POGO
PEDIATRIC ONCOLOGY GROUP OF ONTARIO
FOR KIDS WITH CANCER
FOR NOW, FOR LIFE.

POGO Privacy and Security
Governance and Accountability Framework

Production of this report is made possible by the Pediatric Oncology Group of Ontario (POGO).
The contents of this publication may be reproduced in whole or in part, provided the intended use is for non-commercial purposes and full acknowledgement is given to POGO.

Pediatric Oncology Group of Ontario
480 University Avenue, Suite 1014
Toronto, ON M5G 1V2
Telephone: 416-592-1232
www.pogo.ca
info@pogo.ca

Document Review

Version	Date	Author(s)	Description of Changes
2023	Sept. 29, 2023	B. DiMonte, J. Ross, R. Samaroo	• Annual review • Included new role Director, Information Technology, Data and Analytics

Document Approval

Date	Approver
Oct. 3, 2023	POGO Privacy Officer

Table of Contents

POGO
PEDIATRIC ONCOLOGY GROUP OF ONTARIO
FOR KIDS WITH CANCER
FOR NOW, FOR LIFE.

Introduction to Privacy and Security at POGO

The *POGO Privacy and Security Governance and Accountability Framework* provides a comprehensive approach to privacy and security management at Pediatric Oncology Group of Ontario (POGO). The *Framework* is designed to enable the effective integration and coordination of POGO's privacy and security policies and to provide POGO's decision-makers, Privacy Officer, and the governance structure with a comprehensive view of the organization's information privacy and security management practices. It is a living document, updated as POGO's Privacy and Security Program evolves over time. The *Framework* can also be used for the purposes of communicating POGO's commitment to privacy and security to regulators, stakeholders and the public.

The *Framework* has been informed by best practices for privacy and information management across the public, private and health sectors. As set out in the table that follows, the *Framework* is modular, thus offering POGO the flexibility to share accountability across programs which can identify areas for improvement and to develop action plans specific to privacy and security. In the following table is a brief summary of how POGO has addressed each component.

Table 1: Components of POGO Privacy and Security Governance and Accountability Framework

DRIVERS	**Legal/Statutory**	Ontario *Personal Health Information Protection Act*, 2004 (*PHIPA*) and its Regulations and any other applicable provincial privacy legislation.
	Trust and Confidence	Maintaining the trust and confidence of the Ministry of Health (MOH), the Information and Privacy Commissioner (IPC), stakeholders, healthcare providers, institutions, health professional colleges and associations, childhood cancer patients, survivors, and their families and the public.
	Vision/Mandate	• *Childhood Cancer Care Plan: A Roadmap for Ontario* • *POGO Organizational Strategy* • POGO promotional materials • *POGO Privacy and Data Security Code* • Charitable status
GOVERNANCE	**Organizational Structure**	• POGO letters patent and bylaws • Charitable status • Chief Executive Officer (CEO) or delegate(s) • POGO Board Chair and Directors • Director, Information Technology, Data, and Analytics • Privacy Officer • POGO Privacy and Data Security Committee
	Accountabilities	Individual accountabilities for privacy and security and Terms of Reference for POGO Privacy and Data Security Committee.
	Privacy and Data Security Blueprint	Four documents identify existing privacy and data security policies, standards and procedures:

		• Privacy and Security Policies and Procedures Manual • *POGO Privacy and Data Security Code* • *POGO Privacy and Data Security Procedures* • Policy 9.2.3 *Security Standards and Procedures*
RISK MANAGEMENT	**Risk Identification Tools**	Privacy impact assessments (PIAs), threat and risk assessments (TRAs) and vulnerability assessments
	Risk Mitigation and Acceptance Protocol	Policy 9.1.14 *Privacy Impact Assessment* requires that PIAs are updated annually and includes recommendations for risk mitigation. It assigns ultimate responsibility to the CEO or delegate(s) and through reporting by the Privacy Officer and program managers. POGO has a policy on the acceptable use of POGO's information systems (Policy 9.2.15 *Acceptable Use*). TRAs, vulnerability assessments and penetration testing activities are conducted and include recommendations for risk mitigation. Ultimate responsibility is assigned to the Director, Information Technology, Data, and Analytics, the IT team and the Privacy Officer.
	Benchmarking	The IPC reviews all POGO privacy and security policies and procedures on a triennial basis, pursuant to Section 45 of *PHIPA*. Benchmarking is conducted by the Director, Information Technology, Data, and Analytics and the Privacy Officer.
	Compliance Monitoring	Program-wide risk identification tools to monitor risk and implement recommendations and a master log/inventory to track and log mitigating strategies and recommendations.
	Business Continuity and Disaster Recovery	POGO maintains a Business Continuity and Disaster Recovery (BCDR) Plan.
PROGRAM CONTROLS	**Policies**	As documented in the POGO privacy and security policies and procedures and the *POGO Privacy and Data Security Code*.
	Procedures and Protocols	As documented in the POGO privacy and security policies and procedures.
	Training and Awareness	Policy 9.3.1 *Privacy and Security Training* requires the administration of mandatory and traceable privacy and security orientation, and ongoing training at least annually, for current agents (individuals employed and/or with POGO as a volunteer, Board member, student, etc.). Website privacy- and security-related content updates are ongoing. Regular staff education sessions based on new and emerging trends in privacy and information security.

