Pediatric Oncology Group of Ontario

480 University Avenue, Suite 1014, Toronto, Ontario M5G 1V2

Report to the Information and Privacy Commissioner of Ontario

Three-Year Review as a Prescribed Entity Under PHIPA

Year of Submission: October 2020

Table of Contents

Background Information

Introduction

The Pediatric Oncology Group of Ontario (POGO) was founded in 1983 by a group of pediatric oncologists to champion childhood cancer care and control. As the representative voice of the childhood cancer community, POGO is committed to ensuring that all of Ontario's children have equal access to state-of-the-art diagnosis, treatment, and required ancillary services and the greatest prospects for survival with an optimal quality of life.

POGO's mandate is to:

- Provide advice, leadership, and provincial coordination - functioning as principal source of advice to the Ministry of Health and Long-Term Care (MOHLTC), the Local Health Integration Networks (LHINs), and other stakeholder groups and organizations on childhood cancer control in Ontario;
- Operate as a collegial alliance of specialty programs, community services, parents, survivors, and the voluntary sector;
- Gather, analyze, and share accurate data on the population to support planning and care delivery and standardize all reporting on patterns of disease and care;
- Identify, address, and resolve issues, gaps, and obstacles to state-of-the-art childhood cancer care;
- Undertake the necessary monitoring of issues and programs, surveillance, and information management, including the collection, management, and dissemination of information in support of POGO's core activities;
- Bring about family-centred, coordinated, and well-integrated childhood cancer system for Ontario;
- Manage provincial programs, including the Satellite, AfterCare, and Community Interlink Nursing Programs, which are delivered by academic teaching and community hospitals;
- Provide and regularly renew evidence and consensus guidelines for childhood cancer control;
- Provide ongoing knowledge transfer, education, and professional updates to support best practices and raise awareness about childhood cancer;
- Stimulate scientifically credible, multi- and inter-disciplinary research that refines knowledge and supports evidence-based policy; and
- Provide essential supports for children, survivors, and families.

At that time POGO was a registry that collected data on newly diagnosed cases in 1985. At that time the registry collected unidentifiable demographic information and disease specific information on each case diagnosed at one of the five pediatric tertiary centres in Ontario.

The organization is a collaboration of the five specialty tertiary pediatric oncology programs:

- The Hospital for Sick Children (Toronto);
- McMaster Children's Hospital, Hamilton Health Sciences (Hamilton);
- Children's Hospital, London Health Science Centre (London);

- Kingston General Hospital (Kingston);
- Children's Hospital of Eastern Ontario (Ottawa); as well as
- a growing number of partners drawn from community hospitals, community services, other members of the health care sector, families of children who have or have had cancer, corporate and private benefactors, and volunteers.

In 1995, with the realization that POGO was uniquely placed to acquire data on incidence, treatment and outcomes for the entire population of children with cancer in Ontario, POGO began to transition from a registry to a networked electronic information system with the generous support of the Ontario Ministry of Health and Long Term Care.

POGONIS is a relational database and registry capturing data on key selected aspects of cancer in all children diagnosed with cancer in the POGO network and has been carefully selected to contain standardized medical/biologic, treatment, late effects and outcome information. This database enables POGO to collect, use, disclose and analyze personal health information.

Through strong partnerships with the MOHLTC and the childhood cancer community, POGO has built a reputation for recommendations based on solid provincial data, scientific evidence, and extensive clinical experience. Today, POGO is the official source of advice to the MOHLTC on pediatric cancer care and control.

Major components of current POGO activities include:

- Maintaining and updating a unique database on childhood cancer (POGONIS - Pediatric Oncology Group of Ontario Networked Information System);
- Conducting a surveillance program providing accurate population-based data, addressing childhood cancer incidence, trends, and patterns, and compiling statistical information with respect to the management, evaluation, monitoring, and planning of the delivery system;
- Ongoing analysis and policy development regarding strengths and gaps in Ontario's childhood cancer delivery system;
- A provincial program, operating according to practice and program guidelines, for the delivery of pediatric oncology care at satellite sites throughout the province in order to deliver cancer care close to home;
- A network of AfterCare Clinics for survivors for the surveillance, intervention, and investigation of the late effects of childhood cancer;
- Support for families through the POGO Financial Assistance Program (FAP);
- Hospital to home nursing support for child/families through POGO's Pediatric Interlink Nursing Program;
- Assisting childhood cancer survivors to achieve their educational and career goals through the Successful Academic and Vocational Transition Initiative (SAVTI);
- An education and knowledge transfer program providing educational opportunities for health care professionals, including the annual POGO Symposium, Satellite Education Days, and AfterCare Education Days; and
- The POGO Research Unit (PRU) to stimulate and promote pediatric oncology research, engage in collaborative multi-disciplinary investigations, conduct research in the areas of tracking and forecasting within the childhood cancer population, undertake program evaluations (including utilization of health care resources), and assess the burden of illness in the form of long-term health status and health-related quality of life.

Background

The *Personal Health Information Protection Act, 2004* (the *Act*) came into effect on November 1, 2004. The Information and Privacy Commissioner of Ontario (IPC) was designated as the oversight body responsible for ensuring compliance with the *Act*. The *Act* establishes rules for the collection, use, and disclosure of personal health information by health information custodians that protect the confidentiality and privacy of individuals with respect to that personal health information. In particular, the *Act* stipulates that health information custodians may only collect, use, and disclose personal health information with the consent of the individual to whom the personal health information relates, or as permitted or required by the *Act*.

Subsection 45(1) of the *Act* permits health information custodians to disclose personal health information without consent to certain prescribed entities for the 'purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services', provided the prescribed entities meet the requirements of subsection 45(3).

Subsection 45(3) of the *Act* requires each prescribed entity 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. Subsection 45(3) further requires each prescribed entity to ensure that these practices and procedures are approved by the IPC in order for health information custodians to be able to disclose personal health information to the prescribed entity without consent and for the prescribed entity to:

- Collect personal health information from health information custodians;
- Use personal health information as if it were a health information custodian for the purposes of paragraph 37(1)(j) and subsection 37(3) of the *Act*;
- Disclose personal health information as if it were a health information custodian for the purposes of sections 39(1)(c), 44, 45 and 47 of the *Act*;
- Disclose personal health information back to health information custodians who provided the personal health information; and
- Disclose personal health information to governmental institutions of Ontario or Canada as if it were a health information custodian for the purposes of section 43(1) (h).

POGO was first recognized as a prescribed entity on October 31, 2005 and has since completed four further statutory reviews by the IPC: 2008, 2011, 2013, and 2017. While the IPC has been satisfied that POGO has practices and procedures in place that sufficiently protect the privacy and confidentiality of individuals whose personal health information POGO receives, they have made specific recommendations with each review to further enhance these practices and procedures. POGO has addressed each recommendation to the satisfaction of the IPC, and the current recommendations made by the IPC for the 2014-2017 review have been addressed.

Subsection 18(2) of Regulation 329/04 of the *Act* further requires each prescribed entity to make publicly available a plain language description of its functions. This includes a summary of the practices and procedures described above to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information.

Definitions

ACTS Database

- AfterCare Treatment Summary (ACTS) software that uses complex algorithms to generate risks and recommendations tailored to individual survivors based on their treatment history.

Agents (Internal or External)

- PHIPA defines "agents" as individuals who act for, or on behalf of POGO, and who may or may not be employees of POGO.

- Internal Agents include employees, students, and volunteers engaged in work for, or on behalf of POGO
- External Agents include researchers, Interlink Community Nurses, POGO Data Managers, AfterCare Data Managers, POGO FAP Data Managers, SAVTI Counsellors, Board of Directors or other external POGO associates or third party service providers conducting business for or on behalf of POGO. External Agents do not include contractors.

Data Security Committee

- The POGO committee that reviews and approves new and amended privacy and security policies and procedures, and works directly with the Privacy Officer regarding privacy questions, issues, breaches, or other privacy matters.

Information Technology (IT) Team

- Includes the Senior Database Administrator, and Database and System and Network Administrators/Analysts/Programmers.

Interlink Community Nurses

- POGO Interlink nurses coordinate cancer care for children by linking hospital and community services.

FAP - POGO Financial Assistance Program

- Financial assistance for out-of-pocket costs when a child is in treatment, and that covers a portion of food costs, accommodation when away from home, and care for siblings under 12.

POGO AfterCare Adult Program Hospitals

- The adult hospitals that provide long-term follow up for pediatric cancer survivors.

POGO Satellite Community Hospitals

- Centres that provide components of the cancer treatment and care in community hospitals.

POGO Tertiary Pediatric Oncology Hospital Partners

- The five pediatric teaching hospitals in Ontario that diagnose and treat pediatric oncology cases.

POGONIS Database

- POGO's Networked Information System collects demographic, diagnostic, treatment and outcomes for all cases of childhood cancer in Ontario.

Prescribed Entities

- An organization designated as a Prescribed Entity under section 45(1) of the *Act*.

Privacy and Data Security Code

- The 10 tenets of POGO's Privacy Program.

Privacy and Data Security Procedures

- The procedures that follow the 10 tenets of POGO's Privacy Program.

Privacy and Security Policies and Procedures (the Manual)

- A manual that consists of *POGO Privacy and Data Security Code and POGO Privacy and Data Security Procedures*.

Privacy Team

- Includes the POGO Privacy Officer and the Associate Privacy Officer

The Privacy Program

- Refers to POGO's Privacy Program that consists of the following organizational and administrative materials including: *POGO Privacy and Data Security Code, POGO Privacy and Data Security Procedures*, , POGO's *Security Standards, POGO Privacy and Security Audit Program, Privacy Impact Assessment, Privacy Training, Privacy Complaint Programs, POGO's Privacy and Security Governance and Accountability Framework, POGO's Business Continuity and Disaster Recovery Plan, and POGO's Corporate Risk Management Framework*.

Third Party Service Provider

-is an organization that provides services to POGO pursuant to a third party service agreement. The third party service provider is an agent of POGO except in circumstances where the service is POGO- supervised shredding (disposal) of secured PHI records and does not involve access or use of PHI by the organization.

SAVTI – POGO's Successful Academic Vocational Transition Initiative

- The POGO program that provides survivors with guidance and information as they transition to higher education or to the workforce.

Part 1 – Privacy Documentation

1. Privacy Policy in Respect of POGO's Status as a Prescribed Entity

POGO has a comprehensive Privacy Program in effect in relation to the personal health information it collects, uses, and discloses with respect to its status as a prescribed entity under Ontario's *Personal Health Information Protection Act*, 2004 ("the *Act*"). The Privacy Program is articulated in the following documents: *POGO's Privacy and Data Security Code and POGO's Privacy and Data Security Procedures* (the Manual), *POGO's Privacy and Security Governance and Accountability Framework; POGO's Business Continuity and Disaster Recovery Plan; POGO's Corporate Risk Management Framework;* and *POGO's Security Standards.* (These six documents will be referred to in this report as POGO's "Privacy Program").

Status under the Act

The Privacy Program describes POGO as a prescribed entity under the *Act* and the duties and responsibilities that arise as a result of this designation. The Privacy Program indicates that POGO has implemented policies, procedures, and practices to protect the privacy of individuals whose personal health information it receives and that maintain the confidentiality of that information and that these policies, procedures, and practices are subject to review by the IPC every three years.

The Privacy Program describes POGO's commitment to comply with the provisions of the *Act* and its regulation. Furthermore, the Privacy Program implemented by POGO demonstrates a commitment by POGO to exercise its mandate of planning for provincial pediatric oncology needs, coordinating the allocation of funding, maintaining the provincial pediatric oncology database, and conducting research focusing on childhood cancer in accordance with the *Act* and its regulation.

Privacy and Security Accountability Framework

The Chief Executive Officer of POGO is ultimately accountable for ensuring compliance with the *Act* and its regulations, in addition to ensuring compliance with its privacy and security policies and procedures. Policy #9.4.1 (*Privacy and Security Governance and Accountability Framework*), Policy 9.3.3. (*Delegation of Roles and Responsibilities*), and POGO's Privacy and Data Security Code (*Principle 1 – Accountability*) point out that POGO's Chief Executive Officer reports to the Board of Directors of POGO, which is comprised of POGO tertiary pediatric hospital Program Directors, and other selected members who contribute specific, professional expertise (e.g., other health care professionals, human resources, financial management, etc.).

The Privacy Program, which includes the Security Program, identifies the position of the Privacy Officer as having the authority to manage the Privacy Program, the Associate Privacy Officer who ensures organizational compliance with the Personal Health Information Protection Act (PHIPA) and Information and Privacy Commissioner (IPC) best practices and orders and POGO's System & Network Analyst, and Database Administrator, Analyst & Programmer as having the day-to-day authority to manage POGO's Information Technology (IT) Security Program. The Privacy

Program also defines the responsibilities of these positions by identifying the unique roles of each individual, as related to the specific program functions and key activities. POGO's Privacy Officer reports ultimately to the Chief Executive Officer of POGO. POGO's System & Network Analyst reports to the Privacy Officer.

Collection of Personal Health Information

The Privacy Program and Policy #9.1.4 *(Collection of Personal Health Information)* describe the purpose for which POGO collects personal health information, the type of personal health information it collects, and the POGO tertiary oncology hospitals and other organizations (e.g., POGO Satellite Community Hospitals, POGO AfterCare Adult Program Hospitals and other prescribed entities), from which it collects the information. The Privacy Program and Policy # 9.1.4 further specify that the collection of personal health information must be consistent with the collection of personal health information permitted by the *Act* and its regulation.

The Privacy Program and Policy #9.1.4, and the *Privacy and Data Security Code – Principle 4 Limiting Collection* state that POGO will not collect personal health information if other information will serve the intended purpose and not to collect more personal health information that is reasonably necessary to meet the purpose. The policy and Principle ensure that both the amount and the type of personal health information collected is limited to that which is reasonably necessary for its stated purpose.

POGO's Privacy and Data Security Code and Policy #9.1.5 (*Data Holding Containing Personal Health Information)* indicate that POGO maintains a list and associated purposes of its data holdings of personal health information. The Privacy Officer is identified as the contact for obtaining further information in relation to the purposes, data elements, and data sources of each data holding of personal health information.

Use of Personal Health Information

The Privacy Program and Policy # 9.1.7 (*Use of Personal Health Information for Research*) and Policy # 9.1.1 (*Process for 44 and 45 Projects*) and Policy # 9.1.13 (*De-Identified and Aggregate Personal Health Information)* describe the purpose for which POGO uses personal health information and includes policies and procedures that distinguish between the use of personal health information and the use of de-identified and/or aggregate information under section 45 of the *Act* and the use of personal health information for research purposes. The Privacy Program further specifies that the use of personal health information must be consistent with the uses of personal health information permitted by the *Act* and its regulation.

The Privacy Program states that POGO will not use personal health information if other information will serve the purpose and will not use more personal health information than is reasonably necessary to meet the purpose. Policies, procedures, and practices have been implemented in this regard to establish limits on the use of personal health information by agents. These policies are outlined in the POGO *Privacy and Data Security Procedures* within Principle 2 (*Identifying Purposes*) and within Principle 4 (*Limiting Collection*).

In addition to POGO's *Privacy and Data Security Procedures* within Principle 2 (*Identifying Purposes*) and Principle 4 (*Limiting Collection*), Policy #9.2.6 (*Retention, Return and Destruction of Data)* articulate that POGO is responsible for personal health information used by its agents and identifies the policies, procedures, and practices implemented to ensure agents only collect, use, disclose, retain, and dispose of personal health information in compliance with the *Act* and its regulation and in compliance with POGO's privacy and security policies, procedures, and practices.

Disclosure of Personal Health Information

The Privacy Program and Policy #9.1.8 *(Disclosure of Personal Health Information*), POGO's *Privacy and Data Security Procedures*, specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) and Principle 1 (*Accountability*), and Policy #9.1.1 *(Process for 44 and 45 Projects*) identify when, and under what circumstances, personal health information is permitted to be disclosed for research purposes (44 purposes) and 45 (analysis) purposes, and identify the purposes for which personal health information is disclosed, the organizations/individuals to whom information is disclosed, and the requirements that must be satisfied prior to such disclosures. POGO ensures that each disclosure is consistent with the disclosures of personal health information permitted by the *Act* and its regulation.

The above policies and procedures and Policy # 9.1.13 (*De-Identified and Aggregate Personal Health Information)* distinguish between the purposes for which and the circumstances in which personal health information is disclosed and the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed. The privacy policies and procedures address methods of de-identification and aggregation to ensure that the information cannot be utilized, either alone or with other information, to identify an individual. POGO reviews all de-identified and/or aggregate information prior to disclosure to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.

Furthermore, POGO's privacy policies and procedures state that it will not disclose personal health information if other information will serve the purpose and that it will not disclose more personal health information than is necessary to meet the purpose of the disclosure. Specifically, POGO *Privacy and Data Security Procedures* set out in principles 4 (*Limiting Collection*) and 5 (*Limiting Use, Disclosure, and Retention*) clear rules for limiting collection, use, and disclosure of personal health information and the statutory requirements that must be satisfied prior to disclosure. Further, personal health information in the custody or control of POGO is only disclosed as is permitted or required by law, including PHIPA and its regulation.

Secure Retention, Transfer, and Disposal of Records of Personal Health Information

The Privacy Program and Policy #9.2.6 (Retention, Return and Destruction of Data), Policy #9.2.9 (Secure Transfer of Personal Health Information) and Policy #9.2.7 (Personal Health Information on Mobile Devices) address the secure retention of records of personal health information in paper and electronic format, including the acceptable use of portable media and mobile devices for the collection, transfer, and storage of personal health information. The Privacy Program addresses the permitted retention periods and specifies methods for the secure

transfer and destruction of personal health information depending on the media on which it is stored. Identifiable personal health information is secured and only retained for as long as necessary to meet the purposes of long-term analysis and reporting. Personal health information that is no longer required to fulfill the identified purposes is de-identified or securely destroyed. POGO has developed guidelines and implemented procedures to govern the de-identification of personal health information and has developed guidelines and implemented procedures to govern the secure destruction of personal health information.

Implementation of Administrative, Technical, and Physical Safeguards

The Privacy Program and the Privacy and Data Security Code Principle 7 (*Safeguards)* and Policy #9.2.5 (*Physical/Office Security)* also describe the security measures that POGO has in place to safeguard personal health information and protect the privacy of individuals to whom the information pertains. The policies and procedures cover administrative, physical, and technical security controls implemented to protect personal health information from unauthorized access, copying, modification, use, disclosure, theft, loss, and improper disposal. The safeguards in place include:

a. Physical measures (e.g., locked facility with tracked card access, locked filing cabinets, restricted access to offices, internal/external video monitoring of POGO);
b. Organizational measures (e.g., employee confidentiality agreements (with the potential for immediate dismissal where applicable), limiting access on a "need-to-use" basis, staff training to ensure awareness of the importance of maintaining the confidentiality of personal health information);
c. Technological measures (e.g., the use of firewalls, Virtual Privacy Networks (VPN), File Transfer Protocol (FTP), separation of networks, passwords, encryption, audit logs, data modification logs, backup and recovery systems); and
d. De-Identification (e.g., personal health information is de-identified, and is further de-identified by removing data fields, such as name, health card number, date of birth, etc.).

Inquiries, Concerns, or Complaints Related to Information Practices

The Privacy Program identifies the Privacy Officer of POGO as the contact to whom individuals may direct inquiries, concerns or complaints related to the privacy policies, procedures, and practices of POGO and questions related to POGO's compliance with the *Act* and its regulation. The Privacy Program specifies that contact information, including the name and/or title and mailing address for the Privacy Officer will be provided on POGO's website and that a standard Privacy Inquiries, Challenges, and Complaints form will be made available to the public for filing inquiries or complaints.

The Privacy Program also states that individuals may direct complaints regarding POGO's compliance with the *Act* and its regulation to the IPC and that POGO provides the mailing address and contact information for the IPC on its website.

Transparency of Practices in Respect of Personal Health Information

The Privacy Program commits POGO to being transparent regarding its practices in respect of handling personal health information and states that POGO shall make the POGO *Privacy and Data Security Code*, frequently asked questions (FAQs), and other relevant documents freely available to the public on its website.

2. Policy and Procedures for Ongoing Review of Privacy Policies, Procedures, and Practices

POGO's *Privacy and Security Policies and Procedures Manual* includes policies and procedures governing the regular review of its privacy policies, procedures, and practices. The policies state that POGO shall review its Privacy Program at minimum every September or more frequently should there be changes in technology, best practices, or the *Act* and its regulation.

POGO's Privacy and Security Policies and Procedures Manual state that it is the responsibility of the Privacy Officer to undertake the review, set out the procedure to be followed in undertaking the review and the timeframe in which the review is undertaken. At a minimum, POGO's policies and procedures are reviewed annually. As a result of the review, if deemed necessary the Privacy Officer will amend and/or draft new privacy policies, procedures and practices and will forward to POGO's Data Security Committee for review and approval before the changes are implemented and communicated.

In undertaking the review and determining whether amendments and/or new privacy policies, procedures, and practices are necessary, POGO Policy #9.1.2 (*The Review of Privacy and Security Policies and Procedures*) indicates that updates or changes to POGO's privacy policies, procedures, and practices will take into consideration:

- Any health orders, guidelines, fact sheets, and best practices issued by the IPC under the *Act* and its regulation;
- Evolving industry privacy standards and best practices;
- Amendments to the *Act* and its regulation relevant to the prescribed entity;
- Recommendations arising from privacy and security audits, privacy impact assessments, investigations into privacy complaints, privacy breaches, and information security breaches;
- Whether the privacy policies, procedures, and practices of the prescribed person or prescribed entity continue to be consistent with its actual practices; and
- Whether there is consistency between and among the privacy and security policies, procedures, and practices implemented.

