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***

Matthew Anderson
President and Chief Executive Officer
Ontario Health
525 University Avenue, 5th Floor
Toronto, ON M5G 2L3

Dear Matthew Anderson:

RE: Review of the Practices and Procedures of Ontario Health as a Prescribed Entity, as a Prescribed Person in Respect of Both its Registry of Cardiac and Vascular Services and the Ontario Cancer Screening Registry, and as a Prescribed Organization under the *Personal Health Information Protection Act, 2004*

Pursuant to subsection 45(4) of the *Personal Health Information Protection Act, 2004* ("the *Act*"), subsection 13(2) of Regulation 329/04 under the *Act,* and subsection 55.12(1) of 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 Ontario Health, which has been designated as a prescribed entity under subsection 45(1) of the *Act*, a prescribed person under clause 39(1)(c) of the *Act*, and a prescribed organization under Part V.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/persons/organizations receive, and maintaining the confidentiality of that information.

As you are aware, on October 31, 2020, I approved the practices and procedures of:

- Ontario Health as a prescribed person, in respect of the Ontario Cancer Screening Registry;
- Ontario Health as a prescribed entity; and
- CorHealth Ontario (formerly Cardiac Care Network of Ontario), as a prescribed person in respect of its registry of cardiac and vascular services.

Since the latter approval, and in response to the Minister of Health's transfer order under the *Connecting Care Act, 2019*, CorHealth Ontario was transferred to Ontario Health. In correspondence dated December 24, 2021, I confirmed that my approval of CorHealth Ontario's practices and procedures as a prescribed person under the *Act* would transfer to Ontario Health as part of the current three-year term and continue until its expiry on October 31, 2023.

Finally, I also approved the practices and procedures of Ontario Health as a prescribed organization on October 1, 2021. In order to synchronize the timing of the IPC's next review of Ontario Health as a prescribed organization with the next scheduled review of Ontario Health as a prescribed entity and a prescribed person, this last approval remained in effect only until October 31, 2023.

Based on the current review, I am satisfied that Ontario Health 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 Ontario Health 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 Ontario Health. My staff will continue to monitor Ontario Health'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.

Appendix II to this letter contains those Statements of Requested Exception submitted by Ontario Health 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. The IPC will also be reviewing its *Manual for the Review and Approval of Prescribed Organizations* in a manner consistent with the *New Manual*.

Additionally, based on lessons learned from the current reviews, I expect that the mandatory indicators Ontario Health submits on August 1, 2025 for the next three-year reviews will contain the required level of detail and accuracy to ensure a robust, meaningful and efficient review. Specifically, Ontario Health must ensure that its indicators related to security audits, including the recommendations arising from the audit

and the manner in which they were addressed, to be submitted at an adequate level of detail and accuracy.

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: Anne Corbett, General Counsel & Executive Lead, Legal, Privacy & Risk
Sylvie Gaskin, Chief Privacy Officer
Nadia Remtulla, Privacy Director
Melissa Yakeley, Privacy Lead

Appendix I: Recommendations

Recommendations in Respect of Ontario Health as a Prescribed Entity and Prescribed Person:

1. It is recommended that Ontario Health continue to engage with the IPC to clearly identify the statutory basis in the *Act* that permits it to provide access to and/or disclose personal health information through the legacy CorHealth systems. This recommendation should be addressed as soon as reasonably possible, with a response in writing outlining the statutory authority for these activities to be provided to the IPC not later than April 30, 2024.

2. It is recommended that Ontario Health continue its ongoing work to ensure that linked records of personal health information are de-identified and/or aggregated as soon as reasonable and practicable, including by expediting the migration of the data sets it has identified to its Enterprise Analytics Data Hub. This recommendation should be addressed as soon as possible and on an ongoing basis, with a written update to be provided to the IPC not later than October 31, 2024.