	Secure Information Lifecycle	POGO has a suite of standards and guidelines that provide guidance for the protection of the confidentiality, integrity and availability of data throughout its lifecycle: Collection, registration, access, retention and storage, use, disclosure and destruction.
	Breach and Incident Management Protocols	• Policy 9.1.16 *Privacy Breach and Incident Management* • Policy 9.2.17 *Information Security Breach Management Process* • Breach team
	Agreements	• POGO Confidentiality and Non-Disclosure Agreement with agents • Third-Party Service Provider agreement • Data Sharing Agreements (DSAs) with POGO hospital partners and other providers of administrative data • POGO Data Request Form • Research Agreement, including the POGO Project-Specific PIA
	Service Provider Management	Third-Party Service Provider agreements for software development and system and server programming.
	External Communication	• Privacy information and frequently asked questions (FAQs) on website • *POGO Privacy and Security Governance and Accountability Framework* and *POGO Privacy and Data Security Code* • Statements of purpose for each data holding
AUDITS, COMPLIANCE AND REPORTING	**Audit Program**	*POGO Privacy and Security Audit Program*
	External Review of POGO	Ontario IPC program review and compliance audit every three years.
	External Privacy Expert/Advisor	External privacy advisor to resolve privacy issues/concerns if required.
	Compliance Monitoring/Reporting	Annual POGO Information Privacy and Security Report to the POGO Board of Directors, and reporting on an ad hoc basis, and pursuant to the POGO Privacy and Security Audit Program and PIAs.

1. Drivers

a) Legal and Statutory Drivers

POGO is a legally constituted, not-for-profit organization with charitable status. It is also a Prescribed Entity under Section 45 of Ontario's *Personal Health Information Protection Act*, 2004 (*PHIPA*) and is authorized to collect, use and disclose personal health information for prescribed purposes. As a Prescribed Entity, POGO is subject to oversight by the Ontario Information and Privacy Commissioner (IPC) and must have its practices and procedures with respect to privacy and the protection of health information reviewed and approved every three years. The last such review was completed in October 2020. The renewal of POGO's Prescribed Entity status is viewed by stakeholders across Ontario and beyond as evidence of the soundness of the *POGO Privacy and Security Governance and Accountability Framework*.

PHIPA and all privacy codes generally are based on the ten fair information principles set out in the Canadian Standards Association's Model Privacy Code:

- Principle 1: Accountability
- Principle 2: Identifying purposes
- Principle 3: Consent
- Principle 4: Limiting collection
- Principle 5: Limiting use, disclosure and retention
- Principle 6: Accuracy
- Principle 7: Safeguards
- Principle 8: Openness
- Principle 9: Individual access
- Principle 10: Challenging compliance

These principles are the basis for POGO's self-regulatory privacy and security efforts. POGO also adheres to other provincial legislation as applicable to POGO's mandate and core functions and to POGO bylaws regarding governance.

b) Trust and Confidence

Maintaining the trust and confidence of the MOH, the IPC, stakeholders, healthcare providers, institutions, health professional colleges and associations, childhood cancer patients, survivors, and their families and ultimately the public is critical to the success of POGO and the achievement of its goals. All of its activities must be conducted, and all partnerships established and maintained, in a manner that reflects these expectations.

c) Mission, Vision and Mandate

Mission

We partner to achieve the best childhood cancer care system for children, youth, survivors, and their families in Ontario and beyond.

Vision: What POGO Aspires To Be and To Achieve

A valued partner. An excellent childhood cancer care system.