The Privacy Program further states that the Privacy Officer is responsible for determining the procedure to be followed in communicating the amended or newly developed privacy policies, procedures, and practices. For agents, the Privacy Officer is guided by POGO Policy #9.3.1 (*Privacy and Security Training*) which stipulates that the Privacy Officer will be responsible for determining the method and nature when communicating the amended or newly developed privacy

policies, procedures, and practices. The Privacy Program also identifies that the Privacy Officer is responsible for the procedure to be followed in reviewing and amending the communication materials available to the public and other stakeholders as a result of the amended or newly developed privacy policies, procedures and practices.

Compliance with the *Privacy and Security Policies and Procedures Manual* is mandatory for all agents of POGO and is monitored by POGO's Privacy Team. The Privacy Program specifies that a contravention of the policies and procedures constitutes a breach and includes policies and procedures for corrective actions to be taken in the event of non-compliance.

The Privacy Program includes policies and procedures governing POGO's Privacy Audit Program. The intent of the Privacy Audit Program is to assess compliance with POGO policies and to demonstrate POGO's privacy protection commitment to data providers, the public, and data users.

The Privacy Program states that POGO's Privacy Officer shall conduct an annual privacy audit that involves reviewing four key areas including:

1. Internal POGO Program Area Privacy Compliance Reviews;
2. External Privacy Compliance Reviews;
3. Internal POGO Privacy Topic Reviews;
4. Internal POGO Privacy and Security Policies and Procedures; and
5. Internal POGO Security Audits.

3. Policy on the Transparency of Privacy Policies, Procedures, and Practices

POGO Policy #9.1.3 (*Transparency of Privacy Policies, Procedures and Practices*) and the POGO *Privacy and Data Security Code*, specifically Principle 8 (*Openness*), states that POGO is committed to the transparency of information regarding its policies, procedures, and practices relating to the management and protection of personal health information. This information is available upon request, in written format, and where applicable, is posted on its website. The information available on the website includes the following:

1. POGO's *Privacy and Data Security Code;*
2. POGO's privacy brochure;
3. Answers to FAQs;
4. Cover letter from the IPC Review (dated October 31,2017) approving the documentation related to the review by the IPC in respect of POGO's policies, procedures, and practices implemented to protect the privacy of individuals whose personal health information it holds and to maintain the confidentiality of that information, detailed written Report and sworn affidavit;
5. A list of the data holdings of personal health information maintained by POGO; and
6. The name, title, mailing address, and contact information of the persons(s) to whom inquiries, concerns, or complaints regarding compliance with the privacy policies, procedures, and practices implemented and regarding compliance with the *Act* and its regulation may be directed.

For privacy and security purposes, POGO does not make available to the public and other stakeholders its *Privacy and Data Security Procedures,* policies outside of the *Privacy and Data Security Code,* and privacy impact assessments of data holdings containing personal health information.

In addition, Principle 8 (*Openness*) specifies the minimum content of the POGO privacy brochure and/or FAQs as follows:

1. The status of POGO under the *Act;*
2. POGO's obligations under the *Act;*
3. The types of personal health information collected;
4. The POGO tertiary hospital partner organizations and prescribed registry from which personal health information is collected;
5. The purposes for which personal health information is collected;
6. The purposes for which personal health information is used; and if identifiable information is not routinely used, the nature of the information that is used;
7. The circumstances under which and the purposes for which personal health information is disclosed;
8. The entities to whom personal information is disclosed;
9. Summary of administrative, physical, and technical security controls, including the steps taken to protect personal health information against theft, loss, and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification, or disposal; and
10. The name and/or title, mailing address, and contact information of the person(s) to whom inquiries, concerns, or complaints regarding compliance with the privacy policies, procedures, and practices implemented and regarding compliance with the *Act* and its regulation may be directed.

In respect of the transparency of policies and procedures, Principle 8 (*Openness*) states that the Chief Executive Officer of POGO is responsible for ensuring that the above information is published on POGO's website.

4. Policy and Procedures for the Collection of Personal Health Information

POGO *Policy #9.1.4 (Collection of Personal Health Information)* and POGO's Privacy and Data Security Code - Principle #4 (*Limiting Collection*) identifies the purposes for which personal health information is collected by POGO, the nature of the personal health information that is collected, the health care custodians, and Prescribed Registry from whom the personal health information will be typically collected, and the secure manner in which personal health information is collected.

POGO's policies and procedures articulate a commitment not to collect personal health information unless the collection is permitted by the *Act* and its regulation, not to collect personal health information if other information will serve the purpose, and not to collect more personal health information than is reasonably necessary to meet the purpose. POGO only collects personal health information that is required for its stated purposes and does not collect more personal health information than is necessary to meet the stated purposes.

Personal health information is typically collected, on an on-going basis from POGO's tertiary pediatric oncology hospital partners and other organizations (e.g., POGO Satellite Community Hospitals, POGO AfterCare Adult Program Hospitals, other prescribed entities, and a prescribed registry).

POGO enters into data sharing agreements with its tertiary pediatric oncology hospital partners, POGO AfterCare Adult Program Hospitals, other prescribed entities, and a prescribed registry, and maintains POGO/hospital agreements with the POGO Satellite Community Hospitals to set out purposes and obligations related to the collection of personal health information. POGO's Privacy Officer monitors compliance with the terms of all the data sharing agreements and other agreements and those terms are ultimately enforced by POGO's Board of Directors.

Agents are required to comply with the policy and procedures in regard to the collection of personal health information. Compliance is enforced by the Privacy Officer who is also responsible for enforcing consequences of a breach. Compliance is also audited in accordance with POGO's policies and procedures in respect of POGO's Privacy Audit Program, and Policy #9.1.15 (*Privacy Audits*) which state that privacy audits are carried out annually at minimum by the Privacy Officer.

POGO Policy #9.1.16 (*Privacy Breach and Incident Management*) requires that agents of POGO notify the Privacy Officer of POGO at the first reasonable opportunity if a breach or suspected breach of privacy has occurred. The definition of a breach of privacy includes the failure to comply with POGO's privacy and security policies and procedures.

Review and Approval Process

In 1985 and again in 1995, POGO and its tertiary pediatric oncology hospital partners mutually determined and approved the collection of specific personal health information data elements for POGO's primary database POGONIS, (the POGO Networked Information System).. From time to time, additional data elements have been added while others have been modified.

In 2010, POGO secured two grants that allowed POGO to retrospectively add personal health information data elements (treatment and outcome information) to the POGONIS database on the cases diagnosed between 1985 and 1994. This same information was already collected for the 1995 and forward case population. These additional personal health information data elements were reviewed and approved by POGO's Senior Database Administrator, POGO's Past Medical Director who then moved to a Senior Adviser, Policy and Clinical Affairs role. Currently, POGO's Senior Database Administrator, Medical Director, and other external content experts if applicable, are responsible for reviewing and determining whether to approve a collection of personal health information and determining the process and requirements to be followed and were subsequently endorsed by the Program Directors from each of the POGO tertiary pediatric oncology hospitals. The additional retrospective data collection was completed in April 2013.

In addition, POGO maintains six other databases which collect personal health information from its POGO tertiary pediatric oncology hospital partners, clients, POGO Satellite Community Hospitals and AfterCare Adult programs. This data is collected for the following programs for the purposes of management, planning, and service delivery:

- The Successful Academic Vocational Transitional Initiative (SAVTI);
- The POGO Financial Assistance Program (FAP);
- POGO Satellite Program Database;
- Interlink Community Care Nursing Program
- AfterCare Treatment Summaries (ACTS); and
- AfterCare care and service delivery

POGO's policies and procedures outline the criteria that must be considered by POGO's Data Holding Program Manager, and Medical Director or designate, and external content experts if applicable when determining whether to approve the collection of personal health information. The collection of this personal health information is governed by the data sharing agreements POGO has in place with its tertiary pediatric oncology hospital partners, AfterCare Adult Program Hospitals and other prescribed entities and the POGO/hospital agreements it maintains with the POGO Satellite Community Hospitals. The data sharing agreements contain a listing of the personal health information collected and outlines the purpose and obligations of each partner to achieve compliance with data collection.

In addition, the policies and procedures set out the criteria that must be considered by POGO's Data Holding Program Manager, Medical Director or designate, and external content experts (if applicable) who are responsible for determining whether to approve the collection of personal health information to ensure that the collection is permitted under the *Act* and its regulation and that any and all conditions or restrictions set out in the *Act* and its regulation have been satisfied. The criteria also require POGO's Data Holding Program Manager, Medical Director, and external content experts if applicable when determining whether to approve the collection of personal health to ensure that other information, such as de-identified and/or aggregate information will serve the identified purpose such that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

The policies and procedures also set out the manner in which the decision to approve or deny a request for the collection of personal information and the reasons for the decision are documented: the method by which and the format in which the decision is communicated and documented by the parties involved during the process of establishing a data sharing agreement.

Conditions or Restrictions on the Approval

POGO's policy and procedures state that no personal health information shall be collected in the absence of a legally binding data sharing agreement between POGO and its tertiary hospital partners, AfterCare Adult programs, other prescribed entities, prescribed registry or POGO/hospital agreements such as those it maintains with the POGO Satellite Community Hospitals. The conditions or restrictions identified in Policy #9.1.4 (*Collection of Personal Health Information*) including the documentation and/or agreements that must be completed, provided or executed, shall have regard to the requirements of the *Act* and its regulation. Furthermore, the policies require that each data holding be documented with a statement of purpose, a statement of permitted use, and a statement of retention. It is the responsibility of the Chief Executive Officer of POGO to ensure that these conditions have been met prior to the collection of personal health information.

Secure Retention

POGO's Privacy Program requires that records of personal health information are retained in a secure manner and includes policies and procedures addressing and restricting the secure storage of personal health information on paper records, portable media, mobile devices, email, and computer file/database systems. The personal health information collected by POGO is stored in POGONIS, and other POGO databases are housed within the secured data centre with restricted access, in accordance with Policy #9.2.6 (*Retention, Return, Destruction of Data*) regarding procedures for the secure retention of personal health information).

Secure Transfer

POGO's Privacy Program requires that records of personal health information are transferred in a secure manner and includes policies and procedures addressing and restricting the secure transfer of personal health information using paper records, portable media, mobile devices, email, file transfer protocols (FTP), and computer file/database systems. The day-to-day collection of personal health information from POGO's tertiary pediatric oncology hospital partners, Satellite Community Hospitals, and AfterCare Adult Programs is accomplished by secure fax, and/or encrypted electronic transfer in accordance with the policies and procedures Policy #9.2.9 (*Secure Transfer of Records of Personal Health Information*), and Policy #9.2.6 (*Retention, Return, Destruction of Data).*

Secure Return or Disposal

POGO's privacy policies and procedures identify POGO's Privacy Officer as being responsible for ensuring that records of personal health information that have been collected are either securely returned or securely destroyed upon expiry of the retention period as documented in POGO's policies and procedures, data sharing agreements, and project-specific privacy impact assessments.

POGO's policies and procedures state that records of personal health information that are to be returned to the organization from which they were collected must be returned in accordance with the policies and procedures for the Policy #9.2.9 (*Secure Transfer of Records of Personal Health Information),* and Policy #9.2.6 (*Retention, Return, Destruction of Data*).

The Privacy Program states that records of personal health information that are to be destroyed at the expiry of the retention period must be destroyed in accordance with Policy #9.2.6 (*Retention, Return, Destruction of Data)* which outlines the procedure for the secure disposal of personal health information.

5. List of Data Holdings Containing Personal Health Information

POGO maintains an up-to date list and description of its data holdings of personal health information. This information is found in Appendix B of the POGO *Privacy and Data Security Code,* as well as in other documentation available on POGO's website relating to its collection activities.

6. Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information

The Privacy Program addresses the creation, review, amendment, and approval of statements of purpose for data holdings containing personal health information. The Privacy Program outlines that each data holding will have a statement of purpose and will specify the personal health information contained in the data holding, the source(s) of the personal health information, and the need for the personal health information in relation to the identified purpose.

The Privacy Program also identifies the Privacy Officer as responsible for ensuring the process that must be followed in completing the statements of purpose for the data holdings containing personal health information, including the agent(s) or other organizations that must be consulted in completing the statements of purpose and the agent(s) responsible for approving the statements of purpose. The POGO Privacy Officer's role is to manage the Privacy Program and the process to be followed in respect of preparing, reviewing, and approving the statements of purpose for data holdings containing personal health information. The Privacy Program outlines that POGO's Medical Director together with the Data Holding Program Manager, in consultation with external agents where applicable, are consulted in reviewing and amending the statements of purpose and are responsible for approving the amended statements of purpose. Once finalized, the statement of purpose is reviewed and approved by POGO's Chief Executive Officer.

The statements of purpose shall be provided to the health information custodians and prescribed registry from whom the personal health information is collected and to other stakeholders and the general public via the POGO website.

The Privacy Program also sets out that the statements of purpose for the data holdings will be reviewed on an annual basis or sooner in order to ensure their continued accuracy and in order to ensure that the personal health information collected for purposes of the data holding remains necessary for the identified purposes.

The Privacy Officer is responsible for reviewing the statements of purpose, coordinating and documenting the process for amending the statements of purpose, if necessary. The Privacy Program outlines the process that must be followed and the agent(s) that must be consulted in reviewing and (if necessary) amending the statements of purpose and the agent(s) responsible for approving the amended statements of purpose. The policy and procedures further identify the persons and organization(s) that will be provided amended statements of purpose upon approval, including the POGO Tertiary Pediatric Oncology Hospitals, the POGO Satellite Community Hospitals, and POGO AfterCare Adult Program Hospitals, and prescribed registry from whom the personal health information in the data holding is collected.

Compliance with POGO's *Privacy and Security Policies and Procedures Manual* is mandatory for all agents of POGO and is monitored by POGO's Privacy Officer. The Privacy Program also specifies that a contravention of the policies and procedures constitutes a breach and includes policies and procedures for corrective actions to be taken in the event of non-compliance.

Further, the policies and procedures stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*) that states that policies and procedures will be audited annually or sooner if required, and that the POGO Privacy Officers is responsible for conducting the audit and ensuring compliance.

The Privacy Program also requires agents to notify POGO at the first reasonable opportunity, in accordance with the policy and procedures for Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

7. Statements of Purpose for Data Holdings Containing Personal Health Information

For each data holding containing personal health information, the Data Holding Program Manager, Medical Director or designate drafts a statement identifying the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose.

8. Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information

POGO's Privacy Program sets out and implements policies and procedures that limit access to, and use of, personal health information by agents based on the "need to know" principle. In POGO's *Privacy and Data Security Code*, Principle 5 (*Limiting Use, Disclosure, and Retention*) and its procedures, ensures that agents of POGO access and use both the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual, or other responsibilities.

POGO's *Privacy and Data Security Code*, Principle 5 (*Limiting Use, Disclosure, and Retention*) and its procedures, identify the limited and narrowly defined purposes for which and circumstances in which agents are permitted to access and use personal health information. Furthermore, Policy #9.1.6 (*Levels of Access*) sets out the process in granting levels of access to personal health information that may be granted to agents. POGO's policies and procedures ensure that the duties of agents with access to personal health information are segregated in order to avoid a concentration of privileges that would enable single agents to compromise personal health information.

For all other purposes and in all other circumstances, the policy and procedures require agents to access and use de-identified and/or aggregate information, as defined in Policy #9.1.13 (*De-Identifying Personal Health Information*).

In this regard, POGO's policies and procedures explicitly prohibit access to and use of personal health information if other information, such as de-identified and/or aggregate information, will

serve the identified purpose and prohibit access to or use of more personal health information than is reasonably necessary to meet the identified purpose.

In addition, Policy #9.2.18 (*Confidentiality and Security of Data*) prohibits agents from using de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

Review and Approval Process

POGO's *Privacy and Security Policies and Procedures Manual* outlines that the Senior Database Administrator and Medical Director are responsible for, and have set out the process for receiving, reviewing, and determining whether to approve or deny a request by an agent for access to and use of personal health information and sets out various level(s) of access that may be granted by POGO.

In outlining the process to be followed, the policy and procedures also set out the requirements to be satisfied in requesting, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also set out the criteria that must be considered by the Senior Database Administrator and Medical Director for determining whether to approve or deny a request for access to and use of personal health information and, if the request is approved, the criteria that must be considered in determining the appropriate level of access. At a minimum, the Senior Database Administrator and the Medical Director are responsible for determining whether to approve or deny the request and must be satisfied that:

- The agent making the request routinely requires access to and use of personal health information on an ongoing basis or for a specified period for his or her employment, contractual, or other responsibilities;
- The identified purpose for which access to and use of personal health information is requested is permitted by the *Act* and its regulation;
- The identified purpose for which access to and use of personal health information is requested cannot reasonably be accomplished without personal health information;
- De-identified and/or aggregate information will not serve the identified purpose; and
- In approving the request, no more personal health information will be accessed and used than is reasonably necessary to meet the identified purpose.

The policy and procedures set out the manner in which the decision approving or denying the request for access to and use of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; to whom the decision will be communicated; any documentation that must be completed, provided and/or executed upon rendering the decision; the agent(s) responsible for completing, providing

and/or executing the documentation; and the required content of the documentation.

Conditions or Restrictions on the Approval

POGO's *Privacy and Data Security Procedures*, specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) identifies the conditions or restrictions imposed on an agent granted approval to access and use personal health information, such as read, create, update or delete limitations, and the circumstances in which the conditions or restrictions will be imposed.

In the event that an agent only requires access to, and use of personal health information for a specified period, Principle 5 sets out the process to be followed in ensuring that access to and use of the personal health information is permitted only for that specified time period. In these circumstances, POGO has in place project specific expiry dates, which are pre-determined. At a minimum, the Privacy Officer reviews the expiry dates one year from the date that approval was granted.

In the POGO *Privacy and Security Policies and Procedures Manual*, Policy #9.1.6 (*Levels of Access*) prohibits agents who have been granted approval to access and use personal health information from accessing and using personal health information except as necessary for his or her employment, contractual or other responsibilities; from accessing and using personal health information if other information will serve the identified purpose; and from accessing and using more personal health information than is reasonably necessary to meet the identified purpose. POGO ensures that all accesses to, and uses of personal health information are permitted by the *Act* and its regulation.

Further, Principle 5 imposes conditions and/or restrictions on the purposes for which and the circumstances in which an agent granted approval to access and use personal health information is permitted to disclose that personal health information. POGO ensures that any such disclosures are permitted by the *Act* and its regulation.

Notification and Termination of Access and Use

Policy #9.1.6 (*Levels of Access*) states that an agent granted approval to access and use personal health information, as well as his or her supervisor, notify the POGO Privacy Officer when the agent is no longer employed or retained by POGO or no longer requires access to or use of the personal health information.

The policy also outlines the notification process that must be followed. In particular, the policy and procedures identify that the POGO Privacy Officer must be notified; the time frame within which this notification must be provided; the format of the notification; the documentation that must be completed, provided and/or executed; the Privacy Officer who are responsible for completing, providing and/or executing the documentation; the Privacy Officer to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also identify the Privacy Officer and IT Team as the agents responsible for terminating access to and use of the personal health information, the procedure to be followed in terminating access to and use of the personal health information, and the time frame within which access to and use of the personal health information must be terminated.

POGO ensures that the procedures implemented in this regard are consistent with Policy #9.3.4 (*Termination or Cessation of the Employment or Contractual Relationship*).

Secure Retention

The policy and procedures require an agent granted approval to use personal health information for research purposes to securely retain the records of personal health information in compliance with the written research plan approved by the research ethics board (REB) and in compliance with Policy #9.2.6 (*Retention, Return, and Destruction of Data*).

Secure Disposal

The policy and procedures require an agent granted approval to access and use personal health information and to securely dispose of the records of personal health information in compliance with Policy #9.2.6 (*Retention, Return, and Destruction of Data*).

Tracking Approved Access to and Use of Personal Health Information

POGO ensures that a log is maintained of agents granted approval to access and use personal health information and identifies the Privacy Team as the agent(s) responsible for maintaining the log. The policy and procedures also state that documentation related to the receipt, review, approval, denial, or termination of access to and use of personal health information is retained by the Privacy Team which is also responsible for retaining this documentation.

Compliance, Audit, and Enforcement

POGO requires agents to comply with the policy and its procedures, and addresses how compliance will be enforced and the consequences of breach.

In the event that there is no automatic expiry date on the approval to access and use personal health information, regular audits of agents granted approval to access and use personal health information is conducted in accordance with the Policy #9.1.15 (*Privacy Audits*).

The purpose of the audit is to ensure that agents granted such approval continue to be employed or retained by POGO and continue to require access to the same amount and type of personal health information. In this regard, the policy and procedure identifies the Privacy Officer as the agent responsible for conducting the audits and for ensuring compliance with the policy and its

procedures and the frequency with which the audits must be conducted. At a minimum, audits are conducted on an annual basis.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

9. Log of Agents Granted Approval to Access and Use Personal Health Information

POGO maintains a log of agents granted approval to access and use personal health information. The log includes the name of the agent granted approval to access and use personal health information; the data holdings of personal health information to which the agent has been granted approval to access and use; the level or type of access and use granted; the date that access and use was granted; and the termination date or the date of the next audit of access to and use of the personal health information.

10. Policy and Procedures for the Use of Personal Health Information for Research

POGO's *Privacy and Data Security Code* Principle 5 (*Limiting Use, Disclosure and Retention*), Policy #9.1.1 (*Process for 44 and 45 Projects*), and Policy #9.1.7 (Use of Personal Health Information for Research) outlines that POGO permits personal health information to be used for research purposes.

POGO policies and procedures articulate a commitment by POGO not to use personal health information for research purposes if other information will serve the research purpose and not to use more personal health information than is reasonably necessary to meet the research purpose.

POGO requires agents to comply with its policies and procedures and address how compliance will be enforced and the consequences of breach. POGO policies and procedures also stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*), and states that policies and procedures will be audited by the Privacy Officer annually to ensure compliance with the policy and its procedures.

The policy and procedures also require agents to notify the Privacy Officer at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of the policy or its procedures.

Where the Use of Personal Health Information is Permitted for Research

POGO permits personal health information to be used for research purposes as outlined in POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*), and Policy #9.1.7 (Use of Personal Health Information for Research) which sets out the circumstances in which personal health information is permitted to be used for research purposes.