3. It is recommended that Ontario Health continue to engage with the IPC regarding the recommendations arising from the security audit indicators that were recently provided to the IPC on October 23, 2023 as part of the three-year review. This includes, but is not limited to, providing further information and documentation to the IPC and attending meetings as necessary.

Recommendations in Respect of Ontario Health as a Prescribed Organization:

4. It is recommended that Ontario Health complete its plan to expand the functionality within the ConnectingOntario clinical viewer to ensure that health information custodians accessing the electronic health record through this method are able to distinguish whether a consent override is being conducted for the purposes of subsection 55.7 (2) or (3) of the *Act.* This recommendation should be addressed as soon as reasonably possible, with a written update provided to the IPC not later than April 30, 2024.

5. It is recommended that Ontario Health continue to implement the permanent technological solution that will enable Ontario Health to meet its obligation under sub-paragraph 4.1 i. of section 55.3 of the *Act*, to keep an electronic record that identifies all persons who have viewed, handled or otherwise dealt with personal health information that is accessible through a Hospital Information System integration with the Ontario Laboratories Information System, without having to query or obtain such information from any third party. This recommendation should be addressed as soon as reasonably possible, with a written update provided to the IPC not later than October 31, 2024.

6. It is recommended that Ontario Health continue to implement its plan to ensure that it has adequate contact information for custodians who access personal health

information through the electronic health record, to ensure that notices of consent overrides are provided as required by subsection 55.7 (6) of the *Act*.

Recommendations in Respect of Ontario Health as a Prescribed Entity, Prescribed Person and Prescribed Organization:

7. It is recommended that Ontario Health continue to prioritize the activities currently underway to complete the development and implementation of a business continuity and disaster recovery plan that addresses and applies to all information technology systems containing personal health information. As this has been the subject of previous recommendations, Ontario Health must provide updates to the IPC on its progress every six months until completion, with the first such update being due April 30, 2024.

Appendix II: Approved Statements of Requested Exceptions (SREs)

Unless otherwise stated, all approved SREs are approved for a three-year period, ending on October 31, 2026. Ontario Health 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.

Approved Statements of Requested Exceptions in Respect of Ontario Health as a Prescribed Entity and Prescribed Person

1. Statement of Requested Exceptions: Disclosure of Aggregate Information

The following section of the Information and Privacy Commissioner's (**IPC's**) *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (**IPC PP/PE Manual**) requires that the Prescribed Entities and Prescribed Persons require persons or organizations, 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.

Part 1 – Privacy Documentation:

- 12. Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research

Exception Request and Rationale:
Ontario Health (**OH**) agrees that de-identified, and aggregate data sets may carry a risk of re-identification of individuals, depending on the degree to which de-identification techniques are implemented, and the level of risk of the data set. As such, OH includes a statement restricting persons or organizations from using de-identified or aggregate information, either alone or with other information, to identify an individual, to its 'Health System Planning Data Request Form', which requires a signature from the requester at the time the request for aggregate data is made.

However, where OH has made a determination that a particular data set has been aggregated to such a level that the aggregate information being requested cannot be reasonably re-identified, OH may not require individuals or organizations to acknowledge and agree, in writing, that the person or organization will not use aggregate information, either alone or with other information, to identify an individual. For example, when creating aggregate data sets that have no reasonable risk of re-identification, and that are intended to be published either by OH or an external individual or organization, OH may not require such an acknowledgement statement be made in writing prior to disclosing or making public the aggregate data set.

This approach has been reviewed with the IPC in previous reviews and has been acceptable.

IPC Response

Ontario Health is granted an exception to the requirement that, at a minimum, the 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 requested exception where aggregate information is intended to be made publicly available and there is no risk of re-identification. The granted exception acknowledges that Ontario Health has in place alternative practices and procedures that

have been reviewed by the IPC and found to be satisfactory in providing an equivalent standard to protect the privacy of the individuals whose personal health information it receives and maintain the confidentiality of the information. Moreover, the *New Manual* will address this public release scenario.