Mandate

POGO works to ensure that everyone affected by childhood cancer has access to the best care and support. We partner to achieve an excellent childhood cancer care system for children, youth, survivors, their families, and healthcare teams in Ontario and beyond. POGO champions childhood cancer care and, as the collective voice of this community, is the official advisor to Ontario's Ministry of Health on children's cancer control and treatment. POGO is a non-profit organization with charitable status, here for kids with cancer, for now, for life.

2. Governance

a) Organizational Structure

POGO's privacy and security information governance structure provides assurance that the strategies, policies, standards, processes and resources to manage privacy and security risks are aligned with POGO's objectives and are consistent with applicable laws, standards, and best practices.

POGO's CEO is ultimately accountable for POGO's compliance with these principles by ensuring that all of POGO's activities, as defined within its role as a Prescribed Entity pursuant to Section 45(1) of *PHIPA*, are compliant and by ensuring adherence to the principles of privacy, confidentiality and security.

The CEO is accountable to POGO's Board of Directors, the Ontario MOH, and the IPC of Ontario regarding these matters.

The CEO delegates authority to other individuals within POGO who are responsible for developing and managing POGO's Privacy Program, and updating the POGO Board of Directors on the privacy program and privacy matters on an annual basis.

The CEO has designated staff to perform the following functions:

- The Director, Information Technology, Data and Analytics oversees POGO's information systems security and cybersecurity in alignment with these principles and *PHIPA* and its Regulations. The Director, Information Technology, Data and Analytics reports to the CEO.
- The Privacy Officer oversees POGO's compliance with these principles and oversees POGO's compliance with *PHIPA* and its Regulations jointly with the Director, Information Technology, Data and Analytics. The Privacy Officer reports to the Director, Information Technology, Data and Analytics.

The POGO Privacy and Data Security Committee presides over the organization's privacy and information security structure. In addition to the CEO or delegates, the governance structure also includes the Director, Information Technology, Data and Analytics; Medical Director; Senior Database Administrator and Privacy Officer; and the Program Coordinator, Information Technology, Data, Analytics and Privacy.

The CEO and the Director, Information Technology, Data and Analytics hold senior positions within the organization and, importantly, provide representation for their respective functions on the most senior decision-making bodies within POGO. Specific to privacy and security, these include the POGO Board of Directors and the POGO Privacy and Data Security Committee.

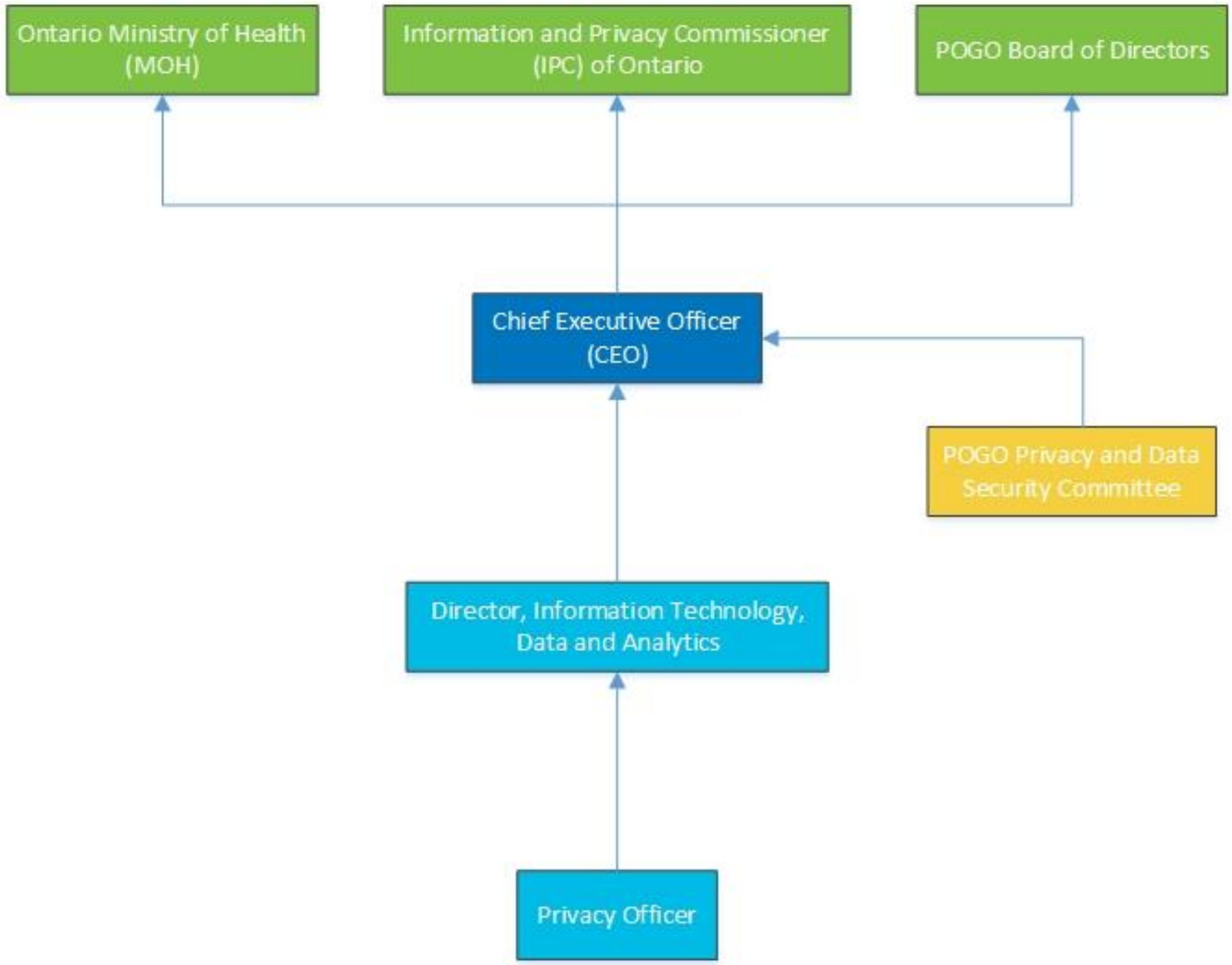
The responsibilities of the Privacy Officer; Director, Information Technology, Data and Analytics; and CEO or delegates are all closely linked. Open and constant communication among these individuals is recognized as vital to a successful information governance model. The Privacy Officer and the Director, Information Technology, Data and Analytics work closely together to coordinate their efforts in areas such as training and awareness, and engaging in mutual consultation regarding policy development.

