recommended that CIHI's *Policy on the Transparency of Privacy Policies, Procedures and Practices* be amended to address each requirement set out in the *Manual*.

6. It is recommended that CIHI's *Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information* be amended to address each requirement set out in the *Manual* respecting the review and approval process and the conditions or restrictions on the approvals given.

7. It is recommended that CIHI's *Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research* be amended to address each requirement set out in the *Manual*.

8. It is recommended that CIHI's *Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements* be amended to address each requirement set out in the *Manual*.

9. It is recommended that CIHI maintain the required logs of privacy impact assessments and logs of data holdings and that each log comply with the requirements set out in the *Manual*.

10. It is recommended that CIHI complete its initiative to combine its various policies and procedures in respect of privacy audits into a single *Policy and Procedures in Respect of Privacy Audits* which addresses each requirement set out in the *Manual*.

11. It is recommended that CIHI amend its *Policy and Procedures for Privacy Breach Management* and *Policy and Procedures for Information Security Breach Management* to clearly define "privacy breach" and "information security breach" and address each requirement set out in the *Manual*.

12. It is recommended that CIHI's *Policy and Procedures for Secure Retention of Records of Personal Health Information* be amended to identify the agent(s) responsible for ensuring the secure retention of records of personal health information, require agents to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal and identify the reasonable steps that must be taken by agents as required in the *Manual*.

13. It is recommended that CIHI's *Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices* be amended to address each requirement set out in the *Manual*.

14. It is recommended that CIHI's *Policy and Procedures for Secure Transfer of Records of Personal Health Information* be amended to address the manner of obtaining and recording acknowledgement of receipt of the records of personal health information transferred as required in the *Manual*.

15. It is recommended that CIHI's *Policy and Procedures for Secure Disposal of Records of Personal Health Information* be amended to address each requirement set out in the *Manual*.

16. It is recommended that CIHI ensure that all information systems, technologies, applications and programs involving personal health information have the functionality to log access, use, modification and disclosure of personal health information as required by the *Manual* when adding or replacing information systems, technologies, applications and programs involving personal health information.

17. It is recommended that CIHI ensure, and that its *Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs* require that its system control and audit logs are immutable.

18. It is recommended that CIHI's *Policy and Procedures for the Execution of Confidentiality Agreements by Agents* be amended to outline the process that must

be followed where an executed confidentiality agreement is not received within a defined period of time as required by the *Manual*.

19. It is recommended that CIHI's *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship* be amended to provide a definition of "property" in compliance with the requirements of the *Manual*.

20. It is recommended that CIHI ensure that the Board of Directors is advised of the results of and any recommendations arising from investigations of any privacy breaches, information security breaches, and privacy complaints that are investigated, and the status of implementation of the recommendations.

21. It is recommended that CIHI ensure that its reporting of indicators related to statements of purpose for data holdings containing personal health information and privacy impact assessments is provided in full compliance with the *Manual* at the start of the next review period.

22. It is recommended that CIHI ensure that its privacy impact assessments are reviewed annually, as required by CIHI's *Privacy Impact Assessment Policy*.