Distinction between the Use of Personal Health Information for Research and Other Purposes

POGO's *Privacy and Data Security Procedures and* Policy #9.1.1 (*Process for 44 and 45 Projects*) distinguishes between the use of personal health information for research purposes (section 44) and the use of personal health information for purposes of section 45 of the *Act*. The criteria that must be considered are outlined in Policy #9.1.1 (*Process for 44 and 45 Projects*) and determine when the use of personal health information is for research purposes and when the use of personal health information is for purposes under section 45 of the *Act*. This policy also designates the Privacy Officer as responsible for, and the procedure which is to be followed when making this determination.

Review and Approval Process

Policy #9.1.1 (*Process for 44 and 45 Projects*) identifies the Privacy Officer and Medical Director as the agents responsible for receiving, reviewing, and determining whether to approve or deny a request for the use of personal health information for research purposes and the process that must be followed in this regard. This policy includes a discussion of the documentation that must be completed, provided and/or executed; the agents responsible for completing, providing and/or executing the documentation; the Privacy Officer to whom this documentation must be provided; and the required content of the documentation.

This policy also addresses the requirements that must be satisfied and the criteria that must be considered by the Privacy Officer,
and Medical Director in determining whether to approve the request to use personal health information for research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy shall have regard to the *Act* and its regulation.

At a minimum, prior to any approval of the use of personal health information for research purposes, the policy sets out that the Privacy Officer and Medical Director are responsible for determining whether to approve or deny the request, to review the written research plan, to ensure it complies with the requirements in the *Act* and its regulation, to ensure that the written research plan has been approved by a REB, and to ensure that the prescribed entity is in receipt of a copy of the decision of the REB approving the written research plan.

In addition, prior to any approval of the use of personal health information for research purposes, the Privacy Officer
and Medical Director are responsible for determining whether to approve or deny the request and ensuring that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the REB. The Privacy Officer
and Medical Director are also responsible for ensuring that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.

The policy also sets out the manner in which the decision approving or denying the request to use personal health information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision is communicated; and to whom the decision is communicated.

Conditions or Restrictions on the Approval

POGO's *Privacy and Data Security Code*, POGO's *Privacy and Data Security Procedures*, and POGO's *Privacy and Security Policies and Procedures Manual* identify the conditions or restrictions that are imposed on the approval to use personal health information for research purposes, including any documentation that must be completed, provided, or executed. In determining the conditions or restrictions that will be imposed, the policies and procedures shall have regard to the *Act* and its regulation. At a minimum, the agent/s granted approval to use personal health information for research purposes are required to comply with subsections 44(6) (a) to (f) of the *Act*.

In addition, the Privacy Officer is also responsible for ensuring that any conditions or restrictions imposed on the use of personal health information for research purposes are in fact being satisfied.

Secure Retention

POGO's *Privacy and Security Policies and Procedures* and Policy #9.2.6 (*Retention, Return and Destruction of Data*) require that the agent granted approval to use personal health information for research purposes, retain the records of personal health information in compliance with the written research plan approved by the REB, and in compliance with the policy and procedure for secure retention, return and destruction.

Secure Return or Disposal

POGO's *Privacy and Security Policies and Procedures* and Policy #9.2.6 (*Retention, Return and Destruction of Data*) sets out that the agent granted approval to use personal health information for research purposes is required to securely return or securely dispose of the records of personal health information or is permitted to de-identify and retain the records following the retention period in the written research plan approved by the REB.

If the records are required to be securely returned to POGO, Policy #9.2.6 (*Retention, Return and Destruction of Data*) stipulates the time frame following the retention period set out in the written research plan within which the records must be securely returned, and the secure manner in which the records must be returned to the designated POGO agent.

If the records of personal health information are required to be disposed of in a secure manner, Policy #9.2.6 (*Retention, Return and Destruction of Data*) requires the records to be disposed of

in accordance with this policy. The policy further stipulates the time frame following the retention period in the written research plan within which the records must be securely disposed of, requires a certificate of destruction to be provided, identifies the Privacy Officer to whom the certificate of destruction must be provided, and identifies the time frame following secure disposal within which the certificate of destruction must be provided. The certificate of destruction confirming the secure disposal of personal health information identifies that the records of personal health information are securely disposed of including the date, time, location, and method of secure disposal employed, and is required to bear the name and signature of the agent who performed the secure disposal.

If the records of personal health information are required to be de-identified and retained by the agent rather than being securely returned or disposed of, Policy #9.1.13 (*De-Identifying Personal Health Information*) requires the records of personal health information to be de-identified in compliance with its policy and its procedures. This policy also stipulates the time frame following the retention period set out in the written research plan within which the records must be de-identified.

Further, this policy identifies the Privacy Officer as the agent responsible for ensuring that records of personal health information used for research purposes are securely returned, securely disposed of, or de-identified within the stipulated time frame following the retention period set out in the written research plan and the process to be followed in the event that the records of personal health information are not securely returned, a certificate of destruction is not received, or the records of personal health information are not de-identified within the time frame identified.

Tracking Approved Uses of Personal Health Information for Research

Policy #9.1.1 (*Process for 44 and 45 Projects*) requires that a log is maintained of the approved uses of personal health information for research purposes and identifies the Privacy Team as responsible for maintaining such a log. The policy also outlines where written research plans, copies of the decisions of REB's, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the use of personal health information for research purposes are retained and the Privacy Team who are responsible for retaining this documentation.

Where the Use of Personal Health Information is not Permitted for Research

POGO permits personal health information to be used for research purposes as outlined in POGO's *Privacy and Data Security Procedures* which sets out the circumstances in which personal health information is permitted to be used for research purposes.

As per POGO's Privacy and Data Security Procedures, POGO prohibits the use of PHI for research purposes when the REB rules accordingly, and indicates that de-identified information may be used if the REB rules accordingly.

Review and Approval Process

POGO permits de-identified and/or aggregate information to be used for research purposes, POGO's *Privacy and Data Security Code and its Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) identifies the Privacy Officer and Medical Director as the agents responsible for receiving, reviewing, and determining whether to approve or deny a request for the use of personal health information for research purposes and the process that must be followed in this regard. This policy includes a discussion of the documentation that must be completed, provided and/or executed; the agents responsible for completing, providing and/or executing the documentation; the Privacy Officer, to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to use de-identified and/or aggregate information for research purposes. At a minimum, the policy and procedures require the de-identified and/or aggregate information to be reviewed prior to the approval and use of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The Privacy Officer and Medical Director are responsible for undertaking this review.

The policy and procedures also set out the manner in which the decision approving or denying the request for the use of de-identified and/or aggregate information for research purposes and the reasons for the decision must be documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

POGO's *Privacy and Data Security Code, POGO's Privacy and Data Security Procedures, and Policy #9.1.1* (*Process for 44 and 45 Projects) and* Policy #9.1.1 (*Process for 44 and 45 Projects*) also identify the conditions or restrictions that will be imposed on the approval to use de-identified and/or aggregate information for research purposes, including any documentation that must be completed, provided or executed and the Privacy Officer as the agent(s) responsible for completing, providing or executing the documentation.

At a minimum, the policy and procedures prohibit an agent granted approval to use de-identified and/or aggregate information for research purposes from using that information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

The policy and procedures also identify the Privacy Officer as the agent responsible for ensuring that any conditions or restrictions imposed on the use of de-identified and/or aggregate information for research purposes are in fact being satisfied.

11. Log of Approved Uses of Personal Health Information for Research

POGO permits the use of personal health information for research purposes and maintains a log of the approved uses that, at a minimum, includes:

- The name of the research study;
- The name of the agent(s) to whom the approval was granted;
- The date of the decision of the REB board approving the written research plan;
- The date that the approval to use personal health information for research purposes was granted by POGO;
- The date that the personal health information was provided to the agent(s);
- The nature of personal health information provided to the agent(s);
- The retention period for the records of personal health information identified in the written research plan approved by the REB;
- Whether the records of personal health information will be securely returned, securely disposed of or de-identified and retained following the retention period; and
- The date the records of personal health information were securely returned; the date, time, location and method of destruction (as per a certificate of destruction); or the date by which they must be returned or disposed of, if applicable; or the date, time and location that de-identification was completed (as per written confirmation).

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

POGO's *Privacy and Data Security Code and its Procedures,* Policy #9.1.1 (*Process for 44 and 45 Projects),* and Policy #9.1.8 (*Disclosure of Personal Health Information for Purposes Other Than Research*) identify whether and in what circumstances personal health information is permitted to be disclosed for purposes other than research (45 analysis purposes).

POGO's *Privacy and Data Security Code and* POGO's *Privacy and Data Security Procedures* articulate a commitment by POGO not to disclose personal health information if other information will serve the same purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose.

POGO requires agents to comply with the *Privacy and Security Policies and Procedures Manual* and also requires that POGO's Privacy Officer enforces compliance and addresses the consequences of any breaches that may occur. Policy #9.1.15 (*Privacy Audits*) stipulates that compliance will be audited and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer who is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

This policy also requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

Where the Disclosure of Personal Health Information is Permitted

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*), and Policy #9.1.8 (*Disclosure of Personal Health Information for Purposes Other Than Research*) permit personal health information to be disclosed for purposes other than research and sets out the circumstances in which the disclosure of personal health information is permitted. The policy further requires that all disclosures of personal health information comply with the Act and its regulation.

Review and Approval Process

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) identify the Privacy Officer, Medical Director, and Chief Executive Officer as responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure of personal health information for purposes other than research and the process that must be followed in this regard. This includes the criteria/documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the Privacy Officer to whom this documentation must be provided; and the required content of the documentation.

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) address the requirements that must be satisfied and the criteria that must be considered by the Privacy Officer, the Medical Director, and Chief Executive Officer in determining whether to approve the request for the disclosure of personal health information for purposes other than research. In identifying the requirements that must be satisfied and the criteria that must be considered, this policy and procedure ensures regard to the *Act* and its regulation.

At a minimum, the Privacy Officer,
Medical Director, and Chief Executive Officer who are responsible for determining whether to approve or deny the request for the disclosure of personal health information for purposes other than research are required to ensure that the disclosure is permitted by the *Act* and its regulation and that any and all conditions or restrictions set out in the *Act* and its regulation have been satisfied. For example, if POGO is requested to disclose personal health information to a health information custodian who provided the personal health information directly or indirectly to POGO, and POGO is relying on Section 18(5) of the regulation under PHIPA, POGO must ensure that the personal health information does not contain any additional identifying information.

POGO's *Privacy and Data Security Code* and POGO's *Privacy and Data Security Procedures* require the , POGO's Senior Adviser, Policy and Clinical Affairs, the Medical Director and Chief Executive Officer who are responsible for determining whether to approve or deny the request are

required to ensure that other information, namely de-identified and/or aggregate information will not serve the identified purpose of the disclosure and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

POGO's *Privacy and Data Security Procedures,* specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) set out the manner in which the decision approving or denying the request for the disclosure of for purposes other than research and the reasons for the decision are documented; the method and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

POGO's *Privacy and Data Security Procedures,* specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for purposes other than research, including any documentation and/or agreements that must be completed, provided, or executed and the agent(s) or other persons or organizations responsible for completing, providing, or executing the documentation and/or agreements. At a minimum, POGO's *Privacy and Security Policies and Procedures Manual,* Section 3 (*Access),* and Policy #9.1.10 *(Execution of Data Sharing Agreements*) requires a Data Sharing Agreement to be executed prior to any disclosure of personal health information for purposes other than research.

POGO's *Privacy and Security Policies and Procedures,* Policy #9.1.10 (*Execution of Data Sharing Agreements*) identify the Privacy Officer *as* responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information have in fact been satisfied, including the execution of a Data Sharing Agreement.

Secure Transfer

POGO's *Privacy and Security Policies and Procedures, and* Policy #9.2.9 (*Secure Transfer of Records of PHI*) require records of personal health information to be transferred in a secure manner.

Secure Return or Disposal

Policy #9.2.6 (*Retention, Return, and Destruction of Data*) identifies the Privacy Officer responsible for ensuring that records of personal health information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement.

This policy further addresses the process that is followed where records of personal health information are not securely returned or a certificate of destruction is not received within a

reasonable period of time following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement. The policy also includes the Privacy Officer as responsible for implementing this process and the stipulated time frame following the retention period or the date of termination within which this process must be implemented.

Documentation Related to Approved Disclosures of Personal Health Information

Policy #9.1.1 (*Process for 44 and 45 Projects*) addresses where documentation related to the receipt, review, approval, or denial of requests for the disclosure of personal health information for purposes other than research is retained and the Privacy Officer who are responsible for retaining this documentation.

Where the Disclosure of Personal Health Information is not Permitted

POGO does not permit personal health information to be disclosed in the circumstance where de-identified and/or aggregate information meet the purposes of the request. POGO's *Privacy and Data Security Code and its Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*), and Policy #9.1.8 (*Disclosure of Personal Health Information for Purposes Other Than Research*) expressly prohibit the disclosure of personal health information for non-research purposes, except where required by law, and if de-identified and/or aggregate information cannot meet the purposes of the request.

Review and Approval Process

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) identify the Privacy Officer, Medical Director, and Chief Executive Officer as responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure of personal health information for purposes other than research and the process that must be followed in this regard. This includes the criteria/documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the Privacy Officer to whom this documentation must be provided; and the required content of the documentation.

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) address the requirements that must be satisfied and the criteria that must be considered by the Privacy Officer, the Medical Director, and Chief Executive Officer in determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for purposes other than research. In identifying the requirements that must be satisfied and the criteria that must be considered, this policy and procedure ensures regard to the *Act* and its regulation.

At a minimum, POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) address the requirement that the de-identified and/or aggregate information be reviewed prior to the disclosure of the de-identified and or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information to identify an individual. The Privacy Officer and Medical Director are responsible for undertaking this review.

POGO's *Privacy and Data Security Procedures,* specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) set out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

POGO's *Privacy and Data Security Procedures,* specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for non-research purposes, including any documentation and/or agreements that must be completed, provided, or executed and the agent(s) or other persons or organizations responsible for completing, providing, or executing the documentation and/or agreements.

At a minimum, POGO requires 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. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. Therefore, POGO's *Privacy and Security Policies and Procedures Manual,* Section 3 (*Access),* and Policy #9.1.10 *(Execution of Data Sharing Agreements*) requires a Data Sharing Agreement to be executed prior to any disclosure of de-identified and/or aggregate information for purposes other than research.

POGO's *Privacy and Security Policies and Procedures,* Policy #9.1.10 (*Execution of Data Sharing Agreements*) identify the Privacy Officer *as* responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of a Data Sharing Agreement. Further, POGO's *Privacy and Security Policies and Procedures,* Policy #9.1.10 (*Execution of Data Sharing Agreements*) shall require the Privacy Officer to track receipt of the executed written acknowledgments and shall set out the procedure that must be followed and POGO's *Privacy and Security Policies and Procedures,* Policy #9.1.10 (*Execution of Data Sharing Agreements*) must be followed and must be maintained in this regard.

13. Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (Process for 44 and 45 *Projects*), and Policy #9.1.9 (*Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*) identify when, and under what circumstances, personal health information is permitted to be disclosed for research purposes (44 purposes).

POGO's *Privacy and Data Security Code* and POGO's *Privacy and Data Security Procedures* articulate a commitment by POGO not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose.

POGO requires agents to comply with the POGO's *Privacy and Data Security Procedures* and that POGO's Privacy Officer enforces compliance and address the consequences of any breach. Policy #9.1.15 (*Privacy Audits*) stipulates that compliance will be audited and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as those responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

This policy also requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

Where the Disclosure of Personal Health Information is Permitted for Research

POGO's *Privacy and Data Security Procedures*, Policy #9.1.1 (*Process for 44 and 45 Projects*) and Policy #9.1.9 (*Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*) permits personal health information to be disclosed for purposes of research and sets out the circumstances in which the disclosure of personal health information is permitted. They further require that all disclosures of personal health information comply with the *Act* and its regulation.

Review and Approval Process

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) and Policy #9.1.9 (*Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*) *identify* the Privacy Officer and Medical Director as those responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure of personal health information for research purposes and the process that must be followed in this regard. This includes the criteria/documentation that must be completed, provided, and/or executed; the agent(s) or other persons or organizations responsible for completing, providing, and/or executing the documentation; the Privacy Officers to whom this documentation must be provided; and the required content of the documentation.

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) address the requirements that must be satisfied and the criteria that must be considered by the Privacy Officer and Medical Director in determining whether to approve the request for the disclosure of personal health information for research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, this policy and procedure ensures regard to the *Act* and its regulation.

At a minimum, the Privacy Officer,
and Medical Director who are responsible for determining whether to approve or deny the request for the disclosure of personal health information for research purposes must be in receipt of a written application, a written research plan, and a copy of the decision of the REB approving the written research plan. The written research plan must also comply with the requirements in the *Act* and its regulation.

In addition, POGO's Privacy Program states that prior to any approval of the disclosure of personal health information for research purposes, the Privacy Officer and Medical Director who are responsible for determining whether to approve or deny the request are required to ensure that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the REB. The Privacy Officer and Medical Director ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.

POGO's *Privacy and Data Security Procedures*, specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) sets out the manner in which the decision approving or denying the request for the disclosure of personal health information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

POGO's *Privacy and Data Security Procedure,* specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for research purposes, including any documentation and/or agreements that must be completed, provided or executed, and the Privacy Officer or researcher responsible for completing, providing or executing the documentation and/or agreements.

At a minimum, POGO's *Privacy and Data Security Code, and* POGO's *Privacy and Data Security Procedures*, Principle 1 (*Accountability*), require a Researcher Agreement to be executed in accordance with the Template Research Agreement in POGO's Manual *Section 3.3 (Research Agreement Between POGO and Researcher(s))* prior to any disclosure of personal health information for research purposes.

POGO's *Privacy and Data Security Code, and* POGO's *Privacy and Data Security Procedures* identify the Privacy Officer is responsible for ensuring that any conditions or restrictions that must

be satisfied prior to the disclosure of personal health information have in fact been satisfied, including the execution of a Researcher Agreement.

Secure Transfer

POGO's *Privacy and Security Policies and Procedures Manual,* Policy #9.2.9 (*Secure Transfer of Records of PHI*) requires records of personal health information to be transferred in a secure manner.

Secure Return or Disposal

Policy #9.2.6 (*Retention, Return, and Destruction of Data*) identifies the Privacy Officer who is responsible for ensuring that records of personal health information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of or de-identified, as the case may be, following the retention period set out in the Researcher Agreement.

This policy further addresses the process that is followed where records of personal health information are not securely returned or a certificate of destruction is not received or written confirmation of de-identification is not received within the time set out in the Researcher Agreement.

Documentation Related to Approved Disclosures of Personal Health Information for Research

Policy #9.1.1 (*Process for 44 and 45 Projects*) and Policy #9.1.9 *(Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*) addresses where documentation related to the receipt, review, approval or denial of requests of personal health information, copies of the decisions of REB, Research Agreements, certificates of destruction and other and other documentation related to for the disclosure of personal health information for research purposes is retained, and the Privacy Officer who is responsible for retaining this documentation.

Where the Disclosure of Personal Health Information is not Permitted for Research

POGO permits personal health information to be used for research purposes as outlined in POGO's *Privacy and Data Security Procedures* which sets out the circumstances in which personal health information is permitted to be used for research purposes.

As per POGO's *Privacy and Data Security Procedures*, POGO prohibits the use of PHI for research purposes when the REB rules accordingly, and indicates that de-identified and/or aggregate information may be used if REB rules accordingly.

Review and Approval Process

POGO permits de-identified and/or aggregate data to be disclosed for research purposes. POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) identify the Privacy Officer and Medical Director as those responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information for research purposes and the process that must be followed in this regard. This includes a discussion of the documentation that must be completed, provided and/or executed by agents of POGO or prescribed entity or by a researcher; the Privacy Officer to whom this documentation must be provided; and the required content of the documentation.

For example, POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) address whether the prescribed person or prescribed entity requires the preparation of a written research plan in accordance with the Act and its regulation and/or required REB approval of the written research plan prior to the disclosure of de-identified and/or aggregate information for research purposes.

The policy and procedures also address the requirements that must be satisfied and the criteria that must be considered by the Privacy Officer and Medical Director responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for research purposes. At a minimum, POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) and Policy #9.1.9 *(Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*) require the de-identified and/or aggregate information to be reviewed prior to the approval and disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The Privacy Officer and Medical Director are responsible for undertaking this review.

POGO's *Privacy and Data Security Procedures*, specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) sets out the manner in which the decision approving or denying the request for the disclosure of personal health information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

POGO's Privacy and Data Security Procedure, specifically Principle 5 (Limiting Use, Disclosure and Retention of Personal Health Information) identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for research purposes, including any documentation and/or agreements that must be completed,

provided or executed, and the Privacy Officer as responsible for completing, providing or executing the documentation and/or agreements.

At a minimum, POGO's Privacy Officer requires the researcher to whom the de-identified and/or aggregate information will be disclosed to 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. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

POGO's *Privacy and Data Security Code*, *and* POGO's *Privacy and Data Security Procedures* identify the Privacy Officer as responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of de-identified and/or aggregate information have been satisfied, including the execution of a written acknowledgment. Further, the policy and procedures require the Privacy Officer to track receipt of the executed written acknowledgements and set out the procedures that must be followed and the documentation that must be maintained in this regard.

14. Template Research Agreement

A Researcher Agreement as per the template in POGO's Manual *Section 3.3 (Research Agreement Between POGO and Researcher(s))* is executed with the researchers to whom personal health information will be disclosed prior to the disclosure of the personal health information for research purposes. At a minimum, the Researcher Agreement must address the matters set out below.

General Provisions

The Researcher Agreement describes the status of POGO under the *Act* and the duties and responsibilities arising from this status. The Researcher Agreement also outlines the precise nature of the personal health information that will be disclosed by POGO for research purposes and provides a definition of personal health information that is consistent with the *Act* and its regulation.

