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***

Robert MacIsaac
President and Chief Executive Officer
Hamilton Health Sciences – King West
P.O. Box 2000
Hamilton, ON L8N 3Z5

Dear Robert MacIsaac:

RE: Review of the Practices and Procedures of the Hamilton Health Sciences Corporation in respect of the Critical Care Information System 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 Hamilton Health Sciences Corporation (HHS), in respect of the Critical Care Information System (CCIS), 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 HHS, in respect of CCIS, 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 HHS, in respect of CCIS, 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 HHS, in respect of CCIS. My staff will continue to monitor HHS' 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 HHS 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*, 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 HHS 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: Isabel Hayward, Executive Director, CritiCall Ontario
Stephanie Piper, Privacy Lead, CritiCall Ontario
Christina Popovich, Interim Director, HHS

Appendix I: Recommendations

1. It is recommended that HHS amend its CCIS Data Sharing Agreement (DSA) with participating hospitals so that the DSA accurately characterizes the access to personal health information in the CCIS by each participating hospital using terms as they are defined in the *Act* and its regulations. This recommendation should be addressed no later than December 31, 2024.

2. It is recommended that HHS amend its contract with the vendor that audits HHS' privacy and information security event logs so that the vendor discloses to HHS general descriptions of the findings, if any, arising from such audits.

3. It is recommended that HHS conduct privacy impact assessments (PIAs) in the circumstances in which the *New Manual* will require PIAs to be conducted.

4. It is recommended that HHS:
    - review its privacy policies and procedures as often as is required by its *Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices*, and at minimum once prior to each three-year review by the IPC; and
    - review its security policies and procedures as often as is required by its *Policy and Procedures for Ongoing Review of Security Policies, Procedures, and Practices*, and at minimum once prior to each three-year review by the IPC.

5. It is recommended that HHS perform privacy audits as often as is required by its *Policy and Procedures in Respect of Privacy Audits* and by the *New Manual*.

6. It is recommended that HHS perform the security audits set out in its *Policy and Procedures in Respect of Security Audits*, as often as is required by its *Policy and Procedures in Respect of Security Audits* and by the *New Manual*.

7. It is recommended that HHS test its *Business Continuity and Disaster Recovery Plan* as often as is required by that plan and by the *New Manual*.

Appendix II: Approved Statement of Requested Exception

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

HHS Statement of Requested Exception

HHS/CritiCall has conducted pen tests, however, to date, these have not included ethical hacks. Going forward, ethical hacks will be added as part of future testing and conducted at the same cadence as pen tests.

IPC Response

This SRE pertains to the requirement in the current *Manual*'s section on *Policy and Procedures In Respect of Security Audits*) that states:

> At a minimum, the audits required to be conducted shall include audits to assess compliance with the security policies, procedures and practices implemented by the prescribed person or prescribed entity; threat and risk assessments; security reviews or assessments; vulnerability assessments; **penetration testing; ethical hacks** and reviews of system control and audit logs. [emphasis added].

The current *Manual* lists "penetration testing" and "ethical hacks" as two distinct types of security audits. However, the *New Manual* will treat "penetration testing **or** ethical hacks" [emphasis added] as a single type. The IPC approves this SRE because, given this impending change in the *New Manual*, HHS will be able to conduct "penetration tests" or "ethical hacks" or both.