2. Statement of Requested Exceptions: Policy and Procedures for Maintaining a Consolidated Log of Recommendations

The following sections of the IPC PE/PP Manual require that the Prescribed Entities and Prescribed Persons to develop and maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches and reviews by the IPC.

Part 4 – Organizational and Other Documentation:

- 6. Policy and Procedures for Maintaining a Consolidated Log of Recommendations

Exception Request and Rationale:
OH does not maintain a single consolidated log for all privacy and security related recommendations. However, OH has developed and maintains policies and procedures that set out the requirement and process for the recommendations relating to privacy impact assessments, threat risk assessments, privacy and security audits, privacy and security incidents, privacy complaints, and IPC reviews, to be logged, tracked and monitored. All privacy and security risks and recommendations are reviewed regularly to identify and discuss a coordinated approach to addressing the risks and recommendations that may impact both privacy and security functions of OH.

This approach has been reviewed with the IPC in the previous review of the PO, and has been acceptable.

IPC Response

Ontario Health is granted an exception to the requirement that the prescribed person or prescribed entity develop and implement a policy and associated procedures requiring a consolidated and centralized log to be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits and the investigation of privacy breaches, privacy complaints and security breaches.

The granted exception acknowledges that Ontario Health has in place alternative practices and procedures that have been reviewed by the IPC and found to be satisfactory in providing an equivalent standard to protect the privacy of the individuals whose personal health information it receives and maintain the confidentiality of the information.

3. Statement of Requested Exceptions: Corporate Risk Management Framework and Register

The following section of the IPC PP/PE Manual requires Prescribed Entities and Prescribed Persons to develop and maintain a corporate risk register that identifies each risk identified that may negatively affect the ability of the Prescribed Person or Prescribed Entity to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information

Part 4 – Organizational and Other Documentation:

- Corporate Risk Register

Exception Request and Rationale:
The IPC PP/PE Manual contemplates a single enterprise risk management framework and risk register that includes all privacy and security risks. However, given the size and complexity of OH, OH currently uses an approach to managing risks across the agency that requires management of risks by each portfolio/region within the organization. Each portfolio/region is required to implement its own risk management process, including maintaining a risk register, and risks evaluated by standard criteria to determine whether they should be escalated to the Corporate Risk Register. The regional/portfolio risk registers inform the enterprise level risk management framework and risk register. All privacy and security risks are reviewed regularly by the Information Security Office (**ISO**) and the Privacy Office, including those identified in the regional/portfolio risk registers. While OH logs the instances of when the Corporate Risk Register is reviewed, it is further updating its process to log the instances when the Privacy Risks and Security Risks are reviewed by ISO and Privacy Office, to be reported in the next IPC review (commencing in 2025).

IPC Response

Ontario Health is granted an exception to the requirement that a prescribed person or prescribed entity must develop and implement a comprehensive and integrated corporate risk management framework to identify, assess, mitigate and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

Additionally, Ontario Health is granted an exception to the requirement that a prescribed person or prescribed entity must develop and maintain a corporate risk register that identifies each risk identified that may negatively affect the ability of the prescribed person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

The granted exception acknowledges that Ontario Health has in place alternative practices and procedures that have been reviewed by the IPC and found to be satisfactory in providing an equivalent standard to protect the privacy of the individuals whose personal health information it receives and maintain the confidentiality of the information.

4. Statement of Requested Exceptions: Password Complexity Requirements

Part 2 – Security Documentation:

- 9. Policy and Procedures Relating to Passwords

Exception Request and Rationale:

OH has adopted industry best practices in its policies for password management that offer equivalent or higher level of protection then requirements from the IPC PE/PP Manual. OH notes that the IPC is currently reviewing and revising the requirements for passwords in this Manual.

IPC Response

Ontario Health is granted an exception to the requirement that, at a minimum, passwords must be comprised of a combination of upper and lower case letters as well as numbers and non-alphanumeric characters.