Purposes of Collection, Use and Disclosure

The research purpose for which personal health information is being disclosed by POGO and the purposes for which the personal health information may be used or disclosed by the researcher are identified in the Researcher Agreement, as well as the statutory authority for each collection, use, and disclosure identified.

In particular, the Researcher Agreement clearly sets out that the researcher may only use the personal health information for the purposes set out in the written research plan approved by the REB and prohibits the use of the personal health information for any other purpose. The Researcher

Agreement also prohibits the researcher from permitting persons to access and use the personal health information except those persons described in the written research plan approved by the REB.

As outlined in the purposes for which the personal health information may be used, the Researcher Agreement explicitly states whether or not the personal health information may be linked to other information and prohibits the personal health information from being linked except in accordance with the written research plan approved by the REB.

The Researcher Agreement requires the researcher to acknowledge that the personal health information that is being disclosed pursuant to the Researcher Agreement is necessary for the identified research purpose and that other information, namely de-identified and/or aggregate information, will not serve the research purpose. The researcher is also required to acknowledge that no more personal health information is being collected and will be used than is reasonably necessary to meet the research purpose.

The Researcher Agreement also imposes restrictions on the disclosure of personal health information. At a minimum, the Researcher Agreement requires the researcher to acknowledge and agree not to disclose the personal health information except as required by law and subject to the exceptions and additional requirements prescribed in the regulation to the *Act*; not to publish the personal health information in a form that could reasonably enable a person to ascertain the identity of the individual; and not to make contact or attempt to make contact with the individual to whom the personal health information relates, directly or indirectly, unless the consent of the individual to being contacted is first obtained in accordance with subsection 44(6) of the *Act*.

Compliance with the Statutory Requirements for the Disclosure for Research Purposes

The Researcher Agreement requires the researcher and POGO to acknowledge and agree that the researcher has submitted an application in writing, a written research plan that meets the requirements of the *Act* and its regulation, and a copy of the decision of the REB approving the written research plan.

The researcher is also required to acknowledge and agree that they will comply with the Researcher Agreement, with the written research plan approved by the REB and with the conditions, if any, specified by the REB in respect of the written research plan.

Secure Transfer

The Researcher Agreement requires the secure transfer of records of personal health information that will be disclosed pursuant to the Researcher Agreement. The Researcher Agreement sets out the secure manner in which records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that will be followed in ensuring that the records of personal health information are transferred in a secure manner. In identifying the secure manner in which the records of personal health information will

be transferred, the Researcher Agreement has regard to Policy #9.2.9 (*Secure Transfer of Records of Personal Health Information*) implemented by POGO.

Secure Retention

The retention period for the records of personal health information, subject to the Researcher Agreement and Privacy Impact Assessment, identify the length of time that the records of personal health information will be retained in identifiable form. The retention period identified is also consistent with that set out in the written research plan approved by the REB.

The Researcher Agreement requires the researcher to ensure that the records of personal health information are retained in a secure manner and shall identify the precise manner in which the records of personal health information in paper and electronic format will be securely retained. In identifying the secure manner in which the records of personal health information will be retained, the Researcher Agreement has regard to the Policy #9.2.9 (*Secure Retention of Records of Personal Health Information*) and to the written research plan approved by the REB.

The Researcher Agreement also requires the researcher to take steps that are reasonable in the circumstances to ensure that the personal health information subject to the Researcher Agreement is protected against theft, loss, and unauthorized use or disclosure and to ensure that the records of personal health information subject to the Researcher Agreement are protected against unauthorized copying, modification, or disposal. The reasonable steps that are required to be taken by the researcher are detailed in the Researcher Agreement and, at a minimum, include those set out in the written research plan approved by the REB.

Secure Return or Disposal

The Researcher Agreement also addresses whether the records of personal health information subject to the Researcher Agreement will be returned in a secure manner, will be disposed of in a secure manner, or will be de-identified and retained by the researcher following the retention period set out in the Researcher Agreement. In this regard, the provisions in the Researcher Agreement will be consistent with the written research plan approved by the REB.

If the records of personal health information are required to be returned in a secure manner, the Researcher Agreement stipulates the time frame following the retention period within which the records must be securely returned, and the secure manner in which the records must be returned to the POGO Privacy Officer.

In identifying the secure manner in which the records of personal health information will be returned, regard will be had to Policy #9.2.6 (*Retention, Return, and Destruction of Data*) implemented by POGO.

If the records of personal health information are required to be disposed of in a secure manner, the Researcher Agreement provides a definition of secure disposal that is consistent with the *Act* and its regulation and identifies the precise manner in which the records of personal health information

subject to the Researcher Agreement must be securely disposed of. The Researcher Agreement also stipulates the time frame following the retention period set out in the Researcher Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.

In identifying the secure manner in which the records of personal health information will be disposed of, POGO ensures that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets, and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including Fact Sheet 10 (*Secure Destruction of Personal Information*). In addition, consideration is given to Policy #9.2.6 (*Retention, Return, and Destruction of Data*) implemented by POGO.

Further, the Researcher Agreement identifies the Privacy Officer to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided, and the required content of the certificate of destruction. At a minimum, the certificate of destruction identifies the records of personal health information being securely disposed of; the date, time, location, and method of secure disposal employed; and the name and signature of the person who performed the secure disposal.

If the records of personal health information are required to be de-identified and retained by the researcher rather than being securely returned or disposed of, the manner and process for de-identification is set out in the Researcher Agreement. In identifying the manner and process for de-identification, consideration must be given to Policy #9.1.13 (*De-Identifying Personal Health Information*) implemented by POGO. The Researcher Agreement also requires that the researcher submit written confirmation that the records were de-identified, and specifies the time frame following the retention period set out in the Researcher Agreement within which the written confirmation must be provided and the POGO Privacy Officer to whom the written confirmation must be provided.

Notification

At a minimum, the Researcher Agreement requires the researcher to notify the Privacy Officer, in writing, if the researcher becomes aware of a breach or suspected breach of the Researcher Agreement, a breach or suspected breach of subsection 44(6) of the *Act*, or if personal health information subject to the Researcher Agreement is stolen, lost, or accessed by unauthorized persons or is believed to have been stolen, lost, or accessed by unauthorized persons. The Researcher Agreement also identifies the Privacy Officer to whom notification must be provided, and requires the researcher to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss, or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance

The Researcher Agreement outlines the consequences of breach of the agreement and indicates that compliance with the Researcher Agreement will be audited by POGO, and if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.

The Researcher Agreement requires the researcher to ensure that all persons who will have access to the personal health information, as identified in the written research plan approved by the REB, are aware of and agree to comply with the terms and conditions of the Researcher Agreement prior to being given access to the personal health information. The Researcher Agreement sets out the method by which this will be ensured by the researcher, for example, requiring the persons identified in the written research plan to sign an acknowledgement prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Researcher Agreement.

15. Log of Research Agreements

POGO maintains a log of executed Researcher Agreements. At a minimum, the log includes:

- The name of the research study;
- The name of the principal researcher to whom the personal health information was disclosed pursuant to the Research Agreement;
- The date(s) of receipt of the written application, the written research plan and the written decision of the REB approving the research plan;
- The date that the approval to disclose the personal health information for research purposes was granted by POGO;
- The date that the Researcher Agreement was executed;
- The date that the personal health information was disclosed;
- The nature of the personal health information disclosed;
- The retention period for the records of personal health information as set out in the Researcher Agreement;
- Whether the records of personal health information will be securely returned, securely disposed of or de-identified and retained by the researcher following the retention period set out in the Research Agreement; and
- The date that the records of personal health information were securely returned, a certificate of destruction was received or written confirmation of de-identification was received, or the date by which they must be returned, disposed of or de-identified.

16. Policy and Procedures for the Execution of Data Sharing Agreements

Policy #9.1.10 (*Execution of Data Sharing Agreements*) identifies the circumstances requiring the execution of a Data Sharing Agreement, the process that must be followed, and the requirements

that must be satisfied prior to the execution of a Data Sharing Agreement.

This policy and procedure sets out the circumstances requiring the execution of a Data Sharing Agreement prior to the collection of personal health information for purposes other than research and requires the execution of a Data Sharing Agreement prior to any disclosure of personal health information for purposes other than research.

The policy and procedure further identifies the Privacy Officer as responsible for ensuring that a Data Sharing Agreement is executed, the process that must be followed, and the requirements that must be satisfied in this regard. These requirements include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the Privacy Officer to whom the documentation must be provided; and the required content of the documentation.

In relation to the disclosure of personal health information for purposes other than research, the Privacy Officer who is responsible for ensuring that a Data Sharing Agreement is executed, must be satisfied that the disclosure was approved in accordance with POGO's *Privacy and Data Security Procedures*, specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*). In relation to the collection of personal health information for purposes other than research, the Privacy Officer are also responsible for ensuring that a Data Sharing Agreement is executed and must also be satisfied that the collection was approved in accordance with Principle 4 (*Limiting Collection)*.

Policy #9.1.10 (*Execution of Data Sharing Agreements*) also sets out that a log of Data Sharing Agreements be maintained and identifies the Privacy Team as responsible for maintaining such a log. In addition, this policy also specifies POGO's secured central files as the location where documentation related to the execution of Data Sharing Agreements will be saved, and the Privacy Offices who are responsible for retention.

POGO's Privacy Officer ensures that agents understand they must comply with the policy and its procedure and that they will enforce compliance and the consequences of breach.

All agents of POGO must understand that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*) on an annual basis or as required, and that the Privacy Officer will be responsible for conducting the audit.

POGO's policies also require agents to notify the Privacy Officer at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

17. Template Data Sharing Agreement

POGO ensures that a Data Sharing Agreement is executed in the circumstances set out in Policy #9.1.10 (*Execution of Data Sharing Agreements*) that, at a minimum, addresses the matters set out below.

General Provisions

POGO's Data Sharing Agreements describe the status of POGO under the *Act* and the duties and responsibilities arising from this status. It also specifies the precise nature of the personal health information subject to the Data Sharing Agreement and provides a definition of personal health information that is consistent with the *Act* and its regulation. The Data Sharing Agreement also identifies the person or organization that is collecting personal health information and the person or organization that is disclosing personal health information pursuant to the Data Sharing Agreement.

Purposes of Collection, Use and Disclosure

The Data Sharing Agreement also identifies the purposes for which the personal health information subject to the Data Sharing Agreement is being collected and for which the personal health information will be used.

In identifying these purposes, the Data Sharing Agreement explicitly states whether or not the personal health information collected pursuant to the Data Sharing Agreement will be linked to other information. If the personal health information is to be linked to other information, the Data Sharing Agreement identifies the nature of the information to which the personal health information will be linked, the source of the information to which the personal health information will be linked, how the linkage will be conducted, and why the linkage is required for the identified purposes.

The Data Sharing Agreement also contains an acknowledgement that the personal health information collected pursuant to the Data Sharing Agreement is necessary for the purpose for which it was collected and that other information, namely de-identified and/or aggregate information, will not serve the purpose and that no more personal health information is being collected and will be used than is reasonably necessary to meet the purpose.

The Data Sharing Agreement also identifies the purposes, if any, for which the personal health information subject to the Data Sharing Agreement may be disclosed and any limitations, conditions or restrictions imposed thereon.

The Data Sharing Agreement also requires the collection, use, and disclosure of personal health information subject to the Data Sharing Agreement to comply with the *Act* and its regulation and must set out the specific statutory authority for each collection, use, and disclosure contemplated in the Data Sharing Agreement.

Secure Transfer

The Data Sharing Agreement requires the secure transfer of the records of personal health information subject to the Data Sharing Agreement. The Data Sharing Agreement sets out the secure manner in which the records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that must be followed in ensuring that the records are transferred in a secure manner. In identifying the secure

manner in which the records of personal health information will be transferred, regard is given to Policy #9.2.9 (*Secure Transfer of Records of Personal Health*) implemented by POGO.

Secure Retention

The retention period for the records of personal health information subject to the Data Sharing Agreement is also specified in the Data Sharing Agreement. In identifying the relevant retention period, the Privacy Officer ensures that the records of personal health information are retained only for as long as necessary to fulfill the purposes for which the records of personal health information were collected.

The Data Sharing Agreement also requires the records of personal health information to be retained in a secure manner and identifies the precise manner in which the records of personal health information in paper and electronic format will be securely retained, including whether the records will be retained in identifiable form. In identifying the secure manner in which the records of personal health information will be retained, the Data Sharing Agreement has regard to Policy #9.2.6 (*Retention, Return, and Destruction*) implemented by POGO.

The Data Sharing Agreement also requires reasonable steps to be taken to ensure that the personal health information subject to the Data Sharing Agreement is protected against theft, loss, and unauthorized use or disclosure, and to ensure that the records of personal health information are protected against unauthorized copying, modification, or disposal. The reasonable steps that are required to be taken are also detailed in the Data Sharing Agreement.

Secure Return or Disposal

The Data Sharing Agreement addresses whether the records of personal health information subject to the Data Sharing Agreement will be returned in a secure manner or will be disposed of in a secure manner following the retention period set out in the Data Sharing Agreement or following the date of termination of the Data Sharing Agreement, as the case may be.

If the records of personal health information are required to be returned in a secure manner, the Data Sharing Agreement stipulates the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of personal health information must be securely returned, the secure manner in which the records must be returned, and the Privacy Officer to whom the records must be securely returned. In identifying the secure manner in which the records of personal health information will be returned, regard is given to Policy #9.2.9 (*Secure Transfer of Records of Personal Health Information*) implemented by POGO.

If the records of personal health information are required to be disposed of in a secure manner, the Data Sharing Agreement provides a definition of secure disposal that is consistent with the *Act* and its regulation, and identifies the precise manner in which the records of personal health information subject to the Data Sharing Agreement must be securely disposed of. The Data Sharing Agreement also sets out the time frame following the retention period or following the date of termination of

the Data Sharing Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.

In identifying the secure manner in which the records of personal health information will be disposed of, the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets, and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10* (*Secure Destruction of Personal Information*). In addition, regard is given to Policy #9.2.6 (*Retention, Return, and Destruction of Data*) implemented by POGO.

Further, the Data Sharing Agreement sets out that the certificate of destruction must be provided to the Privacy Officer, the time frame following secure disposal within which the certificate of destruction must be provided, and the required content of the certificate of destruction. At a minimum, the certificate of destruction must identify the records of personal health information being securely disposed of; the date, time, location, and method of secure disposal employed; and the name and signature of the person who performed the secure disposal.

Notification

At a minimum, the Data Sharing Agreement requires that notification be provided at the first reasonable opportunity if the Data Sharing Agreement has been breached or is suspected to have been breached or if the personal health information subject to the Data Sharing Agreement is stolen, lost, or accessed by unauthorized persons or is believed to have been stolen, lost, or accessed by unauthorized persons. It also identifies the notification will be verbal and written and that the notification must be provided to the Privacy Officer. The Data Sharing Agreement also requires that reasonable steps be taken to contain the breach of the Data Sharing Agreement and to contain the theft, loss, or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance

The Data Sharing Agreement Template outlines the consequences of breach of the agreement and indicates that compliance with the Data Sharing Agreement will be audited, and the manner in which compliance will be audited and the notice that will be provided of the audit.

The Data Sharing Agreement also requires that all persons who will have access to the personal health information are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement prior to being given access to the personal health information. The Data Sharing Agreement sets out the method by which this will be ensured. This includes requiring the persons that will have access to the personal health information to sign a Confidentiality Agreement prior to being granted access, indicating that they are aware of, and agree to comply with the terms and conditions of the Data Sharing Agreement.

18. Log of Data Sharing Agreements

POGO maintains a log of executed Data Sharing Agreements. The log includes:

- The name of the person or organization from whom the personal health information was collected or to whom the personal health information was disclosed;
- The date that the collection or disclosure of personal health information was approved, as the case may be;
- The date that the Data Sharing Agreement was executed;
- The date the personal health information was collected or disclosed, as the case may be;
- The nature of the personal health information subject to the Data Sharing Agreement;
- The retention period for the records of personal health information set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement;
- Whether the records of personal health information will be securely returned or will be securely disposed of following the retention period set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement; and
- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date by which they must be returned or disposed of.

19. Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information

Policy #9.1.11 (*Template for Agreement with Third Party Service Providers*) requires written agreements to be entered into with third party service providers prior to permitting third party service providers to access and use POGO personal health information. The policy requires the written agreements to contain the relevant language from the policy.

The policy also identifies the Privacy Officer who is responsible for ensuring that an agreement is executed, the process that must be followed, and the requirements that must be satisfied prior to the execution of such an agreement.

The policy and procedure also states that POGO will not provide personal health information to a third party service provider if other information, namely de-identified and/or aggregate information, will serve the same purpose and will not provide more personal health information than is reasonably necessary to meet the purpose.

The Privacy Officer is identified in the policy as the agent responsible for making this determination and ensuring that records of personal health information provided to a third party service provider are either securely returned to POGO or are securely disposed of, as the case may be, following the termination of the agreement.

The policy also sets out the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received following the termination of

the agreement, and that the Privacy Officer is responsible for implementing this process and the time frame following termination within which this process must be implemented.

The policy and procedures also require that a log be maintained of all agreements executed with third party service providers and identifies the Privacy Team who are the agents responsible for maintaining such a log. In addition, the policy and procedures state that documentation related to the execution of agreements with third party service providers will be retained in POGO's secured central files by the Privacy Officer.

POGO requires third party service providers to comply with specific policies and procedures as outlined in each Third Party Service Agreement and set out how the Privacy Officer enforce compliance and the consequences of breach. Compliance will be audited in accordance with principles within Policy #9.1.15 (*Privacy Audits*) specific to Third Parties and will be audited by the Privacy Officer annually to ensure compliance with the policy and its procedures.

The policy and procedures also require Third Parties to notify the Privacy Officer at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) if a third party service provider breaches or believes there may have been a breach of specific procedures and/or terms as set out in the agreement.

20. Template Agreement for All Third Party Service Providers

A written agreement must be entered into with third party service providers that will be permitted to access and use personal health information of POGO, including those that are contracted to retain, transfer or dispose of records of personal health information and those that are contracted to provide services for the purpose of enabling POGO to use electronic means to collect, use, modify, disclose, retain, or dispose of personal health information ("electronic service providers"). The written agreement addresses the matters set out below.

General Provisions

The agreement describes the status of POGO under the *Act* and the duties and responsibilities arising from this status. The agreement also states whether or not the third party service provider is an agent of POGO in providing services pursuant to the agreement.

POGO engages with very few third party service providers. It has only one that is permitted to access and use personal health information in the course of providing services to POGO and that is an electronic service provider, which is considered to be a POGO Third Party Agent.
Agreements with the electronic service provider state whether or not the third party service provider is an agent of POGO in providing services pursuant to the agreement.

POGO also engages with a third party service provider who is contracted to dispose of records of personal health information and is not an agent of POGO. The process of disposal does not allow the provider to access or use the personal health information. Under the supervision of POGO the

provider carries locked containers to the shredding vehicle. The PHI is not viewed or handled by the provider.

POGO may also engage, from time to time, third party service providers whose primary purpose is to perform forensic audits on POGO's books and records and where the scope of that audit may involve access and retention of POGO's PHI by the forensic auditor for the limited duration of the audit. This third party service provider may also assist in the secure disposal of records of personal health information at the completion of the audit.

When the third party service provider is an agent of POGO, the agreement requires the third party service provider to comply with the provisions of the *Act* and its regulation relating to prescribed persons or prescribed entities, as the case may be, and to comply with specific privacy and security policies and procedures implemented by POGO in providing services pursuant to the agreement.

The agreement provides a definition of personal health information consistent with the *Act* and its regulation. Where appropriate, the agreement also specifies the precise nature of the personal health information that the third party service provider will be permitted to access and use in the course of providing services pursuant to the agreement.

The agreement also sets out that the services provided by the third party service provider pursuant to the agreement be performed in a professional manner, in accordance with industry standards and practices, and by properly trained agents of the third party service provider.

Obligations with Respect to Access and Use

The agreement identifies the purposes for which the third party service provider is permitted to access and use the personal health information of POGO and any limitations, conditions, or restrictions imposed thereon.

In identifying the purposes for which the third party service provider is permitted to use personal health information, POGO ensures that each use identified in the agreement is consistent with the uses of personal health information permitted by the *Act* and its regulation. The agreement prohibits the third party service provider from using personal health information except as permitted in the agreement.

In the case of an electronic service provider that is not an agent of POGO, the agreement sets out that the electronic service provider is prohibited from using personal health information except as necessary in the course of providing services pursuant to the agreement.

Further, the agreement prohibits the third party service provider from using personal health information if other information will serve the purpose and from using more personal health information than is reasonably necessary to meet the purpose.

Obligations with Respect to Disclosure

This section is not applicable. POGO does not permit third party service providers to disclose personal health information of POGO.

The agreement prohibits the third party service provider and the electronic service provider to disclose the personal health information of POGO to which it has access in the course of providing services, except as required by law.

Secure Transfer

Where it is necessary to transfer records of personal health information to or from POGO to perform forensic audits, the agreement requires the third party service provider to securely transfer the records of personal health information and sets out the responsibilities of the third party service provider in this regard. In particular, the agreement specifies the secure manner in which the records will be transferred by the third party service provider, the conditions pursuant to which the records will be transferred by the third party service provider, to whom the records will be transferred, and the procedure that must be followed by the third party service provider in ensuring that the records are transferred in a secure manner.

In identifying the secure manner in which records of personal health information must be transferred, the agreement shall have regard to Policy #9.2.9 (*Secure Transfer of Records of Personal Health Information*) implemented by POGO.

In addition, where the retention of records of personal health information is required for the scope and duration of a forensic audit or where the disposal of records of personal health information outside the premises of POGO is the primary service provided to POGO, the agreement requires the third party service provider to provide documentation to POGO setting out the date, time, and mode of transfer of the records of personal health information and confirming receipt of the records of personal health information by the third party service provider. In these circumstances, the agreement obligates the third party service provider to maintain a detailed inventory of the records of personal health information transferred.