To further ensure that POGO's Privacy Program is representative of best practices, POGO consults with:

- Legal counsel specializing in privacy and security when applicable

- Other Prescribed Entities

Figure 1: POGO Privacy and Security Governance and Accountability Framework Governance Chart


Ontario Ministry of Health (MOH)
Information and Privacy Commissioner (IPC) of Ontario
POGO Board of Directors
Chief Executive Officer (CEO)
POGO Privacy and Data Security Committee
Director, Information Technology, Data and Analytics
Privacy Officer

b) Accountability, Shared Responsibilities and Transparency

All POGO agents (staff, volunteers, Board members, students, etc.) play a significant role in the privacy and security of the data holdings at POGO. The accountabilities set out herein specifically relate to those committees and individuals who play leadership roles and hold specific accountability for privacy and security.

POGO recognizes the importance of privacy and security obligations and, therefore, established the POGO Privacy and Data Security Committee, which is responsible to the CEO or delegates who reports, in turn, to the Board. This committee represents accountability at the highest possible level, overseeing the Privacy and Security Program and reviewing privacy breaches, audit reports, proposed policy changes and any other issues deemed relevant by the CEO; the Director, Information Technology, Data and Analytics; and/or the Privacy Officer.

Accountability for privacy and security ultimately resides with the CEO of POGO, who formally delegated these functions at an operational level to the Director, Information Technology, Data and Analytics and the Privacy Officer.

The Privacy Officer is responsible for managing the Privacy Program, providing privacy advice and support to program areas, ensuring that the suite of privacy policies and procedures is comprehensive and up-to-date, providing privacy training and conducting PIAs, audits/compliance monitoring and benchmarking. The Privacy Officer is also responsible for ensuring that appropriate Data Sharing and other agreements are in place, and for monitoring legal and other developments in the privacy arena.

The Director, Information Technology, Data and Analytics has overall day-to-day accountability for the confidentiality, integrity and availability of the data holdings within POGO's custody and control and for ensuring that the Security Program and suite of policies dedicated to these ends are robust and up-to-date. The Director, Information Technology, Data and Analytics is also responsible for conducting TRAs, audits and benchmarking as appropriate, and for monitoring industry best practices in information security and implementing corrective actions.

