



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**

Alex Munter  
President and Chief Executive Officer  
Children's Hospital of Eastern Ontario  
401 Smyth Road  
Ottawa, ON K1H 8L1

Dear Alex Munter:

**RE: Review of the Practices and Procedures of the Children's Hospital of Eastern Ontario — Ottawa Children's Treatment Centre in respect of the Better Outcomes Registry and Network under the *Personal Health Information Protection Act, 2004***

Pursuant to subsection 13(2) of Regulation 329/04 under 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 person under clause 39(1)(c) of the *Act*. Such practices and procedures are required for the purposes of protecting the privacy of individuals whose personal health information prescribed persons receive, and maintaining the confidentiality of that information.

As you are aware, the practices and procedures of the Children's Hospital of Eastern Ontario — Ottawa Children's Treatment Centre (CHEO), in respect of the Better Outcomes Registry and Network (BORN), 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 CHEO, in respect of BORN, 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 CHEO, in respect of BORN, 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 CHEO, in respect of BORN. My staff will monitor whether CHEO implements 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.



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  
TTY/ATS : (416) 325-7539  
Web : [www.ipc.on.ca](http://www.ipc.on.ca)

Appendix II to this letter contains those Statements of Requested Exception submitted by CHEO, in respect of BORN, 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.

As you know, the IPC has revised its *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (the *Manual*), and will be reviewing prescribed persons and prescribed entities for compliance with this revised version (the *New Manual*) during the next three-year 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,

A handwritten signature in black ink, appearing to read 'P. Kosseim', with a stylized flourish underneath.

Patricia Kosseim  
Commissioner

cc: Alicia St Hill, Executive Director, BORN  
Eric Smith, Privacy Officer and Counsel, BORN  
Ian Joiner, Manager of Information Protection, BORN

## Appendix I: Recommendations

1. It is recommended that BORN obtain the outstanding acknowledgements or agreements to ensure that the researchers to whom de-identified and/or aggregate information was disclosed, acknowledge and agree in writing that they will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. I ask that BORN confirm to the IPC that all outstanding acknowledgements or agreements have been executed and obtained by April 30, 2024.
2. It is recommended that BORN complete a fresh privacy impact assessment on the Infant Death Registration files it collects from the Ministry of Public and Business Service Delivery (formerly Ministry of Government and Consumer Services) and that BORN confirm to the IPC that any resulting recommendations have been implemented or will be implemented by April 30, 2024.
3. It is recommended that BORN complete a third-party audit that encompasses all services supplied by the third-party service provider respecting the SOC II third-party audit, as its privacy office requested be done in its January to June 2022 privacy review. It is further recommended that BORN confirm to the IPC that the audit has been completed and that any recommendations made have been implemented by December 31, 2024.
4. It is recommended that BORN update its policy *S-09 Password and Multi-Factor Authentication* by December 31, 2023 to assign an appropriate timeframe within which passwords will automatically expire. In determining the timeframe for the expiration of passwords, it is recommended that BORN ensure that its policy and procedures are consistent with any orders, guidelines, fact sheets and best practices issued by the IPC and with evolving privacy and security standards and best practices as set out in the *Policy, Procedures and Practices Relating to Authentication and Passwords* of the *New Manual*.
5. It is recommended that BORN update its policy *P-24: De-Identification and Aggregation* to address the requirements set out in the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation* section of the *New Manual*.

## 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. CHEO, with respect to BORN, must resubmit the below SREs at the beginning of the next three-year review period, starting August 1, 2025 if the requested exceptions are still required at that time.

### 1. Statement of Requested Exception on Obtaining Written Acknowledgements

The *Manual* requires written acknowledgements be obtained from the person or organization to which de-identified and/or aggregate information will be disclosed. The CHEO policies and procedures require this except in cases where aggregate data are made publicly available by CHEO to prevent disease or injury or to promote health. In such cases, CHEO ensures that the information is not published in a form that could reasonably enable a person to ascertain the identity of an individual. In other words, prior to making these CHEO data publicly available, CHEO has concluded that the risk of re-identification of an individual person is in effect, zero. Accordingly, CHEO requests an exception from the requirement for written acknowledgements in respect of information that is intentionally published by CHEO to prevent disease or injury or to promote health, provided that CHEO has concluded that such information could not reasonably enable a person to ascertain the identity of an individual.

#### IPC Response

This SRE pertains to the requirement that, at a minimum, a prescribed person or prescribed entity must require the person or organization to which the 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.

The IPC approves this SRE only where de-identified and/or aggregate information is made publicly available to prevent disease or injury or to promote health, and where CHEO with respect to BORN, has determined there is no risk of re-identification. The *New Manual* has been updated to reflect this public release scenario.

### 2. Statement of Requested Exception on Password Length

The *Manual* requires that policies and procedures must identify the required minimum and maximum length of passwords. CHEO's policies and procedures do not require a maximum length for passwords. This is because longer passwords provide a greater combination of characters and consequently make it more difficult for an attacker to guess. This is because CHEO believes that imposing a maximum

length can impact the strength of a password. Accordingly, CHEO requests an exception from the requirement to have a maximum length of a password.

**IPC Response**

The IPC approves this SRE. The SRE is deemed to be consistent with evolving privacy and security standards and best practices for passwords, and reflects the updated requirements of the *New Manual* that has removed the maximum length for passwords.