Secure Retention

The agreement requires the third party service provider to retain the records of personal health information, where applicable, in a secure manner and shall identify the precise methods by which records of personal health information in paper and electronic format will be securely retained by the third party service provider for the duration of the forensic audit, including records of personal health information retained on various media.

The agreement further outlines the responsibilities of the third party service provider in securely retaining the records of personal health information. In identifying the secure manner in which the records of personal health information will be retained, and the methods by which the records of

personal health information will be securely retained, the agreement shall have regard to Policy #9.2.6 (*Retention, Return, and Destruction of Data*) implemented by POGO.

Secure Return or Disposal Following Termination of the Agreement

The agreement sets out, where applicable, whether records of personal health information will be securely returned to POGO or will be disposed of in a secure manner following the termination of the agreement.

If the records of personal health information are required to be returned in a secure manner, the agreement stipulates the time frame following the date of termination of the agreement within which the records of personal health information must be securely returned, the secure manner in which the records are to be returned, and the agent of POGO to whom the records must be securely returned. In identifying the secure manner in which the records of personal health information will be returned, the agreement will have regard to Policy #9.2.9 (*Secure Transfer of Records of Personal Health Information*) implemented by POGO.

If the records of personal health information are required to be disposed of in a secure manner, the agreement provides a definition of secure disposal that is consistent with the *Act* and its regulation and identifies the precise manner in which the records of personal health information are to be securely disposed.

In identifying the secure manner in which the records of personal health information will be disposed of, the requirements of the agreement ensure that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; with guidelines, fact sheets, and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10* (*Secure Destruction of Personal Information*); and with POGO Policy #9.2.6 (*Retention, Return, and Destruction of Data*) implemented by POGO.

The agreement also stipulates the time frame following termination of the agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided to POGO. The agreement further identifies the agent of POGO to whom the certificate of destruction must be provided and set out the required content of the certificate of destruction. At a minimum, the certificate of destruction must be required to identify the records of personal health information securely disposed of; to stipulate the date, time, and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

Secure Disposal as a Contracted Service

Where the disposal of records of personal health information is the primary service provided to POGO, in addition to the requirements set out above in relation to secure disposal, the agreement sets out the responsibilities of the third party service provider in securely disposing of the records of personal health information, including:

- The time frame within which the records are required to be securely disposed of;
- The precise method by which records in paper and/or electronic format must be securely disposed of, including records retained on various media;
- The conditions pursuant to which the records will be securely disposed of; and
- The Privacy Team who is responsible for ensuring the secure disposal of the records.

The agreement also enables POGO at its discretion to witness the secure disposal of the records of personal health information subject to such reasonable terms or conditions as may be required in the circumstances.

Implementation of Safeguards

The agreement requires the third party service provider to take steps that are reasonable in the circumstances to ensure that the personal health information accessed and used in the course of providing services pursuant to the agreement is protected against theft, transmission, loss, and unauthorized use or disclosure and to ensure that the records of personal health information subject to the agreement are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be implemented by the third party service provider are detailed in the agreement.

Training of Agents of the Third Party Service Provider

The agreement requires the third party service provider to provide training to its agents on the importance of protecting the privacy of individuals whose personal health information is accessed and used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations.

The agreement requires the third party service provider to ensure that its agents who will have access to the records of personal health information are aware of, and agree to comply with the terms and conditions of the agreement prior to being given access to the personal health information. The agreement sets out the method by which this will be assured. This may include requiring agents to sign a confidentiality agreement prior to being granted access to the personal health information, indicating that they are aware of, and agree to comply with the terms and conditions of the agreement.

Subcontracting of the Services

POGO does not permit the third party service provider to subcontract the services provided under the agreement.

Notification

At a minimum, the agreement requires the third party service provider to notify the POGO Privacy Officer at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if personal health information handled by the third party service provider on behalf of POGO's Privacy Officer is stolen, lost, or accessed by unauthorized persons or is believed to have been stolen, lost, or accessed by unauthorized persons. The agreement identifies the notification must be verbal and followed by written notification. The third party service provider is also required to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance

The agreement outlines the consequences of breach of the agreement and sets out that POGO will audit compliance with the agreement, sets out the manner in which compliance will be audited, and the notice, if any, that will be provided to the third party service provider of the audit.

21. Log of Agreements with Third Party Service Providers

POGO maintains a log of executed agreements with third party service providers. The log includes:

- The name of the third party service provider;
- The nature of the services provided by the third party service provider that require access to and use and secure destruction of personal health information;
- The date that the agreement with the third party service provider was executed;
- The date that the records of personal health information or access to the records of personal health information, if any, was provided;
- The nature of the personal health information provided or to which access was provided.
- If applicable, the date of termination of the agreement with the third party service provider;
- Whether the records of personal health information, if any, will be securely returned or will be securely disposed of following the date of termination of the agreement; and
- The date, time and location the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to personal health information was terminated or the date the records of personal health information were securely disposed of with the applicable certificate of destruction provided to the Privacy Team.

22. Policy and Procedures for the Linkage of Records of Personal Health Information

POGO's *Privacy and Security Policies and Procedures* and Policy #9.2.18 (*Confidentiality and Security of Data*) address linkages of records of personal health information.

These policies and procedures indicate that POGO permits the linkage of records of personal health information, and the purposes for which, and the circumstances in which such linkages are permitted.

In identifying the purposes for which, and the circumstances in which the linkage of records of personal health information is permitted, the policies and procedures have regard to the sources of the records of personal health information that are requested to be linked, and the identity of the person or organization that will ultimately make use of the linked records of personal health information, including:

- The linkage of records of personal health information solely in the custody of POGO for the exclusive use of the linked records of personal health information by POGO;
- The linkage of records of personal health information in the custody of POGO with records of personal health information to be collected from another prescribed entity or organization for the exclusive use of the linked records of personal health information by POGO;
- The linkage of records of personal health information solely in the custody of POGO for purposes of disclosure of the linked records of personal health information to another prescribed entity or organization; and
- The linkage of records of personal health information in the custody of POGO with records of personal health information to be collected from another prescribed entity or organization for purposes of disclosure of the linked records of personal health information to that other prescribed entity or organization.

Review and Approval Process

The policy and procedures identify the Senior Database Administrator and the Medical Director as those responsible for receiving, reviewing, and determining whether to approve or deny the request to link records of personal health information and the process that must be followed in this regard. This process includes a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the Senior Database Administrator to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also address the requirements that must be satisfied and the criteria that must be considered by the Senior Database Administrator and the Medical Director who are responsible for determining whether to approve or deny the request to link records of personal health information.

The policy and procedures also set out the manner in which the decision approving or denying the request to link records of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

Where the linked records of personal health information will be disclosed by POGO to another person or organization, e.g. 45 entities or researcher, the policy and procedures require that the disclosure be approved pursuant to Policy #9.1.1 (*Process for 44 and 45 Projects*), and Policy #9.1.10 (*Execution of Data Sharing Agreements*).

Where the linked records of personal health information will be used by POGO, the policy and procedures require that the use be approved pursuant to the Policy #9.1.1 (*Process for 44 and 45 Projects*) or POGO's *Privacy and Data Security Procedures,* Principle 5 (*Limiting Use, Disclosure and Retention*), as may be applicable. The policy and procedures further require that the linked records of personal health information be de-identified and/or aggregated as soon as practicable pursuant to the Policy #9.1.13 *(De-Identifying Personal Health Information*) and that, to the extent possible, only de-identified and/or aggregate information be used by agents of POGO.

Process for the Linkage of Records of Personal Health Information

The policy and procedures outline the process to be followed in linking records of personal health information, the manner in which the linkage of records of personal health information must be conducted, and the IT Team who are responsible for linking records of personal health information when approved in accordance with this policy and its procedures.

Retention

The policy and procedures require that linked records of personal health information be retained in compliance with the Policy #9.2.6 (*Retention, Return, and Destruction of Data*) until they are de-identified and/or aggregated pursuant to the Policy #9.1.13 (*De-Identifying Personal Health Information*).

Secure Disposal

The policy and procedures address the secure disposal of records of personal health information linked by POGO and, in particular, require that the records of personal health information be securely disposed of in compliance with the Policy #9.2.6 (*Retention, Return, and Destruction of Data*).

Compliance, Audit and Enforcement

POGO requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

Tracking Approved Linkages of Records of Personal Health Information

POGO maintains a log of the linkages of records of personal health information approved by POGO, and identifies the Privacy Team as the agents responsible for maintaining such a log, and filing this log on POGO's secured central filing system. The files contain information related to the receipt, review, approval, or denial of requests to link records of personal health information.

23. Log of Approved Linkages of Records of Personal Health Information

POGO maintains a log of all linkages of records of personal health information approved by POGO. At a minimum, the log includes the name of the agent, person, or organization who requested the linkage, the date that the linkage of records of personal health information was approved, and the nature of the records of personal health information linked.

24. Policy and Procedures with Respect to De-Identification and Aggregation

Policy #9.1.13 (*De-Identifying Personal Health Information*) and POGO's *Privacy and Data Security Procedures*, Principle 5 (*Limiting Use, Disclosure and Retention*) require that personal health information not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose.

POGO's Policy #9.2.27 (*Small Cell*) sets out the restrictions related to cell-sizes of less than five and the exceptions thereto are articulated in the policy. In articulating the policy with respect to cell sizes of less than five, regard is had to the restrictions related to cell-sizes of less than five contained in Data Sharing Agreements, Researcher Agreements, and written research plans pursuant to which the personal health information was collected by POGO.

The policy and procedures provide a definition of de-identified information and aggregate information that identifies the meaning ascribed to each of these terms. The definitions adopted and the policy of POGO with respect to cell-sizes of less than five shall have regard to, and are consistent with the meaning of "identifying information" in subsection 4(2) of the *Act*.

The information that must be removed, encrypted and/or truncated in order to constitute de-identified information and the manner in which the information must be grouped, collapsed or averaged in order to constitute aggregate information is identified in Policy #9.1.13 (*De-Identifying Personal Health Information*). The policy and procedures note that the IT Team is responsible for de-identifying and/or aggregating information and the procedure to be followed in this regard.

Further, the policy and procedures require de-identified and/or aggregate information, including information of cell-sizes of less than five, to be reviewed prior to use or disclosure in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The IT Team in concert with the Senior Database Administrator are the agents responsible for conducting this review.

The process to be followed in reviewing the de-identified and/or aggregate information and the criteria to be used in assessing the risk of re-identification is also set out in the policy and procedures of Policy #9.1.13 (*De-Identifying Personal Health Information*). In establishing the criteria to be used in assessing the risk of re-identification, POGO has regard to the type of identifying information available, including information that can be used to identify an individual directly (e.g., name, address, health card number) or indirectly (e.g., date-of-birth, postal code, gender).

POGO continually reviews and adopts new tools that are developed to assist in ensuring that the policy and procedures developed with respect to de-identification and aggregation are based on an assessment of the actual risk of re-identification.

The policy and procedures also prohibit agents from using de-identified and/or aggregate information, including information in cell-sizes of less than five, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

The policy and procedures also identifies the mechanisms implemented to ensure that the persons or organizations to whom de-identified and/or aggregate information is disclosed will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual.

POGO requires agents to comply with the policy and its procedures and sets out how the Privacy Officer will enforce compliance and the consequences of breach. The policy and procedures stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*) annually, and the audit will be conducted by the Privacy Officer who ensure compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

25. Privacy Impact Assessment Policy and Procedures

Policy #9.1.14 (*Privacy Impact Assessment Process*) identifies the circumstances in which privacy impact assessments are required to be conducted.

In identifying the circumstances in which privacy impact assessments (PIAs) are required to be conducted, the policy and procedures ensure that POGO conducts privacy impact assessments on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology, or program involving personal health information is contemplated.

POGO Policy #9.1.14 (*Privacy Impact Assessment Process*) indicates that POGO conducts PIA's on all of its data holdings, and therefore the rationale for not conducting PIA's is not applicable.

The policy and procedures also set out the timing of privacy impact assessments. With respect to proposed data holdings involving personal health information and new or changes to existing information systems, technologies or programs involving personal health information, the policy and procedures set out that privacy impact assessments be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage. With respect to existing data holdings involving personal health information, the policy and procedures set out a timetable to ensure privacy impact assessments are conducted, and the policy and procedures identify the Privacy Officer as the agent for developing the timetable.

Once privacy impact assessments have been completed, the policy and procedures require that they will be reviewed on an ongoing basis, or minimally on an annual basis, in order to ensure that they continue to be accurate and continue to be consistent with the information practices of POGO. The policy and procedures also identify the circumstances in which and the frequency with which privacy impact assessments are required to be reviewed.

The policy and procedures identify the Privacy Officer as the agent responsible, and the process that must be followed in identifying when privacy impact assessments are required; in identifying when privacy impact assessments are required to be reviewed in accordance with the policy and procedures; in ensuring that privacy impact assessments are conducted and completed; and in ensuring that privacy impact assessments are reviewed and amended, if necessary. The Privacy Officer has been delegated day-to-day authority to manage the Privacy and Security Programs, and is also identified in respect of privacy impact assessments.

The policy and procedures stipulate the required content of privacy impact assessments. At a minimum, the privacy impact assessments are required to describe:

- The data holding, information system, technology, or program at issue;
- The nature and type of personal health information collected, used, or disclosed or that is proposed to be collected, used or disclosed;
- The sources of the personal health information;

- The purposes for which the personal health information is collected, used, or disclosed or is proposed to be collected, used, or disclosed;
- The reason that the personal health information is required for the purposes identified;
- The flows of the personal health information;
- The statutory authority for each collection, use, and disclosure of personal health information identified;
- The limitations imposed on the collection, use, and disclosure of the personal health information;
- Whether or not the personal health information is or will be linked to other information;
- The retention period for the records of personal health information;
- The secure manner in which the records of personal health information are or will be retained, transferred, and disposed of;
- The functionality for logging access, use, modification, and disclosure of the personal health information and the functionality to audit logs for unauthorized use or disclosure;
- The risks to the privacy of individuals whose personal health information is or will be part of the data holding, information system, technology, or program and an assessment of the risks;
- Recommendations to address and eliminate or reduce the privacy risks identified; and
- The administrative, technical, and physical safeguards implemented or proposed to be implemented to protect the personal health information.

The process for addressing the recommendations arising from privacy impact assessments, including the Privacy Officer as the agent responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations, and for monitoring and ensuring the implementation of the recommendations, are also outlined.

The policy and procedures require that a log be maintained of privacy impact assessments that have been completed; that have been undertaken but that have not been completed; and that have not been undertaken. The policy and procedures also identify the Privacy Team as the agents responsible for maintaining such a log.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*) which sets out the frequency with which the policy and procedures will be audited and that the Privacy Officer is responsible for conducting the audit, and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

In developing the policy and procedures, regard was had to the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, published by the Information and Privacy Commissioner of Ontario.

26. Log of Privacy Impact Assessments

POGO maintains a log of privacy impact assessments that have been completed and of privacy impact assessments that have been undertaken but that have not been completed. The log describes the data holding, information system, technology, or program involving personal health information that is at issue; the date that the privacy impact assessment was completed or is expected to be completed; the Privacy Team who are the agents responsible for completing or ensuring the completion of the privacy impact assessment; the recommendations arising from the privacy impact assessment; the Privacy Officer as the agent responsible for addressing each recommendation, 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.

POGO also maintains a log of data holdings involving personal health information and of new or changes to existing information systems, technologies or programs involving personal health information for which privacy impact assessments have not been undertaken. For each such data holding, information system, technology or program, the log either sets out the reason that a privacy impact assessment will not be undertaken and that the Privacy Officer is responsible for making this determination, or sets out the date that the privacy impact assessment is expected to be completed and the agent(s) responsible for completing or ensuring the completion of the privacy impact assessment.

27. Policy and Procedures in Respect of Privacy Audits

POGO's *Privacy and Security Policies and Procedures Manual*, Section 4 (*Internal and External Audits*) and Policy #9.1.15 (*Privacy Audits*) set out the types of privacy audits that are required to be conducted. At a minimum, the audits required to be conducted include audits to assess compliance with the privacy policies, procedures and practices implemented by POGO, and audits of the agent(s) permitted to access and use personal health information pursuant to POGO's *Privacy and Data Security Procedures*, Principle 5 (*Limiting Use, Disclosure, and Retention*).

With respect to each privacy audit that is required to be conducted, the policy and procedures set out the purposes of the privacy audit; the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections); the Privacy Officer as the agent responsible for conducting the privacy audit; and the frequency with which and the circumstances in which each privacy audit is required to be conducted. In this regard, the policy and procedures set out a privacy audit schedule to be developed and identify the Privacy Officer as the agent responsible for developing the privacy audit schedule.

For each type of privacy audit that is required to be conducted, the policy and procedures also set out the process to be followed in conducting the audit. This includes the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided. The policy and procedures further discuss the documentation that must be completed, provided, and/or executed in undertaking each privacy audit; the Privacy

Officer to whom this documentation must be provided; and the required content of the documentation.

The Privacy Officer is identified as having been delegated day-to-day authority to manage the Privacy and Security Audit Programs.

The policy and procedures also set out the process that must be followed in addressing the recommendations arising from privacy audits, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations, and for monitoring and ensuring the implementation of the recommendations.

The policy and procedures also set out the nature of the documentation that must be completed, provided, and/or executed at the conclusion of the privacy audit, including the Privacy Officer to whom the documentation must be provided and the required content of the documentation.

The policy and procedures further address the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of addressing the recommendations, are communicated. This includes a discussion of the Privacy Officer as the agent responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit will be communicated, including the Chief Executive Officer.

The policy and procedures further require that a log be maintained of privacy audits and identifies the Privacy Team as the agents responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified time frame. They also set out that the documentation related to privacy audits is retained in POGO's secured central filing system, and that the Privacy Officer is responsible for retaining this documentation.

The policy and procedures also require the Privacy Officer to be responsible for conducting the privacy audit, to notify the Chief Executive Officer and POGO's Medical Director at the first reasonable opportunity of a privacy breach or suspected privacy breach in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*) and of an information security breach or suspected information security breach in accordance with the same policy.

28. Log of Privacy Audits

POGO maintains a log of privacy audits that have been completed. The log sets out the nature and type of the privacy audit conducted; the date that the privacy audit was completed; the Privacy Officer as the agent responsible for completing the privacy audit; the recommendations arising from the privacy audit; the agent(s) responsible for addressing each recommendation; 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.

29. Policy and Procedures for Privacy Breach Management

Policy #9.1.16 (*Privacy Breach and Incident Management*) sets out the policy and procedures that address the identification, reporting, containment, notification, investigation, and remediation of privacy breaches.

The policy and procedures provide a definition of the term "privacy breach." A privacy breach is defined as including:

- The collection, use, and disclosure of personal health information that is not in compliance with the *Act* or its regulation;
- A contravention of the privacy policies, procedures, or practices implemented by POGO;
- A contravention of Data Sharing Agreements, Research Agreements, Confidentiality Agreements, and Agreements with Third Party Service Providers retained by POGO; and
- Circumstances where personal health information is stolen, lost, or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification or disposal.

The policy and procedures impose a mandatory requirement on agents to notify POGO of a privacy breach or a suspected privacy breach.

In this regard, the policy and procedures identify the Privacy Officer as the agent who must be notified of the privacy breach or suspected privacy breach and provides contact information for the Privacy Officer who must be notified. The policy and procedures further stipulate the time frame within which notification must be provided, that the notification must be provided verbally and in writing, and the nature of the information that must be provided upon notification. The policy and procedures also address the documentation that must be completed, provided and/or executed with respect to notification; the agent(s) responsible for completing, providing and/or executing the documentation; the Privacy Officer to whom the documentation must be provided; and the required content of the documentation.

Upon notification, the policy and procedures require a determination to be made of whether a privacy breach has in fact occurred and if so, what, if any, personal health information has been breached. The Privacy Officer responsible for making this determination is also identified.

The policy and procedures further address when senior management will be notified, including the Chief Executive Officer. This includes a discussion of the Privacy Officer who is responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.

The policy and procedures also require that containment be initiated immediately and identify the Privacy Officer and the IT Team who are responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided, and/or

executed by the Privacy Officer responsible for containing the breach and the required content of the documentation.

In undertaking containment, the policy and procedures ensure that reasonable steps are taken in the circumstances to protect personal health information from further theft, loss, or unauthorized use or disclosure and to protect records of personal health information from further unauthorized copying, transmission, modification, or disposal. At a minimum, these steps include ensuring that no copies of the records of personal health information have been made and ensuring that the records of personal health information are either retrieved or disposed of in a secure manner. Where the records of personal health information are securely disposed of, written confirmation is obtained related to the date, time, and method of secure disposal. These steps also include ensuring that additional privacy breaches cannot occur through the same means and determining whether the privacy breach would allow unauthorized access to any other information and, if necessary, taking further action to prevent additional privacy breaches.

The Privacy Officer who is responsible, and the process to be followed in reviewing the containment measures implemented and determining whether the privacy breach has been effectively contained or whether further containment measures are necessary are also identified in the policy and procedures. The policy and procedures also address the documentation that must be completed, provided, and/or executed by the Privacy Officer who is responsible for reviewing the containment measures; the Privacy Officer to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures require the health information custodian, or other organization that disclosed the personal health information to POGO be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost, transmitted, or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization.

In particular, the policy and procedures set out the Privacy Officer as the agent responsible for notifying the health information custodian or other organization, the format of the notification and the nature of the information that must be provided upon notification. At a minimum, the policy and procedures require the health information custodian or other organization to be advised of the extent of the privacy breach, the nature of the personal health information at issue, the measures implemented to contain the privacy breach, and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation. As a secondary collector of personal health information, POGO does not directly notify the individual to whom the personal health information relates of a privacy breach. The required notification shall be provided by the health information custodian.

The policy and procedures also set out whether any other persons or organizations must be notified of the privacy breach and sets out the Privacy Officer as the agent responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification, and the time frame for notification.