The granted exception acknowledges that Ontario Health has in place alternative practices and procedures that have been reviewed by the IPC and found to be satisfactory in providing an equivalent standard to protect the privacy of the individuals whose personal health information it receives and maintain the confidentiality of the information. In addition, the *New Manual* has been amended to remove the maximum length for passwords consistent with evolving privacy and security standards.

Approved Statements of Requested Exceptions in Respect of Ontario Health as a Prescribed Organization

5. Statement of Requested Exceptions: End User Agreements

The following sections of the Information and Privacy Commissioner's (**IPC's**) *Manual for the Review and Approval of Prescribed Organizations* (**IPC PO Manual**) require that the Prescribed Organization develop, and implement a policy and procedures requiring each end user who provides personal health information (**PHI**) to, or collects PHI by means of, the electronic health record (**EHR**) to acknowledge and agree to comply with an end user agreement. The IPC PO Manual further sets out the matters that must be addressed in the End User Agreement, and requires the Prescribed Organization to log all End User Agreements, and sets out the minimum contents of this log.

Part 2 – Security Documentation

- Policy and Procedures for End User Agreements
- Template End User Agreements
- Log of End User Agreements

Exception Request and Rationale:
Given the high volume of end users Ontario Health (**OH**) does not execute agreements directly with each end user of the EHR. However, OH does execute relevant contributor and access agreements with all health information custodians (**HICs**) and coroners, under whose authority PHI is provided to the EHR, or under whose authority PHI is collected by means of the EHR. These agreements addresses the matters set out in the IPC's PO Manual with respect to End User Agreements. The EHR contributor and access agreements require HICs and coroners to require their agents to comply with these obligations. OH maintains a log of all EHR contributor and access services agreements executed with HICs and coroners.

Additionally, OH is working to amend its terms of its agreements with HICs and Coroners, to require HICs and coroners to ensure that their agents regularly acknowledge and agree to the terms set out in the EHR contributor and access agreement (at least annually), and to maintain a log that tracks the administration and acknowledgement of these agreements.

This approach has been reviewed with the IPC in the previous review of the PO and has been acceptable.

IPC Response

Ontario Health is granted an exception to the requirements that a policy and procedures must be developed and implemented requiring each end user (including an end user who is a health information custodian or an agent of a health information custodian), who provides personal health information to or collects personal health information by means of the electronic health record to acknowledge and agree to comply with the End User

Agreement and that a log must be maintained of all End User agreements acknowledged and agreed to by end users.

The granted exception acknowledges that Ontario Health has in place alternative practices and procedures that have been reviewed by the IPC and found to be satisfactory in providing an equivalent standard to protect the privacy of the individuals whose personal health information it receives and maintain the confidentiality of the information.

6. Statement of Requested Exceptions: Policy and Procedures for Maintaining a Consolidated Log of Recommendations

The following sections of the IPC PO Manual require that the Prescribed Organization to develop and maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches and reviews by the IPC.

Part 4 – Organizational and Other Documentation:

- Policy and Procedures for Maintaining a Consolidated Log of Recommendations

Exception Request and Rationale:
OH does not maintain a single consolidated log for all privacy and security related recommendations. However, OH has developed, and maintains policies and procedures that set out the requirement and process for the recommendations relating to privacy impact assessments, threat risk assessments, privacy and security audits, privacy and security incidents, privacy complaints, and IPC reviews, to be logged, tracked and monitored. All privacy and security risks and recommendations are reviewed regularly to identify, and discuss a coordinated approach to addressing the risks and recommendations that may impact both privacy and security functions of OH.

This approach has been reviewed with the IPC in the previous review of the PO and has been acceptable.

IPC Response

Ontario Health is granted an exception to the requirement that the prescribed organization develop and implement a policy and associated procedures requiring a consolidated and centralized log to be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits and the investigation of privacy breaches, privacy complaints and security breaches.