Finally, transparency is a fundamental principle in the world of privacy: Policies and procedures need to be accessible. POGO is committed to transparency and accessibility of information to its stakeholders and to the public and uses various policy instruments to demonstrate its commitment. For example, POGO makes this *Framework* – the *POGO Privacy and Security Governance and Accountability Framework* – and the *POGO Privacy and Data Security Code* available on its website. In addition, other documentation is also made available by the same means. This includes FAQs, a description of data security safeguards, an inquiry and/or complaint mechanism and *Access To and Use of POGO Data* guidelines.

c) Privacy and Data Security Blueprint

POGO's Privacy and Data Security Blueprint is comprised of four key documents that outline POGO's policies, standards and procedures for its Privacy and Security Programs. These documents are informed by best practices and together provide the desired optimal platform for relevant policy development and decision-making. These documents include the following:

- POGO's Privacy and Security Policies and Procedures Manual
- *POGO Privacy and Data Security Code*: Highlights POGO's practices with respect to personal health information (PHI) and is based on the ten principles of the Canadian Standards Association's fair information practices
- *POGO Privacy and Data Security Procedures*: Outlines the processes that relate to the ten principles
- Policy 9.2.3 *Security Standards and Procedures* defines POGO's security guidelines and procedures followed by the IT team

3. Risk Management

In 2004, when POGO's Privacy Program was initiated to protect PHI holdings, POGO developed a comprehensive and integrated corporate risk management framework that enables the Director, Finance and Administration, the Director, Information Technology, Data and Analytics and the Privacy Officer to identify, evaluate, assess and manage corporate, privacy and security risks.

a) Risk Identification Tools

POGO recognizes that one of the most effective ways to ensure privacy and information security is to identify, mitigate and manage risks. Consistent with the "Privacy by Design" concept developed by Dr. Ann Cavoukian, Ontario's former Information and Privacy Commissioner, POGO has adopted a proactive and preventative approach to privacy and security. This entails embedding privacy in the design, implementation and management of POGO programs, practices and processes and in the modus operandi of its IT system. It also involves processes designed for the early identification of any privacy or information security risks.

POGO employs a number of different privacy and security risk identification tools, including PIAs, TRAs, vulnerability assessments and penetration testing ("ethical hacks"). PIAs and TRAs ensure that privacy and security principles are taken into account during the design, implementation and evolution of a program, initiative, process or system.

More specifically from a privacy perspective, PIAs are integral to the fulfillment of POGO's key commitment to privacy and security management. POGO has effectively integrated the PIAs into all programs that involve collection, use or disclosure of data and research reviews. Importantly, POGO makes PIAs a shared responsibility among the program staff or Research Coordinators/Investigators and the Privacy Officer. PIAs are conducted in the design phase of a new program or when there is a significant change in an existing program, where such activity involves the collection, use or disclosure of data. Further, all POGO employees are required to review existing PIAs annually to identify any discrepancies between their content and actual practices. This requirement serves a two-fold purpose: 1) It assists the program in identifying risk during the design phase and 2) it alerts the program that incremental changes have occurred that could result in a potential privacy issue.

In addition, on a regular basis, POGO's IT team conducts TRAs designed to identify, assess and manage information security risks and, through commissioning of vulnerability assessments and penetration testing, to test and identify risks to POGO's information and information systems.

b) Risk Mitigation and Acceptance Protocol

As noted above, PIAs identify potential privacy and security issues and concerns. POGO's Privacy Impact Assessment policy includes the following critical statement: "The POGO PIA process determines the privacy, confidentiality, and security risks (low, medium, or high) associated with the collection, use, and disclosure of personal and personal health information. This process also outlines the measures used to mitigate and, wherever possible, eliminate the identified risks."

The Privacy Officer and Program Manager develop and document the plan for implementing appropriate mitigating strategies arising from PIAs with final sign-off from the relevant Program Manager and the Privacy Officer. These strategies are reported prior to implementation to the CEO for approval. This ensures that the findings are complete and accurate from both a program and a risk perspective and also ensures that any recommendations documented in the PIA are agreed upon through a consensus-based approach.

POGO also has a number of policies outlining the acceptable use of POGO information systems, which are intended to inform POGO staff and researchers of the appropriate, authorized and unauthorized uses of those systems to ensure that vulnerabilities are not introduced into POGO's information processing facilities.