The policy and procedures further identify the Privacy Officer as the agent responsible for investigating the privacy breach, the nature and scope of the investigation, (i.e. document reviews,

interviews, site visits, inspections) and the process that must be followed in investigating the privacy breach. This process includes a discussion of the documentation that must be completed, provided, and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing, and/or executing the documentation; the Privacy Officer to whom this documentation must be provided; and the required content of the documentation.

The Privacy Officer has been delegated day-today authority to manage the Privacy and Security Breach Programs.

The policy and procedures also identify the Privacy Officer as the agent responsible for assigning other agent(s) to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations of the privacy audit are implemented within the stated timelines. The policy and procedures also set out the nature of the documentation that must be completed, provided, and/or executed at the conclusion of the investigation of the privacy breach, including the Privacy Officer as the agent responsible for completing, providing, and/or executing the documentation, and the required content of the documentation; and the agents to whom the documentation must be provided.

The policy and procedures also address the manner and format in which the findings of the investigation of the privacy breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This includes a discussion of the Privacy Officer who is responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation are communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer.

In addition, the policy and procedures address whether the process to be followed in identifying, reporting, containing, notifying, investigating, and remediating a privacy breach is different where the breach is both a privacy breach or suspected privacy breach, as well as an information security breach or suspected information security breach.

Further, the policy and procedures require that a log be maintained of privacy breaches and identify the Privacy Team as the agents responsible for maintaining the log and the Privacy Officer for tracking that the recommendations arising from the investigation of privacy breaches are addressed within the identified timelines. The policy and procedure further state that the documentation related to the identification, reporting, containment, notification, investigation, and remediation of privacy breaches will be retained in POGO's secured central files by the Privacy Team who are responsible for retaining this documentation.

POGO requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*), sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

When developing the policy and procedures, POGO had regard to the guidelines produced by the Information and Privacy Commissioner of Ontario entitled, *What to do When Faced with a Privacy Breach: Guidelines for the Health Sector*.

30. Log of Privacy Breaches

The POGO Privacy Team maintains a log of privacy breaches setting out:

- The date of the privacy breach;
- The date that the privacy breach was identified or suspected;
- Whether the privacy breach was internal or external
- The nature of the personal health information that was the subject matter of the privacy breach and the nature and extent of the privacy breach
- The date that the privacy breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to POGO was notified;
- The date that the investigation of the privacy breach was completed;
- The Privacy Officer responsible for conducting the investigation;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

31. Policy and Procedures for Privacy Complaints

POGO's *Privacy and Data Security Procedures*, Principle 10 (*Challenging Compliance*) addresses the process to be followed in receiving, documenting, tracking, investigating, remediating, and responding to privacy complaints. A definition of the term "privacy complaint" is provided and it includes concerns or complaints relating to the privacy policies, procedures and practices implemented by POGO and related to the compliance of POGO with the *Act* and its regulation.

The information that must be communicated to the public relating to the manner in which, to whom, and where individuals may direct privacy concerns or complaints is also identified. At a minimum, the name and/or title, mailing address, and contact information of the Privacy Officer to whom concerns or complaints may be directed and information related to the manner in which and format in which privacy concerns or complaints may be directed to POGO is made publicly available. It is also stated that individuals may make a complaint regarding compliance with the *Act* and its regulation to the Information and Privacy Commissioner of Ontario and the mailing address and contact information for the Information and Privacy Commissioner of Ontario is provided.

The policy and procedures further establish the process to be followed in receiving privacy complaints. This includes any documentation that must be completed, provided, and/or executed

by the individual making the privacy complaint; the Privacy Officer as the agent for receiving the privacy complaint; the required content of the documentation, if any; and the nature of the information to be requested from the individual making the privacy complaint.

Upon receipt of a privacy complaint, the policy and procedures require a determination to be made of whether or not the privacy complaint will be investigated. In this regard, the policy and procedures identify the Privacy Officer as the agent responsible for making this determination, the time frame within which this determination must be made and the process that must be followed and the criteria that must be used in making the determination, including any documentation that must be completed, provided, and/or executed and the required content of the documentation.

In the event that it is determined that an investigation will not be undertaken, the policy and procedures require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken; advising the individual that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that POGO has contravened or is about to contravene the *Act* or its regulation; and providing contact information for the Information and Privacy Commissioner of Ontario.

In the event that it is determined that an investigation will be undertaken, the policy and procedures require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; advising that an investigation of the privacy complaint will be undertaken; explaining the privacy complaint investigation procedure; indicating whether the individual will be contacted for further information concerning the privacy complaint; setting out the projected time frame for completion of the investigation; and identifying the nature of the documentation that will be provided to the individual following the investigation.

The policy and procedures identify the Chief Executive Officer and Privacy Officer as the agent responsible for sending the above noted letters to the individuals making privacy complaints and the time frame within which the letters will be sent to the individuals.

Where an investigation of a privacy complaint will be undertaken, the policy and procedures identify the Privacy Officer as the agent responsible for investigating the privacy complaint, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy complaint. This process includes a discussion of the documentation that must be completed, provided, and/or executed in undertaking the investigation; the Privacy Officer as the agent responsible for completing, providing, and/or executing the documentation, the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The Privacy Officer has been delegated day-to-day authority to manage the Privacy Program and the Security Program and are identified in the policy and procedures.

The process for addressing the recommendations arising from the investigation of privacy complaints and the Privacy Officers as the agent responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, and for

monitoring and ensuring the implementation of the recommendations is also addressed in the policy and procedures. The policy and procedures set out the nature of the documentation that will be completed, provided, and/or executed at the conclusion of the investigation of the privacy complaint, including the Privacy Officer as the agent responsible for completing, preparing, and/or executing the documentation, the Privacy Officer to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also address the manner and format in which the findings of the investigation of the privacy complaint, including recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This process includes a discussion of the Privacy Officer as the agent responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings must be communicated, including the Chief Executive Officer.

The policy and procedures further require the individual making the privacy complaint to be notified, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint. The individual making the privacy complaint will be advised that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the *Act* or its regulation has been or is about to be contravened. The contact information for the Information and Privacy Commissioner of Ontario is also provided. The Privacy Officer is the agent responsible for providing the written notification to the individual making the privacy complaint and the time frame within which the written notification must be provided, is also addressed.

The policy and procedures also address whether any other person or organization must be notified of privacy complaints and the results of the investigation of privacy complaints, and if so, the manner by which, the format in which, and the time frame within which the notification must be provided as well as the Privacy Officer who is responsible for providing the notification.

Further, the policy and procedures require that a log be maintained of privacy complaints and identifies the Privacy Team as the agents responsible for maintaining the log and for tracking whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines. The process further addresses that the documentation related to the receipt, investigation, notification, and remediation of privacy complaints will be retained on POGO's secured central files by the Privacy Officer who is responsible for retaining this documentation.

POGO requires agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with the Policy #9.1.15 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and procedures and Policy #9.1.16 (*Privacy Breach and Incident Management*) is also addressed.

32. Log of Privacy Complaints

POGO maintains a log of privacy complaints received that, at a minimum, sets out:

- The date that the privacy complaint was received and the nature of the privacy complaint;
- The determination as to whether or not the privacy complaint will be investigated and the date that the determination was made;
- The date that the individual making the complaint was advised that the complaint will not be investigated and was provided a response to the complaint;
- The date that the individual making the complaint was advised that the complaint will be investigated;
- The agent(s) responsible for conducting the investigation;
- The dates that the investigation was commenced and completed;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed;
- The manner in which each recommendation was or is expected to be addressed; and
- The date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint.

33. Policy and Procedures for Privacy Inquiries

POGO's *Privacy and Data Security Procedures*, Principle 10 (*Challenging Compliance and Privacy Inquiries*) addresses the process to be followed in receiving, documenting, tracking, and responding to privacy inquiries. A definition of the term "privacy inquiry" is provided that includes inquiries relating to the privacy policies, procedures and practices implemented by POGO and related to the compliance of POGO with the *Act* and its regulation.

The information that must be communicated to the public relating to the manner in which, to whom, and where individuals may direct privacy inquiries is also identified. At a minimum, the information communicated to the public includes the name and/or title, mailing address, and contact information of the Privacy Officer to whom privacy inquiries may be directed; information relating to the manner in which privacy inquiries may be directed to POGO; and to and information as to where individuals may obtain further information about the privacy policies, procedures and practices implemented by POGO by contacting the Privacy Officer directly.

The policy and procedures further establish the process to be followed in receiving and responding to privacy inquiries. This includes the Privacy Officer as the agent responsible for receiving and responding to privacy inquiries; any documentation that must be completed, provided, and/or executed; the required content of the documentation; and the format and content of the response to the privacy inquiry. The role of the Privacy Officer has been delegated day-to-day authority to manage the privacy program and the Security Program and is also identified.

POGO requires agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures

must also stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited, and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and POGO's *Privacy and Data Security Procedures*, Principle 10 (*Challenging Compliance and Privacy Inquiries*) and Policy #9.1.16 (*Privacy Breach and Incident Management*) is also addressed.

Part 2 – Security Documentation

1. Information Security Policy

POGO's Privacy Program, which includes the Security Program, is articulated in the following overarching information security documents: POGO's *Privacy and Data Security Code, and* POGO's *Privacy and Data Security Procedures (the Manual), POGO's Business Continuity and Disaster Recovery Plan*, POGO's *Corporate Risk Management Framework*, POGO's *Security Standards*, and *POGO's Privacy and Security Governance and Accountability Framework*. These documents have been implemented in relation to personal health information received by POGO under the *Act*. The Privacy Program as well as POGO Policy #9.2.3 (*Security Standards and Procedures*) require that steps be taken to ensure that personal health information is protected against theft, loss, and unauthorized use or disclosure and ensures that the records of personal health information are protected against unauthorized copying, modification, or disposal.

The Privacy Program and POGO Policy #9.2.4 (*Threat and Risk Assessment*) require POGO to undertake comprehensive and organization-wide threat and risk assessments of all information security assets including personal health information, as well as appropriate project specific threat and risk assessments. Policy #9.2.4 (*Threat and Risk Assessment*) establishes and documents the methodology for identifying, assessing, and remediating threats and risks and for prioritizing all threats and risks identified for remedial action.

The Privacy Program together with POGO's Policy# 9.2.3 (*Security Standards and Procedures)* sets out the comprehensive Information Security Program, which consists of administrative, technical, and physical safeguards that are consistent with established industry standards and practices. The Privacy Program and POGO Policy #9.2.4 (*Threat and Risk Assessment*) effectively address the threats and risks identified, are amenable to independent verification, and are consistent with established security frameworks and control objectives. The duties and responsibilities of agents in respect of the Information Security Program and in respect of implementation of the administrative, technical, and physical safeguards are addressed in the Privacy Program.

The Privacy Program requires the Information Security Program to consist of the following control objectives and security policies, procedures, and practices:

- A Security Program for the implementation of the Information Security Program, including security training and awareness (i.e., Policy #9.2.3: *Security Standards and Procedures* and Policy #9.3.1: *Privacy and Security Training*);
- Policies and procedures for the ongoing review of the security policies, procedures, and practices implemented (i.e., Policy #9.1.2: *Review of Privacy and Security Policies and Procedures* and Policy #9.2.2: *Ongoing Review of Security Policies, Procedures and Practices*);
- Policies and procedures for ensuring the physical security of the premises (i.e., Policy #9.2.5: *Physical-Office Security*);
- Policies and procedures for the secure retention, transfer, and disposal of records of personal health information, including policies and procedures related to mobile devices, remote access and security of data at rest (i.e., Policy #9.2.6: *Retention, Return, and Destruction of Data*);
- Policies and procedures to establish access controls and authorization including business requirements, user access management, user responsibilities, network access control, operating system access control, and application and information access control (i.e., Policy #9.2.3 *Security Standards and Procedures*, and Section 3.3 of the POGO Privacy Binder: *POGONIS Security Controls and Performance*);
- Policies and procedures for information systems acquisition, development, and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development, and support procedures and technical vulnerability management (i.e., Policy #9.2.3: *Security Standards and Procedures*);
- Policies and procedures for monitoring, including policies and procedures for maintaining and reviewing system control and audit logs and security audits (i.e., Policy #9.2.3: *Security Standards and Procedures*);
- Policies and procedures for network security management, including change and patch management (i.e., Policy #9.2.13: *Change Managemen*t);
- Policies and procedures related to the acceptable use of information technology (i.e., Policy #9.2.15: *Acceptable Usage*);
- Policies and procedures for back-up and recovery (i.e., Policy #9.2.14: *Back-up and Recovery of Records of Personal Health Information* and Policy #9.2.3 *Security Standards and Procedures*);
- Policies and procedures for information security breach management (i.e., Policy 9.1.16 *Privacy Breach and Incident Management* and Policy #9.2.17: *Information Security Incident Management Process*); and
- Policies and procedures to establish protection against malicious and mobile code (i.e., Policy #9.2.3: *Security Standards and Procedures* and Policy #9.2.24: *Anti-Virus Spam*).

The Privacy Program together with POGO Policy #9.2.3 (*Security Standards and Procedures*) outlines the information security infrastructure implemented by POGO including the transmission of personal health information over authenticated, encrypted and secure connections; the establishment of hardened servers, firewalls, demilitarized zones, and other perimeter defences; anti-virus, anti-spam and anti-spyware measures; intrusion detection and prevention systems; privacy and security enhancing technologies; and mandatory system-wide password-protected screen savers after a defined period of inactivity.

In addition, POGO's Privacy Program, Policy #9.2.3 (*Security Standards and Procedures*), and POGO's Privacy and Security Audit Program constitute a credible program for the continuous assessment and verification of the effectiveness of the POGO Security Program in order to deal with threats and risks to data holdings containing personal health information.

POGO requires agents to comply with these above policies and with all other security policies, procedures, and practices implemented by POGO. Compliance and consequences of breach are enforced by the Privacy Officer and the IT Team. Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17: (*Information Security Incident Management Process*) indicate that a breach may result in discipline, up to and including termination of an employee or termination of a relationship with agents who are not POGO employees.

POGO's *Privacy and Security Policies and Procedures Manual,* Section 4, outlines that compliance will be audited annually in accordance with POGO's Privacy and Security Audit Program and identifies the Privacy Officer and the IT Team as the agents responsible for conducting the audit and for ensuring compliance with the policy.

Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) also requires agents to notify POGO at the first reasonable opportunity, if an agent breaches or believes there may have been a breach of these policies or any other security policies, procedures and practices implemented.

2. Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices

POGO has developed and implemented Policy #9.1.2 (*Review of Privacy and Security Policies and Procedures*) and Policy #9.2.2 (*Ongoing Review of Security Policies, Procedures and Practices*) for the ongoing review of its security policies, procedures and practices. The purpose of the review is to determine whether amendments are needed or whether new security policies, procedures and practices are required.

Policy #9.1.2 (*Review of Privacy and Security Policies and Procedures*) and Policy #9.2.2 (*Ongoing Review of Security Policies, Procedures and Practices*) indicate that the Privacy Officer and the IT Team will undertake the annual review. These policies and procedures also identify the Privacy Officer and the IT Team as the agents responsible, and the procedure to be followed in amending and/or drafting new security policies, procedures and practices if deemed necessary as a result of the review, and the Privacy Officer as the agent responsible, and the procedure that must be followed in obtaining approval of any amended or newly developed security policies, procedures and practices.

In undertaking the review and determining whether amendments and/or new security policies, procedures and practices are necessary, POGO has regard for any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation; evolving industry security standards and best practices; technological advancements; amendments to the *Act* and its regulation relevant to POGO; and recommendations

arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches. It also takes into account whether the security policies, procedures and practices of POGO continue to be consistent with its actual practices and whether there is consistency between and among the Security and Privacy Policies, Procedures and practices implemented.

Policy #9.1.2 (*Review of Privacy and Security Policies and Procedures*) and Policy #9.2.2 (*Ongoing Review of Security Policies, Procedures and Practices*) indicate that the Privacy Officer and the IT Team will be responsible for amending and/or drafting new policies, procedures, or practices if deemed necessary after the review and that the Privacy Officer and the IT Team will be responsible for any such amendments or additions to the policy suite. Further, the Privacy Officer is responsible for communicating applicable policy changes or additions that are able to be shared with its agents, and determining the method and nature of the communication. The Privacy Officer ensures that any communication materials made available to the public and other stakeholders are reviewed and amended accordingly, the procedure for which is set out in the policy.

POGO requires agents to comply with the policy and its procedures which are enforced by POGO's Chief Executive Officer through the Privacy Officer. According to the POGO Confidentiality and Non-Disclosure Agreement, the consequence of a breach may include discipline up to and including termination of employment with POGO, or termination of a relationship with agents who are not POGO employees. As indicated in the POGO Privacy and Security Audit Program, compliance will be audited on an annual basis and the Privacy Officer will be responsible for conducting the audit.

3. Policy and Procedures for Ensuring Physical Security of Personal Health Information

POGO's Privacy Program and Policy #9.2.5 (*Physical-Office Security*) addresses the physical safeguards implemented by POGO to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

In addition, POGO Policy #9.1.6 (*Levels of Access*) requires POGO to implement controlled access to the premises and to locations within the premises where records of personal health information are retained such as locked, alarmed, restricted and/or monitored access.

Policy #9.1.6 (*Levels of Access*) outlines the premises of POGO be divided into five levels of security (with zero level being the most secure level and restricted to fewer individuals). In order to gain physical access to records of personal health information, individuals would be required to pass through three levels of security.

Furthermore, agents of POGO are assigned a system level of access on a need-to-know basis. This level is assigned and approved by the Privacy Officer.

Policy #9.1.6 (*Levels of Access*), and Policy #9.2.5 (*Physical-Office Security*) POGO privacy and security policies, require agents of POGO to comply with its terms. Compliance is enforced by the Privacy Officer as per Policy # 9.3.6 (*Disciplinary Action – Privacy Breach*).The policy and procedure also outline that breach of the policy may result in discipline, up to and including termination of an employee or termination of a relationship with agents who are not POGO employees.

As indicated in the Policy #9.1.6 (*Levels of Access*), and Policy #9.2.5 (*Physical-Office Security*) compliance is audited in accordance with POGO's Privacy and Security Audit Program on an annual basis and the Privacy Officer is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Policy #9.1.6 (*Levels of Access*) also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes that there may have been a breach of these policies or their associated procedures. Any breach of this policy will lead to a review of the incident by the POGO Privacy Officer and may result in disciplinary action as per Policy #9.3.6 (*Disciplinary Action - Privacy Breach*) and the POGO Confidentiality and Non-Disclosure Agreement.

Policy, Procedures and Practices with Respect to Access by Agents

The various levels of access that may be granted to the POGO premises and locations within the POGO premises where records of personal health information are retained are set out in Policy #9.1.6 (*Levels of Access*).

Policy #9.1.6 (*Levels of Access*) identifies the Privacy Officer as the agent responsible for receiving, reviewing, granting and terminating access by agents to the premises and to locations within the premises where records of personal health information are retained, including the levels of access that may be granted. The process to be followed and the requirements that must be satisfied are included in Policy #9.1.6 (*Levels of Access*). The Access Control Card Tracking Log is completed by the Privacy Team who are the agents to whom the documentation must be provided and includes the required content of the documentation.

Policy #9.1.6 (*Levels of Access*) further addresses the criteria that must be considered by the Privacy Officer for approving and determining the appropriate level of access. The criteria are based on the "need to know" principle and ensure that access is only provided to agents who routinely require such access for their employment, contractual or other responsibilities. In the event that an agent only requires such access for a specified period, the policy and procedures establish a process for ensuring that access is permitted only for that specified period.

This policy and procedures also set out the manner in which the determination relating to access and the level of access is documented; to whom this determination is to be communicated; any documentation that must be completed, provided, and/or executed by the Privacy Officer who is responsible for making the determination; and the required content of the documentation.

Policy #9.1.6 (*Levels of Access*) also addresses the Privacy Team who are responsible, and the process to be followed in providing identification cards, access cards and/or keys to the premises and to locations within the premises. This policy includes a discussion of any documentation that must be completed, provided and/or executed; the Privacy Team who are responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

Theft, Loss and Misplacement of Identification Cards, Access Cards and Keys

POGO Policy #9.2.5 (*Physical-Office Security*) requires agents to notify POGO at the first reasonable opportunity of the theft, loss or misplacement of identification cards, access cards and/or keys and sets out the process that must be followed in this regard. This policy identifies the Privacy Team as the agents to whom the notification must be provided; the nature and format of the notification; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The safeguards that are required to be implemented as a result of the theft, loss or misplacement of identification cards, access cards and/or keys and the agent(s) responsible for implementing these safeguards is also outlined in Policy #9.2.5 (*Physical-Office Security*).

The policy and procedures also addresses the circumstances in which and the procedure that must be followed in issuing temporary or replacement identification cards, access cards and/or keys and the agent(s) responsible for their issuance. This includes a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; the required content of the documentation; the agent(s) to whom temporary identification cards, access cards and/or keys shall be returned; and the time frame for return.

The process to be followed in the event that temporary identification cards, access cards and/or keys are not returned, including the agent(s) responsible for implementing the process and the time frame within which the process must be implemented, is also addressed.

Termination of the Employment, Contractual or Other Relationship

Policy #9.3.4 (*Termination or Cessation of Employment or Contractual Relationship*) requires agents, as well as their supervisors, to notify POGO of the termination of their employment, contractual or other relationship with POGO and to return their identification cards, access cards and/or keys to the POGO Privacy Team on or before the date of termination of their employment, contractual or other relationship.

Policy #9.3.4 (*Termination or Cessation of Employment or Contractual Relationship*) also requires that access to the premises be terminated upon the cessation of the employment, contractual or other relationship.

Notification When Access is No Longer Required

Policy #9.1.6 (*Levels of Access*) requires an agent granted approval to access location(s) where records of personal health information are retained, as well as his or her supervisor, to notify POGO's Privacy Team when the agent no longer requires such access.

