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***

Dr. Michael Schull
Chief Executive Officer
Institute for Clinical Evaluative Sciences
V1 06, 2075 Bayview Avenue
Toronto, ON M4N 3M5

Dear Michael Schull:

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

Pursuant to subsection 45(4) of the *Personal Health Information Protection Act, 2004* (PHIPA), 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 PHIPA. 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 Institute for Clinical Evaluative Sciences (ICES) 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 PHIPA on or before October 31, 2023.

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 PHIPA.

Accordingly, effective October 31, 2023, I hereby advise that the practices and procedures of ICES 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 ICES. My staff will continue to monitor ICES' 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.

Appendix II to this letter contains those Statements of Requested Exception submitted by ICES that I have approved, together with my reasons.

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.

Given that ICES now has multiple statuses under PHIPA, the *Coroners Act*, and the *Freedom of Information and Protection of Privacy Act* (a situation that did not apply during the 2020 review period), it is imperative that ICES's privacy and security programs be appropriately resourced to address fully the different requirements of each Act. In particular, ICES must have sufficient resources to address requirements around the completion of audits and around the timely preparation of accurate and thorough privacy impact assessments. Additionally, based on lessons learned from the current review, I expect that the mandatory indicators ICES submits on August 1, 2025 for the next three-year review cycles 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: Rosario Cartagena, Chief Privacy and Legal Officer
Ash-Lei Lewandoski, Legal Counsel

Appendix I: Recommendations

1. It is recommended that ICES complete the necessary revisions to its *Business Continuity and Disaster Recovery Policy* and associated procedures by December 31, 2023, and report back to the IPC when the revisions are complete. If they are not complete by that date, it is recommended that ICES submit status updates on or before December 31, 2023, and at the end of every three months following that until the revisions are complete.

2. It is recommended that, in consultation with the IPC, ICES amend the *Collection of ICES Data Policy* to provide greater clarity and rigor regarding the roles and responsibilities of the parties involved in the process of reviewing and determining whether to approve the collection of personal information, including by separating the role of the reviewer from the role of the decider who determines whether to approve the collection of personal information. I ask that you initiate this consultation with the IPC by December 31, 2023.

3. Recognizing that ICES has already amended its *Collection of ICES Data Policy* to clarify that it cannot approve any exception to the requirements established under the *Act* or the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the *Manual*"), it is recommended that ICES further amend the *Collection of ICES Data Policy* and/or *ICES Exceptions Policy* by August 31, 2024 to:

    a. identify the kinds of cases in which exceptions to the policy may be granted;
    b. specify criteria by which exceptions can be granted;
    c. set out the level of approval authority;
    d. require that all granted exceptions be documented with details about the case, the grounds on which the exception was granted, the approval authority, conditions (if any), the date of the approval, and the duration of the exception granted; and
    e. require that such documentation be retained consistent with ICES' authorized retention policy, with updates to that policy as needed.

Appendix II: Approved Statements of Requested Exceptions

Unless otherwise stated, all approved Statements of Requested Exceptions (SREs) are approved for a three-year period, ending on October 31, 2026. ICES must resubmit the below SREs at the beginning of the next three-year review period, starting August 1, 2025, if the requested exception is still required at that time.

ICES Statement of Requested Exception

"The policy and procedures must identify the conditions or restrictions that are required to be satisfied prior to the collection of personal health information, including any documentation and/or agreements that must be completed, provided or executed..."
(Policy and Procedure for Collection of Personal Information, pg 21)

Although ICES' policies and procedures require DSAs for all data holdings, ICES has identified an instance in which it does not appear to have DSAs for an older data holding.

IPC Response

The IPC **approves** the exception to the *Policy and Procedures for the Collection of Personal Health Information* for the lack of a data sharing agreement for the EFFECT database, on the grounds that initial collection for the EFFECT database began prior to ICES' status as a prescribed entity and ceased in 2008.

ICES Statement of Requested Exception

"It must also specify the precise nature of the personal health information subject to the Data Sharing Agreement…"
(Template Data Sharing Agreement, pg 47)

Although ICES' policies and procedures require that ICES specify the precise nature of the PHI, after a DSA is signed there are instances when the party disclosing PHI to ICES provides PHI variables that are not explicitly set out in the corresponding DSA. ICES collects and retains this additional PHI but does not make the additional PHI available in the project folder for use. Operationally, it is difficult to capture extraneous variables in all DSAs, particularly for data holdings with potentially thousands of variables.

IPC Response

The IPC **approves** the exception to the *Template Data Sharing Agreement* on the grounds that planned revisions to the *Manual* allow for personal health information subject to a data sharing agreement to be identified by categories of data elements or variables.

This exception is approved under the condition that ICES apply the data minimization principle thoroughly and carefully, and securely destroy unneeded personal health information as soon as practicable.

ICES Statement of Requested Exception

"A policy and procedures must be developed and implemented with respect to passwords for authentication and passwords for...applications and programs regardless of whether they are owned, leased or operated by the prescribed person or prescribed entity."
(Policy and Procedures Related to Passwords, pg. 91)

ICES hosts a single application that does not comply with the Logical Access Management Standard, which sets out ICES' password requirements, including requirements set out in the Manual.

IPC Response

The IPC **approves** this exception for the single instance it occurs on the grounds that ICES has identified compensating controls to limit risk consistent with the intent of the *Manual*.

ICES Statement of Requested Exception

"At a minimum, passwords must be comprised of a combination of upper and lower case letters as well as numbers and non-alphanumeric characters."
(Policy and Procedures Related to Passwords, pg. 91)

ICES hosts an application that does not comply with the Logical Access Management Standard, which sets out ICES' password requirements, including requirements set out in the Manual.

IPC Response

The IPC **approves** this exception on the grounds that ICES has identified compensating controls to limit risk consistent with the intent of the *Manual*.