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

October 31, 2023 ***VIA ELECTRONIC MAIL***

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

Dear David O'Toole:

RE: Review of the Practices and Procedures of the Canadian Institute for Health Information under the *Personal Health Information Protection Act, 2004*

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 an organization designated as a prescribed entity under subsection 45(1) of the *Act*. Such practices and procedures are required for the purposes of protecting the privacy of individuals whose personal health information prescribed entities receive, and maintaining the confidentiality of that information.

As you are aware, the practices and procedures of the Canadian Institute for Health Information (CIHI) were last approved on October 31, 2020. Thus, 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, 2023.

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, 2023, I hereby advise that the practices and procedures of CIHI continue to be approved for a further three-year period.

Appendix I to this letter contains my recommendations to further enhance the practices and procedures of CIHI. My staff will continue to monitor CIHI's implementation of these recommendations. Please be advised that these recommendations are to be addressed by August 1, 2025, or sooner, if and as indicated in Appendix I.

This three-year review cycle was marked by an unprecedented challenge for the health sector: the COVID-19 pandemic. The pandemic laid bare the importance of planning for business continuity and disaster recovery, and allocating resources to privacy and

security programs so that they can continue to operate effectively throughout such situations. At the same time, the pandemic has been a time of dramatic health sector transformation, providing an opportunity for prescribed persons, entities, and organizations to re-examine and improve their practices. Given the lessons learned from the pandemic, the Business Continuity and Disaster Recovery Plan of each prescribed person, entity, and organization may be one of our areas of focus in the next three-year review.

As you know, the IPC has revised the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, and will be reviewing prescribed persons and prescribed entities for compliance with this revised version (the *New Manual*) during the next three-year review. Additionally, based on lessons learned from the current review, I expect that the mandatory indicators CIHI submits on August 1, 2025 for the next three-year review will contain the required level of detail and accuracy to ensure a robust, meaningful and efficient review.

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. My office will continue to monitor your implementation of the recommendations made during this review period and we look forward to the next review cycle.

Through your ongoing collaboration with my office and your demonstrable commitment to continuous improvement, these three-year reviews help reassure Ontarians in the policies, procedures and practices you have in place to protect the privacy and confidentiality of the personal health information they have entrusted in you.

Yours sincerely,

Patricia Kosseim
Commissioner

cc: Dr. Nasir Kenea, Vice President and Chief Information Officer, Information Technology and Services
Mary Ledoux, Senior Privacy Consultant
Nilesh Shastri, Chief Information Security Officer
Rhonda Wing, Executive Director, Chief Privacy Officer and General Counsel

Appendix I: Recommendations

1. It is recommended that CIHI ensure that its PIAs and statements of purpose are reviewed annually, as required by CIHI's *Privacy Impact Assessment Policy* and that CIHI confirm the implementation of this recommendation to the IPC by January 31, 2024.

2. It is recommended that CIHI maintain the required log of data holdings and that the log comply with the requirements set out in the *New Manual*.

3. It is recommended that CIHI ensure that its privacy impact assessments (PIAs) describe any recommendations made to address the privacy risks that have been identified, even if CIHI then decides to redact such information from the publicly available version of the PIA.

4. It is recommended that CIHI amend its *Privacy and Security Incident Management Protocol* to address the agent(s) to whom the Incident Response Team (IRT) must provide its recorded results of its review of the containment measures.

5. It is recommended that CIHI amend its *Privacy and Security Incident Management Protocol* to set out the frequency of the audit of the Protocol and the agent(s) responsible for conducting the audit and for ensuring compliance with the Protocol.

6. It is recommended that CIHI amend its *Privacy and Security Incident Management Protocol* so that its definition of "privacy breach" or "privacy incident" complies with the requirements set out in the *New Manual*.

7. It is recommended that CIHI amend its *Privacy and Security Incident Management Protocol* so that its definition of "information security breach" or "information security incident" complies with the requirements set out in the *New Manual*.