This policy identifies the Privacy Team as the agents to whom the notification must be provided; the nature and format of the notification; the time frame within which the notification must be provided; the process that must be followed in providing the notification; the agent(s) responsible for terminating access; the procedure to be followed in terminating access; the method by which access will be terminated; and the time frame within which access must be terminated.

Audits of Agents with Access to the Premises

Audits must be conducted of agents with access to the premises of POGO and to locations within the premises where records of personal health information are retained in accordance with Policy #9.1.6 (*Levels of Access*). The purpose of the audit is to ensure that agents granted access to the premises and to locations within the premises where records of personal health information are retained continue to have an employment, contractual or other relationship with POGO and continue to require the same level of access.

In this regard, the Policy #9.1.6 (*Levels of Access*) identifies the Privacy Officer as the agent responsible for conducting the audits and for ensuring compliance with the policy and its procedures and the frequency with which the audits must be conducted. These audits are conducted on an annual basis.

Tracking and Retention of Documentation Related to Access to the Premises

Policy #9.1.6 (*Levels of Access*) requires that a log be maintained of agents granted approval to access the premises of POGO and to locations within the premises where records of personal health information are retained and identifies the Privacy Team as the agents responsible for maintaining such a log. The policy and procedures also address where documentation related to the receipt, review, approval and termination of access to the premises and to locations within the premises where personal health information is retained is maintained, and indicates the Privacy Team as the agents responsible for maintaining this documentation.

Policy, Procedures and Practices with Respect to Access by Visitors

POGO's Policy #9.1.24 (*POGO Visitor Sign-In*) outlines POGO's process for identifying, screening, and supervising visitors on the premises. The policy and procedure sets out the identification that is required to be worn by visitors; the documentation that must be completed, provided and /or executed by the agents responsible for identifying, screening, and supervising visitors; and the documentation that must be completed, provided and /or executed by the visitors.

POGO visitors are required to record their name, date and time of arrival, time of departure and the name of the agent(s) with whom the visitors are meeting.

The agent(s) responsible for identifying, screening, and supervising visitors ensure that visitors are accompanied at all times; also ensure that visitors are wearing the identification issued by the responsible POGO agent receiving the visitor; ensuring that the identification is returned prior to departure; and that visitors complete the appropriate documentation upon arrival and departure.

The policy addresses the process followed by the Privacy Team when the visitor does not return the identification provided or does not document the date and time of their departure.

The policy also indicates that the Privacy Team members are the agents who retain the documentation related to the identification, screening, and supervision of the visitor.

4. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity

POGO maintains an Access Control Card Tracking Log of agents granted approval to access the premises of POGO and the level of access granted. The log includes the name of the agent granted approval to access the premises; the level and nature of the access granted; the locations within the premises to which access is granted; the date that the access was granted; the date(s) that identification cards, access cards and/or keys were provided to the agent; the identification numbers on the identification cards, access cards and/or keys, if any; the date of the next audit of access; and the date that the identification cards, access cards and/or keys were returned to POGO, if applicable.

5. Policy and Procedures for Secure Retention of Records of Personal Health Information

POGO's Privacy Program and Policy #9.2.6 (*Retention, Return, and Destruction of Data*), was developed and implemented with respect to the secure retention of records of personal health information in paper and electronic format.

This policy identifies the retention period for records of personal health information in both paper and electronic format, including various categories thereof. For records of personal health information used for research purposes, POGO ensures that the records of personal health information are not being retained for a period longer than that set out in the written research plan approved by a REB. For records of personal health information collected pursuant to a Data Sharing Agreement, the policy and procedures prohibit the records from being retained for a period longer than that set out in the Data Sharing Agreement. In any event, the policy and procedures mandate that records of personal health information be retained for only as long as necessary to fulfill the purposes for which the personal health information was collected.

This policy also requires the records of personal health information to be retained in a secure manner and identifies the Privacy Officer as the agent responsible for ensuring the secure retention of these records. In this regard, the policy and procedures identify the precise methods by which records of personal health information in paper and electronic format are to be securely retained, including records retained on various media.

Further, this policy requires agents of POGO to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal. These steps that must be taken by agents are also outlined in the policy and procedures.

POGO does not retain a third party service provider whose primary service to POGO is the retention of records of PHI. Accordingly, POGO does not require any third party service provider to maintain a detailed inventory of records of personal health information, in regard to such retention.

As indicated in POGO's Privacy Program and Policy #9.2.6 (*Retention, Return, and Destruction of Data*) compliance is audited in accordance with POGO's Privacy and Security Audit Program on an annual basis and the Privacy Officer is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

POGO's Policy #9.2.6 (*Retention, Return, and Destruction of Data*) requires agents to notify the Privacy Officer at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes that there may have been a breach of these policies or their associated procedures. Any breach of this policy will lead to a review of the incident by the POGO Privacy Officer and may result in disciplinary action as per Policy #9.3.6 (*Disciplinary Action - Privacy Breach*) and the POGO Confidentiality and Non-Disclosure Agreement.

6. Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices

POGO's Privacy Program and Policy #9.2.7 (*Personal Health Information on Mobile Devices*) identifies whether and in what circumstances, if any, POGO permits personal health information to be retained on a mobile device. In this regard, the policy and procedures provide a definition of "mobile device."

In drafting this policy, POGO had regard to orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-004 and Order HO-007; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including Fact Sheet 12: *Encrypting Personal Health Information on Mobile Devices* and Fact Sheet 14: *Wireless Communication Technologies: Safeguarding Privacy and Security and Safeguarding Privacy in a Mobile Workplace.*

POGO requires agents to comply with this policy and its procedures, and addresses how and by whom compliance will be enforced and the consequences of breach. This policy stipulates that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting an annual audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

Where Personal Health Information is Permitted to be Retained on a Mobile Device

Policy #9.2.7 (*Personal Health Information on Mobile Devices*), and Policy # 9.1.6 *(Levels* of Access) also set out the circumstances in which POGO permits personal health information to be retained on a mobile device.

Personal health information is retained on a mobile device for the purposes of section 45 of PHIPA when data is:

- Transferred to external agents into an encrypted mobile device by a secure file transfer server for analysis purposes or to another 45 entity for linkage purposes. The PHI file is only retained in the secure file transfer server until it is downloaded by the agent as per Policy # 9.29 (*Secure Transfer of Records of Personal Health Information*). Agreements must be in place before transfer; and
- Retained on backup tape and transferred to offsite secure bank safety deposit box.

For purposes of section 44 of PHIPA, when data is transferred to the research team.

For POGO consent-based programs (SAVTI and Interlink Community Cancer Nurses) personal health information (specifically, name and contact information) is being retained on mobile devices for the purposes of scheduling appointments with the clients.

Approval Process

Policy #9.2.7 (*Personal Health Information on Mobile Devices*) states whether approval is required prior to retaining personal health information on a mobile device.

If approval is required, the policy and procedures identify the process that must be followed and the Privacy Officer as the agent responsible for receiving, reviewing and determining whether to approve or deny a request for the retention of personal health information on a mobile device. This also includes a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the Privacy Officer to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures further address the requirements that must be satisfied and the criteria that must be considered by the Privacy Officer when determining whether to approve or deny a request for the retention of personal health information on a mobile device.

Prior to any approval of a request to retain personal health information on a mobile device, the policy and procedures require the Privacy Officer who is responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information will not serve the identified purpose, and that no more personal health information will be retained on the mobile device than is reasonably necessary to meet the identified purpose.

The policy and procedures also require the Privacy Officer as the agent responsible for determining whether to approve or deny the request to ensure that the use of the personal health information has been approved pursuant to Policy #9.1.6 (*Levels of Access*), and Policy #9.2.7 (*Personal Health Information on Mobile Devices*).

Policy #9.1.6 (*Levels of Access*), and Policy #9.2.7 (*Personal Health Information on Mobile Devices*) also set out the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Retention of Personal Health Information on a Mobile Device

Policy #9.2.7 (*Personal Health Information on Mobile Devices)* requires mobile devices containing personal health information to be encrypted as per Policy #9.2.21 (*Encryption*) as well as password-protected using strong and complex passwords that are in compliance with Policy #9.2.10 (*Password*). Where mobile devices have display screens, the policy and procedures further require that a mandatory standardized password-protected screen saver be enabled after a defined period of inactivity. The host hospital for the Interlink Nurse is responsible for encrypting mobile devices and for ensuring that the mandatory standardized password-protected screen saver is enabled.

Policy #9.2.7 (*Personal Health Information on Mobile Devices*) also identifies the conditions or restrictions with which agents granted approval to retain personal health information on a mobile device must comply. The agents must:

- Be prohibited from retaining personal health information on a mobile device if other information, such as de-identified and/or aggregate information, will serve the purpose;
- De-identify the personal health information to the fullest extent possible;
- Be prohibited from retaining more personal health information on a mobile device than is reasonably necessary for the identified purpose;
- Be prohibited from retaining personal health information on a mobile device for longer than necessary to meet the identified purpose;
- Ensure that the strong and complex password for the mobile device is different from the strong and complex passwords for the files containing the personal health information and that the password is supported by "defence in depth" measures.

The policy also details the steps that must be taken by agents to protect the personal health information retained on a mobile device against theft, loss and unauthorized use or disclosure and to protect the records of personal health information retained on a mobile device against unauthorized copying, modification or disposal.

The policy and procedures also require agents to retain the personal health information on a mobile device in compliance with Policy #9.2.7 (*Personal Health Information on Mobile Devices*) and to securely delete personal health information retained on a mobile device in accordance with the process and in compliance with the time frame outlined in the policy and procedures.

Where Personal Health Information is not Permitted to be Retained on a Mobile Device

As discussed above, POGO does allow personal health information to be stored on mobile devices under specific circumstances.

In the circumstances where personal health information is not permitted to be retained on a Mobile Device, Policy #9.2.7 (*Personal Health Information on Mobile Devices)* identifies that POGO permits access of personal health information via secure connection and virtual private network.

Approval Process

Policy #9.2.7 (*Personal Health Information on Mobile Devices)* also identifies the conditions or restrictions with which agents are granted approval prior to accessing personal health information through the secure connection and virtual private network.

The policy refers to Policy #9.1.6 (*Levels of Access)* which identifies the process that must be followed and identifies the Privacy Officer as the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for remote access to personal health information. Policy #9.1.6 *(Levels of Access)* outlines the documentation that must be completed in Policy #9.2.15 *(Acceptable Usage)*; and the agent(s) responsible for completing, providing and executing

the documentation; the agent(s) to whom these documentation must be provided; and the required content of the documentation. Policy #9.1.6 (*Levels of Access)* also addresses the requirements that must be satisfied and the criteria that must be considered by the Privacy Officer for determining whether to approve or deny the request for remote access.

Policy #9.1.6 (*Levels of Access)* also requires the Privacy Officer to ensure that other information, namely de-identified and/or aggregate information will not serve the identified purpose and that no more personal health information will be accessed than is reasonably necessary to meet the identified purpose and that the use of personal health information has been approved pursuant to Policy #9.1.6 (*Levels of Access).*

Policy #9.1.6 (*Levels of Access)* also sets out the manner in which the decision to approve or deny the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated by the Privacy Officer.

Conditions or Restrictions on the Remote Access to Personal Health Information

Policy #9.3.26 *(Remote Access*), and Policy #9.1.6 (*Levels of Access)* identify the conditions and restrictions with which agents are granted approval to access personal health information remotely, and must comply. Agents are prohibited from remotely accessing personal health information if other information, such as de-identified and/or aggregate information, will serve the purpose and from remotely accessing more personal health information than is reasonably necessary for the identified purpose. The policies and its procedures set out the administrative, technical and physical safeguards that must be implemented by agents in remotely accessing personal health information.

7. Policy and Procedures for Secure Transfer of Records of Personal Health Information

POGO has developed and implemented a guiding policy, Policy #9.2.9 (*Secure Transfer of Records of PHI*) with respect to the secure transfer of records of personal health information in paper and electronic format. In addition, POGO has developed and implemented, in respect of secure paper transfer, Policy #9.2.18 (*Confidentiality and Security of Data*) and Policy #9.2.20 (*Secured Faxes*), in respect of secure electronic transfer of personal health information; Policy #9.2.18 (*Confidentiality and Security of Data*), and Policy #9.2.21 (*Encryption*).

POGO's Privacy Program, Section 3.3 (*POGONIS Security Controls and Performance*) was specifically developed and implemented for the secure transfer of personal health information from the POGO tertiary pediatric oncology hospital partners to POGONIS.

These policies require records of personal health information to be transferred in a secure manner and set out the secure methods of transferring records of personal health information in paper and electronic format that have been approved by POGO. The policies and procedures require agents

to use the approved methods of transferring records of personal health information and prohibit all other methods.

The procedures to be followed in transferring records of personal health information through each of the approved methods are outlined. The polices include a discussion of the conditions pursuant to which records of personal health information will be transferred; the agent(s) responsible for ensuring the secure transfer; any documentation that is required to be completed, provided and/or executed in relation to the secure transfer; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

The policy and procedures also stipulate that the agents transferring records of personal health information are required to document the date, time, mode of transfer; the recipients of the records of personal health information; and the nature of the records of personal health information transferred. Further, the policy and procedures note that confirmation of receipt of the records of personal health information from or to the recipient, and the manner in obtaining the receipt is logged. All transfers of personal health information from the POGO tertiary pediatric oncology hospital partners to POGONIS are systematically logged. All POGO transfers of records of PHI for 44 and 45 projects are logged in the POGO Research Unit (PRU) Database.

Policy # 9.2.9 (*Secure Transfer of Records of PHI*) addresses the administrative, technical and physical safeguards that have been implemented for transferring records of personal health information through each of the approved methods in order to ensure that the records of personal health information are transferred in a secure manner.

POGO ensures that the approved methods of securely transferring records of personal health information and the procedures and safeguards that are required to be implemented in respect of the secure transfer of records of personal health information are consistent with:

- Orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including but not limited to Order HO-004 and Order HO-007;
- Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario, including *Privacy Protection Principles for Electronic Mail Systems* and *Guidelines on Facsimile Transmission Security*; and
- Evolving privacy and security standards and best practices.

POGO requires agents to comply with Policy # 9.2.9 (*Secure Transfer of Records of PHI*) and addresses how and by whom compliance will be enforced and the consequences of breach. This policy stipulates that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

8. Policy and Procedures for Secure Disposal of Records of Personal Health Information

POGO's Privacy Program, Policy #9.2.6 (*Retention, Return, and Destruction of Data*) and Policy #9.2.19 (*Document Shredding*) were developed and implemented with respect to the secure disposal of records of personal health information in both paper and electronic format in order to ensure that reconstruction of these records is not reasonably foreseeable in the circumstances.

These policies require records of personal health information to be disposed of in a secure manner and provide a definition of secure disposal that is consistent with the *Act* and its regulation. The policies and procedures further identify the precise method by which records of personal health information in paper format are required to be securely disposed of and the precise method by which records of personal health information in electronic format, including records retained on various media, are required to be securely disposed of.

In addressing the precise method by which records of personal health information in paper and electronic format are to be securely disposed of, POGO ensures that the method of secure disposal adopted is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including Fact Sheet 10: *Secure Destruction of Personal Information*.

The policy and procedures further address the secure retention of records of personal health information pending their secure disposal in accordance with Policy #9.2.6 *(Retention, Return, and Destruction of Data*), and Policy #9.2.28 *(Inventory of PHI Placed in Secure Gray Bin*).
These policies and procedures require the physical segregation of records of personal health information intended for secure disposal from other records intended for recycling, ensures an area is designated for the secure retention of records of personal health information pending their secure disposal, and requires the records of personal health information to be retained in a clearly marked and locked container pending their secure disposal. These policies and procedures also identify the Privacy Officer as the agent responsible for ensuring the secure retention of records of personal health information pending their secure disposal.

In the event that records of personal health information will be securely disposed of by a designated agent who is not a third party service provider, POGO's Researcher Agreement and Policy #9.2.6 (*Retention, Return, and Destruction of Data*) identify the designated agent as the designated agent responsible for securely disposing of the records of personal health information; the responsibilities of the designated agent in securely disposing of the records; and the time frame within which, the circumstances in which and the conditions pursuant to which the records of personal health information must be securely disposed of. The policy and procedures also require the designated agent to provide a certificate of destruction:

- Identifying the records of personal health information to be securely disposed of;
- Confirming the secure disposal of the records of personal health information;
- Setting out the date, time, location, and method of secure disposal employed; and

- Bearing the name and signature of the agent(s) who performed the secure disposal.

Policy #9.2.6 (*Retention, Return, and Destruction of Data*) sets out the time frame within which, and the Privacy Officer as the agent to whom certificates of destruction will be provided following the secure disposal of the records of personal health information.

In the event that records of personal health information will be securely disposed of by an agent that is a third party service provider, the policy and procedures address the following additional matters.

Policy #9.2.19 (*Document Shredding*) and POGO's *Third Party Service Agreement* details the procedure to be followed by POGO in securely transferring the records of personal health information to the third party service provider for secure disposal. The policy and procedures identify the secure manner in which the records of personal health information will be transferred to the third party service provider, the conditions pursuant to which the records will be transferred and the agent(s) responsible for ensuring the secure transfer of the records. In this regard, the policy and procedures comply with Policy #9.2.19 (*Document Shredding*).

The policy and procedures also designates the Privacy Officer as the agent responsible for ensuring the secure transfer of records of personal health information to document the date, time and mode of transfer of the records of personal health information and to maintain a repository of written confirmations received from the third party service provider evidencing receipt of the records of personal health information. The Privacy Team maintains an inventory related to the records of personal health information transferred to the third party service provider for secure disposal.

In the course of POGO's 44 and 45 purposes, paper copies of electronic documents containing personal health information for review and analysis are created. As per Policy #9.2.19 (*Document Shredding* and Policy #9.2.28 *(Inventory of PHI Placed in Secure Gray Bin*), following analysis, the paper copies that are no longer required are placed in the secure bin in the secured POGONIS room until the third party service provider shreds the documents following the secure shredding protocol.

Further, where a third party service provider is retained to securely dispose of records of personal health information, the policy and procedures require that a written agreement be executed with the third party service provider containing the relevant language from Policy #9.1.11 (*Template Agreement for All Third Party Service Provider*), and identifies the Privacy Officer as the agent responsible for ensuring that the agreement has been executed prior to the transfer of records of personal health information for secure disposal.

Policy #9.2.6 *(Retention, Return, and Destruction of Data*) and Policy #9.2.19 (*Document Shredding*) also outline the procedure to be followed in tracking the dates that records of personal health information are transferred for secure disposal and the dates that certificates of destruction are received, whether from the third party service provider or from the researcher that is not a third party service provider, and the Privacy Team who are the agents responsible for conducting such tracking. Further, the policy and procedures outline the process to be followed where a certificate of destruction is not received within the time set out in the policy and its procedures or within the

time set out in the agreement with the third party service provider and the agents responsible for implementing this process.

The policy and procedures also address where certificates of destruction are retained and the Privacy Team as the agents responsible for retaining the certificates of destruction.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, set out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent or third party service provider breaches or believes there may have been a breach of these policies or their procedures.

9. Policy and Procedures Relating to Passwords

Policy #9.2.10 (*Password*) was developed and implemented with respect to passwords for authentication and passwords for access to information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by POGO.

The policy and procedures identify the required minimum and maximum length of the password, the standard mandated for password composition and any other restrictions imposed on passwords, such as re-use of prior passwords and the use of passwords that resemble prior passwords. Further, the policy stipulates that passwords must be comprised of a combination of upper and lower case letters as well as numbers and non-alphanumeric characters.

The time frame within which passwords will automatically expire, the frequency with which passwords must be changed, the consequences arising from a defined number of failed log-in attempts and the imposition of a mandatory system-wide password-protected screen saver after a defined period of inactivity are also addressed in Policy #9.2.10 (*Password*).

Policy #9.2.10 (*Password*) further identifies the administrative, technical and physical safeguards that must be implemented by agents in respect of passwords in order to ensure that the personal health information is protected against theft, loss and unauthorized use or disclosure and that the records of personal health information are protected against unauthorized copying, modification or disposal. Agents are required to keep their passwords private and secure and to change their passwords immediately if they suspect that their password has become known to any other individual, including another agent. Agents are also prohibited from writing down, displaying, revealing, hinting at, providing, sharing or otherwise making their password known to any other individual, including another agent of POGO.

POGO ensures that the policy and procedures it has developed in this regard are consistent with any orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation; with any guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario; and with evolving privacy and security standards and best practices.

POGO requires agents to comply with the policy and its procedures and addresses how, and by whom compliance will be enforced and the consequences of breach. The policy stipulates that compliance will be audited in accordance with the POGO's Privacy and Security Audit Program and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

10. Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs

POGO has developed and implemented Policy #9.2.3 (*Security Standards and Procedures*) for the creation, maintenance and ongoing review of system control and audit logs that are consistent with evolving industry standards and that are commensurate with the amount and sensitivity of the personal health information maintained, with the number and nature of agents with access to personal health information and with the threats and risks associated with the personal health information.

Policy# 9.2.3 (*Security Standards and Procedures)* require POGO to ensure that all information systems, technologies, applications and programs involving personal health information have the functionality to log access, use, modification and disclosure of personal health information.

Policy #9.2.3 (*Security Standards and Procedures*), and POGO's Privacy Program, Section 3.3 (*POGONIS Security Controls and Performance*) also set out the types of events that are required to be audited and the nature and scope of the information that must be contained in system control and audit logs. The system control and audit logs set out the date and time that personal health information is accessed; the date and time of the disconnection; the nature of the disconnection; the name of the user accessing personal health information; the network name or identification of the computer through which the connection is made; and the operations or actions that create, amend, delete or retrieve personal health information including the nature of the operation or action, the date and time of the operation or action, the name of the user that performed the action or operation and the changes to values, if any.

The Privacy Officer and the IT Team are responsible for ensuring that the types of events that are required to be audited are in fact audited and that the nature and scope of the information that is required to be contained in system control and audit logs is in fact logged.