Information security risks identified through TRAs, vulnerability assessments and other security audit activities are assessed by the Director, Information Technology, Data and Analytics together with the IT team and third parties as necessary. Risk treatment plans are developed and specific mitigation activities are assigned, tracked and reported to senior management.

c) Benchmarking

Privacy and security risks shift over time, and the corresponding controls at POGO may therefore be expected to evolve. While *PHIPA* provides direction on compliance, stakeholder expectations regarding PHI practices change over time, as do associated regulatory and best practices. In addition, the Ontario IPC conducts a rigorous privacy review every three years, providing a snapshot of POGO's Privacy and Security Programs as benchmarked against current standards and practices. POGO's Director, Information Technology, Data and Analytics and the Privacy Officer also engage on an ongoing basis in informal discussions with other Prescribed Entities with a view to benchmarking and ongoing re-assessment of privacy and security program attributes and controls, shifting trends and emerging national and international best practices.

d) Compliance Monitoring

Effective risk identification tools, like those employed by POGO, are only effective if identified risks are acted upon. The Privacy Officer, the Director, Information Technology, Data and Analytics and applicable Program Managers are responsible for implementing recommendations generated in response to PIAs and TRAs, and by means of other risk identification tools. POGO has a monitoring program that documents the identified problem, the related recommended actions and the mitigating strategies implemented. POGO maintains a master log/inventory to ensure that recommendations are duly implemented.

e) Business Continuity and Disaster Recovery

A Business Continuity and Disaster Recovery (BCDR) Plan is a critical component to the recovery of data holdings when a disaster occurs. POGO has a BCDR Plan which ensures that privacy and information security concerns are anticipated and well planned for, and that they are considered throughout a disaster and may be factored proactively into decisions made in real time.

The Director, Finance and Administration, the Director, Information Technology, Data and Analytics and the Privacy Officer are involved with the POGO BCDR Plan. It is of critical importance that a plan is in place that protects the data holdings from destruction and safeguards the vital records of POGO and its clients. The absence of a BCDR Plan often presents very real risks to privacy and information security. By its very nature, a plan of action in an emergency will take an organization outside of its normal processes. Such plans are critical to the privacy and security of data holdings in order to minimize all risks possible.

4. Program Controls

a) Policies

POGO's privacy and security policies set the tone for and its approach to information management practices. Moreover, the *POGO Privacy and Data Security Code* and its policies and procedures regarding the confidentiality and security of data, retention and destruction of data and de-identifying PHI all address the collection, use, disclosure and retention of personal health information. These POGO documents are based on the Canadian Standards Association's Model Code for the Protection of Personal Information, which is the foundation of privacy at POGO. The code embodies the internationally accepted privacy principles of minimal collection, identification of use, disclosure and retention and the right of access and correction.

POGO's privacy and security policies communicate the goals and directions set by POGO's Board of Directors, the POGO Privacy and Data Security Committee, the Director, Information Technology, Data and Analytics and the Privacy Officer. These policies also enable the organization to meet legislative requirements and other goals in relation to information management and data protection. Finally, policies are an extension of the governance structure, setting out the duties and responsibilities for privacy and security throughout the organization in clear and unequivocal terms.

POGO's privacy and security policies are accessible, transparent, and comprehensive. From 2005 to 2020, the Ontario IPC found POGO's program to be consistent with best practices in information management. All recommendations made by the Ontario IPC are implemented following IPC reviews. Improvements to POGO's Privacy and Security Program through an ongoing program and policy revision process ensures that the policies remain current and up-to-date.

b) Procedures and Protocols

POGO has set out policies and procedures regarding both privacy and information security.

c) Training and Awareness

The *POGO Privacy and Security Governance and Accountability Framework* is supported by a robust internal and external training and awareness program that includes a number of key initiatives:

POGO's shared internal privacy folder includes comprehensive information about POGO's Privacy and Security Program, policies and procedures, questions and answers, guidelines and other key privacy- and security-related documents.

- Mandatory and traceable privacy and security training is documented formally in POGO's policy relating to staff training and education, including:
    - Role-based privacy and security orientation for all new agents
    - Ongoing role-based privacy and security training at least annually for current agents
    - Confidentiality agreements that are renewed each year with POGO agents (individuals who act for, or on behalf of, POGO and who may or may not be employees of POGO and who include POGO staff, the POGO Board, researchers, volunteers, or those who are seconded employees to POGO)
    - Ad hoc training and information sessions delivered to highlight new and emerging trends in privacy and information security

  - Research project teams privacy and security training
- Ongoing communications to report on, and raise awareness of, privacy and security matters among POGO staff, researchers and the POGO network of childhood cancer professionals across Ontario in order to foster a privacy-protective culture.
- On an ongoing basis, POGO staff receive email correspondence related to POGO's Privacy and Security Program and practices.
- The Director, Information Technology, Data and Analytics and the Privacy Officer update the CEO on a regular basis regarding privacy and security issues/concerns or new initiatives/reporting.
- The Director, Information Technology, Data and Analytics and the Privacy Officer report to the Board on an annual basis or more regularly as required.

