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***

Jill Ross
Chief Executive Officer
Pediatric Oncology Group of Ontario
480 University Avenue, Suite 1014
Toronto, ON M5G 1V2

Dear Jill Ross:

**RE: Review of the Practices and Procedures of the Pediatric Oncology Group of Ontario under the *Personal Health Information Protection Act, 2004***

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 an organization designated as a prescribed entity under subsection 45(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 receive, and maintaining the confidentiality of that information.

As you are aware, the practices and procedures of the Pediatric Oncology Group of Ontario (POGO) 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 POGO 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 POGO continue to be approved for a further three-year period.

Appendix I to this letter contains my recommendation to further enhance the practices and procedures of POGO. My staff will monitor whether POGO implements the recommendation, which is to be addressed by August 1, 2025.

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

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

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 recommendation 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: Bruna DiMonte, RN, Senior Database Administrator and Privacy Officer
Rabin Samaroo, Director, Information Technology, Data and Analytics
Mandy Sala, Program Coordinator, Technology, Data, Analytics and Privacy

## Appendix I: Recommendation

1. Where privacy impact assessments are conducted on requests for disclosure of personal health information for research purposes, it is recommended that POGO ensure that its policies, practices and procedures require the documentation of risks to the privacy of individuals, POGO's assessment of the risks, and POGO's recommendations to address and eliminate or reduce the privacy risks identified, in compliance with the *Policy, Procedures and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements* and the *Policy, Procedures and Practices for Privacy Impact Assessments* sections 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. POGO 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 Exceptions: Log of Data Sharing Agreements

Appendix A:

Part 1: Privacy Documentation, policy and procedure 18. Log of Data Sharing Agreements (page 50, the *Manual*):

- The date the personal health information was collected.

With respect to the POGONIS, Satellite and AfterCare databases, POGO requests that:

a. Logging of the date of initial data collection in each of these holdings in the Log of Data Sharing Agreements, and

b. The presence of the function which logs all data entry (collection) transactions within each of these applications, be deemed sufficient to meet the stated requirement.

Data collection resulting from data entry by hospital staff in specialized childhood cancer programs occurs on an ongoing basis into the POGONIS, Satellite and AfterCare database, as services are continuously provided to patients. Collection transactions are very high volume given the number of data managers and nurses who enter data on daily basis into these POGO data holdings. Due to the volume of transactions, transcribing these dates into the Log of Data Sharing Agreements is impractical.

POGO to continue with process of logging the date of the initial data collection into each of these holdings in the Log of Data Sharing Agreements. POGO to make available to the IPC, upon request, excerpts of the data collection logs from these applications.

**IPC Response**

POGO is granted an exception to the requirement that, at a minimum, the log [of DSAs] must include the date the personal health information was collected.

This granted exception is limited to collections of personal health information completed by way of POGO's POGONIS, Satellite and AfterCare databases. The IPC approves POGO's plan to ensure its Log of Data Sharing Agreements includes the initial date it collects personal health information into each of the three databases; and ensure it maintains the data collection logs for each database for its own use and in the event the excerpts of the logs are requested by the IPC. The IPC is satisfied that POGO is able to track the dates that personal health information was collected into each of the above listed databases pursuant to each Data Sharing Agreement in the above-noted manner.

## 2. Statement of Requested Exceptions: Penetration Testing

Appendix A:

Part 2: Security Documentation

15. Policy and Procedures In Respect of Security Audits (page 99, the *Manual*)

With respect to "At a minimum, the audits required to be conducted shall include audits to …penetration testing…", POGO requests an exception given our current system configurations provide an equivalent standard of protection to PHI data in our custody.

POGO has confidence that our current configuration of our system/network Firewalls to allow only approved IP addresses and, in addition, our use of reverse proxy, layered security and remote access gateway services to enable connection to our PHI applications adequately mitigate risks of unauthorized access and protects the privacy and confidentiality of the individuals whose PHI data we receive and maintain.

In addition, POGO engaged with a third party to conduct continuous external vulnerability assessment.

POGO has completed a Statement of Work and has engaged a vendor to conduct Network Penetration testing of our External and Internal networks. This work will commence in Fall 2023 once POGO staff return to the POGO office (currently closed due to construction).

**IPC Response**

POGO is granted an exception to the requirement to complete penetration testing.

The IPC approves the SRE, on condition that POGO conduct a third-party penetration test by March 1, 2024 and that POGO report to the IPC on its completion of this penetration test by April 30, 2024, including the recommendations arising from the penetration test; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed. Subject to these conditions, the IPC is satisfied that POGO's plan will adequately address the risks associated with the penetration tests that have not previously been conducted.

## 3. Statement of Requested Exceptions: Consolidated Log of Recommendations

Appendix A:

Part 4: Organizational and Other Documentation

7. Consolidated Log of Recommendations (page 122, the *Manual*)

POGO requests that recommendations arising from privacy impact assessments, IPC audits, privacy audits, security audits, the investigation of privacy complaints and privacy and security breaches be retained in separate logs and that including links to these logs within an consolidated log document be accepted as meeting the stated requirement.

Creating a consolidated log that duplicates entries in other logs is impractical due to the significant effort required and creates the potential risk of inconsistencies across duplicate logs.

In the Feedback letter on the *New Manual* submitted to the IPC dated June 15, 2022, POGO and other Prescribed Entities and Persons proposed separate logs be allowed. POGO appreciates the IPC's review and consideration of this proposal.

**IPC Response**

POGO 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 IPC approves POGO's proposed plan to ensure it maintains a consolidated log document, in the place of the Consolidated Log of Recommendations, that links to the separate logs summarizing the recommendations arising from privacy impact assessments; privacy audits; security audits; the investigation of privacy breaches, privacy complaints and security breaches; and reviews by the IPC. The IPC is satisfied that POGO's proposed plan will promote a consolidated and consistent approach to recommendations arising out of different processes.