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

Dr. Michael Schull, CEO
Institute for Clinical Evaluative Sciences
G1 06, 2075 Bayview Avenue
Toronto, ON
M4N 3M5

Dear Dr. Schull:

RE: Review of the Report on the Practices and Procedures of the Institute for Clinical Evaluative Sciences

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 Institute for Clinical Evaluative Sciences (ICES) 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*"), ICES, 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 ICES 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 ICES continue to be approved for a further three-year period.

Attached is an Appendix containing recommendations to enhance the practices and procedures of ICES. My staff will continue to actively monitor ICES' 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 ICES, 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. Rosario G. Cartagena, Chief Privacy and Legal Officer

Appendix

1. It is recommended that ICES improve its policies, practices and procedures in respect of privacy audits to be in full compliance with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (the "*Manual*"). In particular, it is recommended that ICES enhance its policies, practices and procedures regarding the auditing and removal of agent access to personal health information when such access is no longer required. This recommendation should be addressed as soon as reasonably possible, providing written confirmation to the IPC of this no later than October 31, 2021.

2. It is recommended that that ICES improve its information security policies, practices and procedures to be in full compliance with the *Manual*, including:
    a. Conducting systematic and meaningful reviews of ICES' system control and audit logs;
    b. Enhancing security audits, including penetration testing and vulnerability assessments;
    c. Improving ICES' network security and cybersecurity programs and its tracking and management of information security breaches;
    d. Conducting audits of agents granted access to the premises of ICES and to locations within the premises where records of personal health information are retained, at a minimum, on an annual basis;
    e. Amending ICES' policies, practices and procedures with respect to remote access to personal health information; and
    f. Amending and enhancing ICES' policies, practices and procedures with respect to passwords in relation to system-wide password-protected screen savers after a defined period of inactivity.

    Recommendations 2 "a" to "d" should be addressed as soon as reasonably possible, providing written confirmation to the IPC of this no later than June 30, 2021. Recommendations 2 "e" to "f" should be addressed as soon as reasonably possible providing written confirmation to the IPC of this no later than October 31, 2021.

3. It is recommended that ICES address the concerns expressed by the IPC in correspondence dated October 2, 2020 in determining whether to treat risk-reduced coded data (RRCD) or other similar information as de-identified. If these data are treated as de-identified, ICES must amend its policies, practices and procedures and reporting of indicators to the IPC to reflect this treatment. If ICES continues to treat RRCD as identifiable information, ICES must ensure that its policies, practices and procedures and reporting of indicators to the IPC are applied and implemented accordingly. This recommendation should be addressed as soon as reasonably possible, providing written confirmation to the IPC of this no later than October 31, 2022.

4. It is recommended that ICES ensure that it sets reasonable target dates for the completion of any outstanding recommendations arising from privacy impact assessments, privacy and security audits, privacy and security-related investigations and reviews by the Information and Privacy Commissioner of Ontario. It is further recommended that ICES ensure that it reports these target dates to the IPC as part of its indicators in full compliance with the *Manual* and provides an explanation where target dates are not met. This recommendation should be addressed as soon as reasonably possible, providing written confirmation to the IPC of this no later than October 31, 2021.

5. It is recommended that ICES develop and implement a Corporate Risk Management Framework in full compliance with the *Manual* that is operational across all departments and all ICES sites. This recommendation should be addressed as soon as reasonably possible, providing written confirmation to the IPC of this no later than October 31, 2022.