The granted exception acknowledges that Ontario Health has in place alternative practices and procedures that have been reviewed by the IPC and found to be satisfactory in providing an equivalent standard to protect the privacy of the individuals whose personal health information it receives and maintain the confidentiality of the information.

7. Statement of Requested Exceptions: Log of Notices of Consent Directives

The following section of the IPC PO Manual requires that the Prescribed Organization maintain a log of notices of consent directives that have been provided to a HIC pursuant to subsection 55.6 (7) of the *Personal Health Information Protection Act, 2004* (**PHIPA**). The IPC PO Manual also sets out the required content of the log.

Part 1 – Privacy Documentation:

- Log of Notices of Consent Directives

Exception Request and Rationale:
OH does not maintain a log of each instance an end user is notified of the existence of a consent directive. However, OH has in place adequate controls to ensure each consent directive is implemented and is functioning as intended. Every consent directive is tested after it is implemented and OH conducts functional testing and auditing of its consent management products. Controls are in place to ensure that the electronic alerts continue to function properly, and without disruption ("service health checks"). Service health checks are a method for ensuring the electronic alert function notifies the user each time they attempt to view an individual's information that is subject to a consent directive block. Service health checks mimic an end user's interaction with the EHR to ensure that the directive is displaying as it is expected to. Service health checks are supported by technical staff, and procedures to initiate corrective actions in the event of a failed service health check.

This approach has been reviewed with the IPC in the previous review of the PO and has been acceptable.

IPC Response

Ontario Health is granted an exception to the requirement that the prescribed organization maintain a log of notices of consent directives that have been provided to a health information custodian pursuant to subsection 55.6 (7) of the Act.

The granted exception acknowledges that Ontario Health has in place alternative practices and procedures that have been reviewed by the IPC and found to be satisfactory in providing an equivalent standard to protect the privacy of the individuals whose personal health information it receives and maintain the confidentiality of the information.

8. Statement of Requested Exceptions: Corporate Risk Management Framework and Register

The following section of the IPC PO Manual requires that the Prescribed Organization develop and maintain a corporate risk register that identifies each risk identified that may negatively affect the ability of the Prescribed Organization to protect the privacy of individuals whose PHI is received for the purpose of developing or maintain the EHR and to maintain the confidentiality of that information.

Part 4: Organizational and Other Documentation:

- Corporate Risk Register

Exception Request and Rationale:
The IPC PO Manual contemplates a single enterprise risk management framework, and risk register that includes all privacy and security risks. However, given the size and complexity of OH, OH currently uses an approach to managing risks across the agency that requires management of risks by each portfolio/region within the organization. Each portfolio/region is required to implement its own risk management process, including maintaining a risk register, and risks are evaluated by standard criteria to determine whether they should be escalated to the Corporate Risk Register. The regional/portfolio risk registers inform the enterprise level risk management framework and risk register. All privacy and security risks are reviewed regularly by the Information Security Office (ISO) and the Privacy Office, including those identified in the regional/portfolio risk registers. While OH logs the instances of when the Corporate Risk Register is reviewed, it is further

updating its process to log the instances when the Privacy Risks and Security Risks are reviewed by ISO and Privacy Office, to be reported in the next IPC review (commencing in 2025).

IPC Response

Ontario Health is granted an exception to the requirement that a prescribed organization develop and implement a comprehensive and integrated corporate risk management framework to identify, assess, mitigate and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received for the purpose of developing or maintaining the electronic health record and to maintain the confidentiality of that information.

Additionally, Ontario Health is granted an exception to the requirement that a prescribed organization develop and maintain a corporate risk register that identifies each risk identified that may negatively affect the ability of the prescribed organization to protect the privacy of individuals whose personal health information is received for the purpose of developing or maintain the electronic health record and to maintain the confidentiality of that information.

The granted exception acknowledges that Ontario Health has in place alternative practices and procedures that have been reviewed by the IPC and found to be satisfactory in providing an equivalent standard to protect the privacy of the individuals whose personal health information it receives and maintain the confidentiality of the information.