d) Secure Information Lifecycle

POGO recognizes that information is only secure if it is secure throughout its entire lifecycle: Collection, registration, access, retention and storage, use, disclosure and destruction. Accordingly, POGO has implemented administrative (organizational), technical and physical safeguards to protect the privacy of individuals whose PHI POGO receives, and to maintain the confidentiality of that PHI. A comprehensive set of policies, guidelines and standard operating procedures reflects best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of POGO's information assets, including policies on encryption and secure destruction.

e) Breach and Incident Management Protocols

The POGO Privacy and Security Policies and Procedures Manual and its operational policies include a coordinated approach to breach and incident management to appropriately respond to and recover from privacy and security weaknesses and incidents. Reporting and addressing such incidents promptly will minimize the risks or harm to any individuals whose data may be compromised and to POGO's business. All POGO agents are expected to protect POGO's data holdings through immediate identification of their concerns to POGO's Privacy Officer regarding actual or potential privacy or security incidents, including any perceived deficiencies in privacy and security procedures and controls, according to the Policy 9.1.14 *Privacy Breach and Incident Management*.

The *Privacy Breach and Incident Management* policy has the following six steps:

- Step 1: Identification and initial notification
- Step 2: Containment
- Step 3: Investigation
- Step 4: Documentation
- Step 5: Notification
- Step 6: Action and recommendations (remediation/prevention of future breaches)

POGO has breach protocols for breaches of low-, medium- or high-risk, with distinct orders of events and notification processes for low-risk breaches versus medium- or high-risk breaches.

POGO has developed staff training sessions to ensure organization-wide understanding of the six key steps in its breach management protocols.

f) Agreements

POGO is a leading source of credible pediatric oncology health information and data in Ontario. Hospitals and healthcare practitioners entrust sensitive data to POGO. Therefore, POGO requires all agents to sign the POGO Confidentiality and Non-Disclosure Agreement on an annual basis.

POGO is committed to maintaining the trust of those who provide data by negotiating and signing DSAs that require POGO to maintain the privacy and ensure the security of its data holdings. In addition, POGO also administers a data request process for research and other purposes consistent with POGO’s mandate.

- Prior to releasing aggregate data, a POGO Data Request Form is completed and reviewed by the Senior Database Administrator and Privacy Officer.
- Prior to releasing record-level data, authorized POGO agents complete a POGO Data Request Form, submit a research proposal and complete a PIA.
- Prior to releasing record-level data, external researchers complete a POGO Data Request Form, submit a research proposal, supply research ethics board (REB) approval documentation, complete a PIA and sign both the Research Agreement and the POGO Confidentiality and Non-Disclosure Agreement. The process for record-level data requests requires individuals to agree to comply with the conditions and restrictions imposed by POGO’s Privacy Program relating to the collection, purpose, use, security, disclosure and return or disposal of data, and permits POGO to audit compliance upon reasonable notice.

g) Third-Party Service Provider Management

POGO has limited outsourcing arrangements involving information or information systems with third-party vendors (that is, arrangements where the vendor performs a function or process that could not be provided by POGO itself). Examples of outsourcing arrangements include POGONIS database platform development and system and server programming. All such outsourcing arrangements are formally documented in written contracts. For third parties with direct access to PHI, those service providers must also sign confidentiality agreements with POGO.

h) External Communication

POGO’s commitment to privacy and security is also supported by a series of external communication efforts. POGO makes information about its privacy and security policies readily available on its website, including an overview of its Privacy and Security Program, an FAQs section and contact information for the Privacy Officer. The POGO Data Request Form is also publicly available on POGO’s website.

POGO values its cooperative relationship with the IPC. To that end, POGO’s Privacy Officer is charged with ensuring that the views, feedback and recommendations from the IPC are incorporated into POGO’s Privacy and Security Program as applicable and communicated to the IPC, as well as to POGO’s stakeholders.

5. Audits, Compliance and Reporting

a) Privacy and Security Audit Program

The Director, Information Technology, Data and Analytics and the Privacy Officer carry out POGO's Privacy and Security Audit Program. The governing document *POGO Privacy and Security Audit Program* sets out five types of privacy and security compliance monitoring:

1. POGO internal programs' compliance with privacy and security policies and practices, include comparing internal practices against best practices.
2. POGO data recipients' compliance with the Research Agreement and the POGO Confidentiality and Non-Disclosure Agreement for the purpose of POGO's review of the recipients' use and management of the data and plans for disclosure of research findings. This review is a measure of the data recipients' compliance rather than POGO's, but it demonstrates POGO's due diligence in rigorous management and the integrity of its management of researchers' privacy and security compliance.
3. Privacy and security compliance across the POGO organization with policies relating to a particular topic. Priority for topic reviews is given to highly sensitive, visible or generally high-risk activities that cut across the organization. This review provides a wider angle on a particular topic and can also be used to identify policy gaps and/or actual vulnerabilities.
4. The Director, Information Technology, Data and Analytics and the Privacy Officer triennially review all privacy and security policies and procedures to review and assess compliance against current legislation and amend accordingly. All amendments will be reported to the POGO Privacy and Data Security Committee.
5. All security policies and procedures and audit of all security processes, including the review of system control and audit logs and TRAs (vulnerability, penetration and ethical hacks).

The governing document identifies POGO's audit schedule. POGO's *Privacy and Security Audit Program* is consistent with best practices in that it monitors compliance with legislative or regulatory requirements, internal policy and any other contractual obligations pertaining to privacy and security.

b) External Review of POGO

As stated above, the POGO Privacy Program itself is the subject of an audit or review every three years by the IPC. This external review provides POGO and its stakeholders with independent and objective verification that POGO maintains a standard of excellence in maintaining the privacy and security of the sensitive data entrusted to it. The last external review was conducted in 2020, and POGO's status as a Prescribed Entity under Section 45 of Ontario's *PHIPA* was renewed.

c) External Privacy Expert/Advisor

When privacy issues cannot be resolved, an independent third-party Privacy Advisor will be retained to advise and act as a Mediator. This advisor's role will be to investigate the issues thoroughly and work with the Director, Information Technology, Data and Analytics, the Privacy Officer and the complainant to successfully resolve the matter. A report will then be prepared and, if recommendations are made, the Privacy Advisor will work with the Director, Information Technology, Data and Analytics, Privacy Officer and the CEO or delegates to amend POGO's policies and procedures. The report will then be provided to the POGO Board for their review. To date, engaging an external advisor has not been warranted.

d) Compliance Monitoring/Reporting

A compliance monitoring program must be able to document a link between recommended actions and the controls that are implemented. POGO maintains a privacy and security master inventory to ensure that recommendations are duly implemented.

The Privacy Officer is responsible for documenting and reporting significant work in all areas of the Privacy Program (including PIAs, privacy audits conducted under the *Privacy and Security Audit Program*, breaches, policy development, training and any highlights from the IPC reports, including recommendations and their implementation) to the POGO Privacy and Data Security Committee, which includes Senior Management, on an annual basis or more often as required. Formally the Director, Information Technology, Data and Analytics, Privacy Officer and the CEO are responsible for reporting compliance and other privacy and security matters annually to the POGO Board.

Under the *Privacy and Security Audit Program*, POGO prepares reports for all audits. These are presented not only to the program manager or researcher, but also to the POGO Privacy and Data Security Committee and the CEO.

The Director, Information Technology, Data and Analytics and the Privacy Officer may also be required to prepare presentations to Senior Management and/or the POGO Board on sensitive privacy or security issues on an ad hoc basis.

Review of the *POGO Privacy and Security Governance and Accountability Framework*

POGO is committed to maintaining the currency of its Privacy and Security Program, ensuring always that it is consistent with best practices as they evolve over time. Accordingly, this *Framework* is designed to be a living document and will be updated as privacy and security practices continue to develop. POGO will formally review this document and relevant policies on a yearly basis, at a minimum.

More specifically, the Director, Information Technology, Data and Analytics and the Privacy Officer will jointly assume the responsibility to coordinate the review of all privacy and security policies, as well as any related procedures and practices, to ensure that they remain current and up-to-date. This review will take place in accordance with the triennial audit set by the IPC.

The Director, Information Technology, Data and Analytics and the Privacy Officer will ensure that the required approval process is followed. In the case of changes to the privacy and security policies, these will be reviewed by the CEO or delegate(s) in consultation with the POGO Privacy and Data Security Committee if required. In some cases, the approval process and the extent of internal and external communication are dependent on the nature of the document and may require approval.

Updates or changes to POGO’s privacy and security policies, procedures, and practices will take into consideration health orders, guidelines, fact sheets and best practices issued by the IPC of Ontario, evolving industry privacy and security standards and best practices and amendments to privacy and personal health information legislation relevant to POGO as well as recommendations from privacy and security audits, PIAs and complaint and breach investigations, as the case may be.