Policy# 9.2.3 (*Security Standards and Procedures)* and POGO's Privacy Program , Section 3.3 (*POGONIS Security Controls and Performance*) require the system control and audit logs to be immutable, that is, POGO is required to ensure that the system control and audit logs cannot be accessed by unauthorized persons, amended or deleted in any way. Policy# 9.2.3 (*Security Standards and Procedures),* and POGO's Privacy Program, Section 3.3 (*POGONIS Security Controls and Performance*) also set out the procedures that must be implemented in this regard and the Privacy Officer and IT Team as the agents responsible for implementing these procedures.

POGO's Policy# 9.2.3 (*Security Standards and Procedures)*, POGO's Privacy Program , Section 3.3 (*POGONIS Security Controls and Performance*) also identify the length of time that system control and audit logs are required to be retained, the IT Team as responsible for retaining the system control and audit logs and where the system control and audit logs must be retained.

The review of system control and audit logs is also addressed, including the IT Team that is responsible for reviewing the system control and audit logs, the frequency with which and the circumstances in which system control and audit logs are required to be reviewed and the process to be followed in conducting the review.

The IT Team is responsible for reviewing system control and audit logs and are required to notify POGO, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) of an information security breach or suspected information security breach. The relationship between these two policies and their procedures is also identified.

Further, POGO's Policy# 9.2.3 (*Security Standards and Procedures)* addresses the findings arising from the review of system control and audit logs, including the Privacy Officer who is responsible for assigning other agent(s) to address the findings, for establishing timelines to address the findings, for addressing the findings and for monitoring and ensuring that the findings have been addressed.

POGO's Policy# 9.2.3 (*Security Standards and Procedures)* also sets out the nature of the documentation, if any, that must be completed, provided and/or executed following the review of system control and audit logs; the IT Team who are responsible for completing, providing and/or executing the documentation; the Privacy Officer to whom the documentation must be provided; the time frame within which the documentation must be provided; and the required content of the documentation.

The manner and format for communicating the findings of the review and how the findings have been or are being addressed is also outlined. This includes a discussion of the agent(s) responsible for communicating the findings of the review of system control and audit logs; the mechanism and format for communicating the findings of the review; the time frame within which the findings of the review will be communicated; and to whom the findings of the review are communicated.

Further, POGO's Policy #9.2.3 (*Security Standards and Procedures)* sets out the process to be followed in tracking that the findings of the review of system control and audit logs have been addressed within the identified timelines, including the IT Team who is responsible for tracking that the findings have been addressed.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

11. Policy and Procedures for Patch Management

Policy #9.2.13 (*Change Management*) outlines the procedures that have been developed and implemented for patch management.

The policy identifies the IT Team as responsible for monitoring the availability of patches on behalf of POGO, the frequency with which such monitoring must be conducted and the procedure that must be followed in this regard.

The IT Team who is responsible for analyzing the patch and making a determination as to whether or not the patch should be implemented is also identified. Policy #9.2.13 (*Change Management*) further discusses the process that must be followed and the criteria that must be considered by the IT Team when undertaking this analysis and making this determination. All critical security patches are implemented.

Policy #9.2.13 (*Change Management*) indicates in which circumstances patches will not be implemented. The policy and procedure requires the IT Team who are responsible for this determination, to document the description of the patch: the date that the patch became available; the severity level of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; and the rationale for the determination that the patch should not be implemented.

In circumstances where a determination is made that the patch should be implemented, Policy #9.2.13 (*Change Management*) identifies the IT Team as responsible for determining the time frame for implementation of the patch and the priority of the patch. The policy also sets out the criteria upon which these determinations are to be made, the process by which these determinations are to be made and the documentation that must be completed, provided and/or executed in this regard.

The policy also sets out the process for patch implementation, including the IT Team as the agents responsible for patch implementation and any documentation that must be completed, provided and/or executed by the agent(s) responsible for patch implementation.

The circumstances in which patches must be tested, the time frame within which patches must be tested, the procedure for testing and the IT Team who are responsible for testing are also addressed, including the documentation that must be completed, provided and/or executed by the IT Team.

Policy #9.2.13 (*Change Management*) also requires documentation to be maintained in respect of patches that have been implemented and identifies the IT Team who are responsible for maintaining this documentation. The documentation includes a description of the patch; the date that the patch became available; the severity level and priority of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; the date that the patch was implemented; the IT Team who are responsible for implementing the patch; the date, if any, when the patch was tested; the IT Team who are responsible for testing; and whether or not the testing was successful.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy also stipulates that compliance will be audited in accordance with the POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Policy #9.2.13 (*Change Management*) also requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) if an agent breaches or believes there may have been a breach of these policies or their procedures.

12. Policy and Procedures Related to Change Management

POGO Policy #9.2.13 (*Change Management*) was developed and implemented for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment of POGO.

This policy and its procedures identify the IT Team as responsible for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment and the process that must be followed and the requirements that must be satisfied in this regard. This includes a discussion of the documentation that must be completed, provided and/or executed; the

IT Team that is responsible for completing, providing and/or executing the documentation; the Privacy Officer as the agent to whom this documentation must be provided; and the required content of the documentation. The documentation describes the change requested, the rationale for the change, why the change is necessary and the impact of executing or not executing the change to the operational environment.

The criteria that must be considered by the IT Team who are responsible for determining whether to approve or deny a request for a change to the operational environment is also identified.

Policy #9.2.13 (*Change Management*) also sets out the manner in which the decision approving or denying the request for a change to the operational environment and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

If the request for a change to the operational environment is not approved, Policy #9.2.13 (*Change Management*) requires the IT Team to document the change to the operational environment requested, the name of the agent requesting the change, the date that the change was requested and the rationale for the determination that the change should not be implemented.

If the request for a change to the operational environment is approved, Policy #9.2.13 (*Change Management*) identifies the IT Team who is responsible for determining the time frame for implementation of the change, and the priority assigned to the change requested. Policy #9.2.13 (*Change Management*) also sets out the criteria upon which these determinations are to be made, the process by which these determinations are to be made and any documentation that must be completed, provided and/or executed in this regard.

Policy #9.2.13 (*Change Management*) also sets out the process for implementation of the change to the operational environment, including the IT Team as those agents responsible for implementation and any documentation that must be completed, provided and/or executed by the IT Team.

The circumstances in which changes to the operational environment must be tested, the time frame within which changes must be tested, the procedure for testing and the IT Team that is responsible for testing is also addressed in the policy and procedures, including the documentation that must be completed, provided and/or executed by the IT Team.

Policy #9.2.13 (*Change Management*) also requires documentation to be maintained of changes that have been implemented, and identifies the IT Team as responsible for maintaining this documentation. The documentation includes a description of the change requested; the name of the agent requesting the change; the date that the change was requested; the priority assigned to the change; the date that the change was implemented; the IT Team as responsible for implementing the change; the date, if any, when the change was tested; the IT Team as the agents responsible for testing; and whether or not the testing was successful.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Policy #9.2.13 (*Change Management*) policy also requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) if an agent breaches or believes there may have been a breach of these policies or their procedures.

13. Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information

POGO's Policy# 9.2.3 (*Security Standards and Procedures)* were developed and implemented and includes back-up and recovery of records of personal health information.

Policy# 9.2.3 (*Security Standards and Procedures)* and Policy #9.2.14 (*Back-up and Recovery of Records of Personal Health Information*) identify the nature and types of back-up storage devices maintained by POGO; the frequency with which records of personal health information are backed-up; the IT Team that is responsible for the back-up and recovery of records of personal health information; and the process that must be followed and the requirements that must be satisfied in this regard. This includes a discussion of any documentation that must be completed, provided and/or executed; the IT Team that is responsible for completing, providing and/or executing the documentation; the Senior Database Administrator to whom this documentation must be provided; and the required content of the documentation.

Policy# 9.2.3 (*Security Standards and Procedures)* and Policy #9.2.14 (*Back-up and Recovery of Records of Personal Health Information*) also address testing the procedure for back-up and recovery of records of personal health information, the IT Team that is responsible for testing, the frequency with which the procedure is tested and the process that must be followed in conducting such testing. This includes a discussion of any documentation that must be completed, provided and/or executed by the IT Team.

These documents further identify the IT Team as responsible for ensuring that back-up storage devices containing records of personal health information are retained in a secure manner, the location where they are required to be retained and the length of time that they are required to be retained. These documents, as well as POGO's Privacy Program, Section 3.3 (*POGONIS Security Controls and Performance*) require the backed-up records of personal health information to be retained and identifies that IT Team as responsible for ensuring that they are retained in a secure manner.

POGO does not contract a third-party service provider to retain backed-up records of PHI.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Policy# 9.2.3 (*Security Standards and Procedures)* and POGO's Policy #9.2.14 (*Back-up and Recovery of Records of Personal Health Information*) requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

14. Policy and Procedures on the Acceptable Use of Technology

POGO Policy #9.2.15 (*Acceptable Usage*) was developed and implemented, and outlines the acceptable use of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by POGO.

Policy #9.2.15 (*Acceptable Usage*) sets out the uses that are prohibited without exception, the uses that are permitted without exception and the uses that are permitted only with prior approval.

For those uses that are permitted only with prior approval, Policy #9.2.15 (*Acceptable Usage*) identifies the IT Team in consultation with the Privacy Officer as the agents responsible for receiving, reviewing and determining whether to approve or deny the request, and the process that must be followed, and the requirements that must be satisfied in this regard. This includes a discussion of any documentation that must be completed, provided and/or executed; the IT Team that is responsible for completing, providing and/or executing the documentation; the Privacy Officer as the agent to whom this documentation must be provided; and the required content of the documentation. The criteria that must be considered by the IT Team and Privacy Officer for determining whether to approve or deny the request are also identified.

Policy #9.2.15 (*Acceptable Usage*) also identifies the conditions or restrictions with which agents granted approval must comply.

The policy also sets out the manner in which the decision approving or denying the request and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Policy #9.2.15 (*Acceptable Usage*) also requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (Privacy *Breach and Incident Management*) and Policy #9.1.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

15. Policy and Procedures In Respect of Security Audits

POGO's Privacy Program Section 4 - Privacy and Security Audit Program, sets out the types of security audits that are required to be conducted. The audits currently conducted are: the assessment of compliance with security policies, procedures and practices implemented by POGO; security reviews or assessments; and reviews of system control and audit logs; threat and risk assessments; vulnerability assessments; penetration testing; and ethical hacks.

With respect to each security audit POGO's Privacy and Security Audit Program sets out the purposes of the security audit; the nature and scope of the security audit; the IT Team that is responsible for conducting the security audit; and the frequency with which and the circumstances in which each security audit is required to be conducted. In this regard, POGO's Privacy and Security Audit Program requires a security audit schedule which identifies the IT Team and Privacy Officer as the agent responsible for developing the security audit schedule.

For each type of security audit that is required to be conducted, POGO's Privacy and Security Audit Program sets out the process to be followed in conducting the audit. This includes the criteria to be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification will be provided. The policy further discusses the documentation that is completed, provided and/or executed in undertaking each security audit; the IT Team that is responsible for completing, providing and/or executing the documentation; the Privacy Officer as the agent to whom this documentation must be provided; and the required content of the documentation.

The role of the Privacy Officer, who has been delegated the day-to-day authority to manage the Privacy and Security Audit Program, is identified. The IT Team has been delegated the day-to-day responsibility for completing, providing and/or executing the security audits.

POGO's Privacy and Security Audit Program also sets out the process that must be followed in addressing the recommendations arising from security audits, including the Privacy Officer who is the agent responsible for assigning other agents to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations.

POGO's Privacy and Security Audit Program also sets out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the security audit, including the IT Team that is responsible for completing, providing and/or executing the documentation, the required content of the documentation and the Privacy Officer to whom the documentation must be provided.

The policy also addresses the manner and format in which the findings of security audits, including the recommendations arising from the security audits and the status of addressing the recommendations, are communicated. This includes a discussion of the agent(s) responsible for communicating the findings of the security audit; the mechanism and format for communicating the findings of the security audit; the time frame within which the findings of the security audit must be communicated; and to whom the findings of the security audit will be communicated, including the Chief Executive Officer.

POGO's Privacy and Security Audit Program further requires that a log be maintained of security audits and identifies the Privacy Officer and the IT Team as responsible for maintaining the log and for tracking that the recommendations arising from the security audits are addressed within the identified time frame. The logs further address where documentation related to security audits will be retained and that the Privacy Team is responsible for retaining this documentation.

POGO's Privacy and Security Audit Program also requires the IT Team who are responsible for conducting the security audit to notify POGO's Privacy Officer at the first reasonable opportunity, of an information security breach or suspected information security breach in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) or Policy #9.2.17 (*Information Security Incident Management Process*).

16. Log of Security Audits

POGO maintains a log of security audits that have been completed. The log sets out the nature and type of the security audit conducted; the date that the security audit was completed; the IT Team that is responsible for completing the security audit; the recommendations arising from the security audit; the IT Team in collaboration with the Privacy Officer who is responsible for addressing each recommendation; 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.

17. Policy and Procedures for Information Security Breach Management

POGO Policy #9.1.16 (*Privacy Breach and Incident* Management) and Policy #9.2.17 (*Information Security Incident Management Process*) address the identification, reporting, containment, notification, investigation and remediation of information security breaches, and provides a definition of the term "information security breach". At a minimum, an information security breach is defined as a contravention of the security policies, procedures or practices implemented by POGO.

POGO Policy #9.1.16 (*Privacy Breach and Incident* Management) and Policy #9.2.17 (*Information Security Incident Management Process*) impose a mandatory requirement on agents to notify POGO of an information security breach or suspected information security breach.

In this regard, the policy identifies the Privacy Officer as the agent who must be notified of the information security breach or suspected information security breach and provides contact

information for the Privacy Officer. The policy further stipulates the time frame within which notification must be provided, that notification must be provided verbally and in writing, and the nature of the information that must be provided upon notification. The policy also addresses the documentation that must be completed, provided and/or executed with respect to notification; the agent(s) responsible for completing, providing and/or executing the documentation; the Privacy Officer as the agent to whom this documentation must be provided; and the required content of the documentation.

Upon notification, Policy #9.1.16 (*Privacy Breach and Incident* Management) and Policy #9.2.17 (*Information Security Incident Management Process*) require a determination to be made of whether an information security breach has in fact occurred, and if so, what if any personal health information has been breached. A determination is further made of the extent of the information security breach and whether the breach is an information security breach or privacy breach or both. The Privacy Officer who is the agent responsible for making these determinations are also identified.

The policy and procedures address the process to be followed where the breach is a privacy breach as well as an information security breach and when the breach is reported as an information security breach but is determined to be a privacy breach.

The policy further addresses when senior management, including the Chief Executive Officer will be notified. This includes a discussion of the Privacy Officer who is the agent responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.

The policy also requires that containment be initiated immediately and identifies the Privacy Officer in collaboration with the IT Team as the agents responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the Privacy Officer and/or IT Team who are responsible for containing the breach and the required content of the documentation. In undertaking containment, the policy ensures that reasonable steps are taken in the circumstances to ensure that additional information security beaches cannot occur through the same means.

The Privacy Officer, and the IT Team, who are the agents responsible, and the process to be followed in reviewing the containment measures implemented and determining whether the information security breach has been effectively contained or whether further containment measures are necessary, are identified in the policy and procedures. POGO Policy #9.1.16 (*Privacy Breach and Incident* Management) and Policy #9.2.17 (*Information Security Incident Management Process*) also address any documentation that must be completed, provided and/or executed by the Privacy Officer and/or IT Team who are responsible for reviewing the containment measures; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy requires the health information custodian or other organization that disclosed the personal health information to POGO be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons

and whenever required pursuant to the agreement with the health information custodian or other organization.

In particular, POGO Policy #9.1.16 (*Privacy Breach and Incident* Management) and Policy #9.2.17 (*Information Security Incident Management Process*) sets out the Privacy Officer as the agent responsible for notifying the health information custodian or other organization, the format of the notification and the nature of the information that will be provided upon notification. The policy and procedures require the health information custodian or other organization to be advised of the extent of the information security breach; the nature of the personal health information at issue, if any; the measures implemented to contain the information security breach; and further actions that will be undertaken with respect to the information security breach, including investigation and remediation.

The policy also sets out whether any other persons or organizations must be notified of the information security breach and sets out the Privacy Officer as the agent responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification.

POGO Policy #9.1.16 (*Privacy Breach and Incident* Management) and Policy #9.2.17 (*Information Security Incident Management Process*) further identify the Privacy Officer as the agent responsible for investigating the information security breach, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the information security breach. This includes a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the Privacy Officer as the agent to whom this documentation must be provided; and the required content of the documentation. The role of the Privacy Officer that has been delegated day-to-day authority to manage the Privacy Program is also identified.

The policy also identifies the Privacy Officer as the agent responsible for assigning other agent(s) to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines. The policy also sets out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the information security breach, including the agent(s) responsible for completing, providing and/or executing the documentation; the Privacy Officer as the agent to whom the documentation must be provided; and the required content of the documentation.

POGO Policy #9.1.16 (*Privacy Breach and Incident* Management) and Policy #9.2.17 (*Information Security Incident Management Process*) also address the manner and format in which the findings of the investigation of the information security breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This includes a discussion of the agents responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the timeframe within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer.

Further, the policy requires that a log be maintained of information security breaches and identifies the Privacy Officer and the IT Team that is responsible for maintaining the log and for tracking that the recommendations arising from the investigation of information security breaches are addressed within the identified timelines. The policy further addresses where documentation related to the identification, reporting, containment, notification, investigation and remediation of information security breaches will be retained and the Privacy Team as the agents responsible for retaining this documentation.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

18. Log of Information Security Breaches

POGO maintains a log of information security breaches setting out:

- The date of the information security breach;
- The date that the information security breach was identified or suspected;
- The nature of the personal health information, if any, that was the subject matter of the information security breach and the nature and extent of the information security breach;
- The date that the information security breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to POGO was notified, if applicable;
- The date that the investigation of the information security breach was completed;
- The agent(s) responsible for conducting the investigation;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

Part 3 – Human Resources Documentation

1. Policy and Procedures for Privacy Training and Awareness

POGO has in place policies and procedures that require all POGO agents to attend an initial privacy orientation as well as ongoing privacy training.

Policy #9.3.1 (*Privacy and Security Training*) sets out the timeframe within which agents must complete their initial privacy orientation as well as the frequency for ongoing privacy training. The policy and procedures require agents to complete the initial privacy orientation within the first two weeks of their employment, contractual, or other relationship with POGO, prior to being given access to personal health information, and to attend ongoing privacy training provided by POGO on an annual basis.

The Privacy Officer is responsible for preparing and delivering the initial privacy orientation and ongoing privacy training. The policy and procedures also set out the process that is followed in notifying the Privacy Officer who is responsible for preparing and delivering the initial privacy orientation when an agent has commenced or will commence an employment, contractual, or other relationship with POGO. This also includes a discussion of the agents responsible for providing notification to the Privacy Officer, the time frame within which notification must be provided, and the format of the notification.

Policy #9.3.1 (*Privacy and Security Training*) also identifies the content of the initial privacy orientation to ensure that it is formalized and standardized. The policy and procedures require that the initial privacy orientation include:

- A description of the status of POGO under the *Act* and the duties and responsibilities that arise as a result of this status;
- A description of the nature of the personal health information collected and from whom this information is typically collected;
- An explanation of the purposes for which personal health information is collected and used and how this collection and use is permitted by the *Act* and its regulation;
- Limitations placed on access to and use of personal health information by agents;
- A description of the procedure that must be followed in the event that an agent is requested to disclose personal health information;
- An overview of the privacy policies, procedures, and practices that have been implemented by POGO, and the obligations arising from these policies, procedures, and practices;
- The consequences of breach of the privacy policies, procedures, and practices implemented;
- An explanation of the privacy program, including the key activities of the program and an explanation that the Privacy Officer has been delegated day-to-day authority to manage the privacy program;

- The administrative, technical, and physical safeguards implemented by POGO to protect personal health information against theft, loss, and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification, or disposal;
- The duties and responsibilities of the Privacy Team in implementing the administrative, technical, and physical safeguards put in place by POGO;
- A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute and the key provisions of the Confidentiality Agreement; and
- An explanation of Policy #9.1.16 (*Privacy Breach and Incident Management*) and the duties and responsibilities imposed on agents in identifying, reporting, containing, and participating in the investigation and remediation of privacy breaches.

Policy #9.3.1 (*Privacy and Security Training*) sets out that ongoing privacy training is formalized and standardized; includes role-based training in order to ensure that agents understand how to apply the privacy policies, procedures, and practices in their day-to-day employment, contractual or other responsibilities; and addresses any new privacy policies, procedures, and practices and significant amendments to existing privacy policies, procedures, and practices; and has regard to any recommendations with respect to privacy training made in privacy impact assessments, privacy audits, and the investigation of privacy breaches and privacy complaints.

The policy and procedures further set out that a log is maintained to track attendance at the initial privacy orientation as well as the ongoing privacy training, and identifies the Privacy Team as the agents responsible for maintaining the log and tracking attendance.

The policy and procedures also outline the process to be followed in tracking attendance at the initial privacy orientation as well as the ongoing privacy training, including the documentation that must be completed, provided, and/or executed to verify attendance; the Privacy Team as the agents responsible for completing, providing, and/or executing the documentation; and the required content of the documentation. The procedure to be followed by the Privacy Team in identifying the agent(s) who do not attend the initial privacy orientation or the ongoing privacy training, and for ensuring that such agent(s) attend the initial privacy orientation and the ongoing privacy training is also outlined, including the time frame following the date of the privacy orientation or the ongoing privacy training.

Documentation related to attendance at the initial privacy orientation and the ongoing privacy training is retained by the Privacy Team who is responsible for its retention.

The policy and procedures also discuss other mechanisms implemented by POGO to foster a culture of privacy and to raise awareness of the privacy program and the privacy policies, procedures, and practices implemented. The policy and procedures discuss the frequency with which POGO communicates with its agents in relation to privacy, the method and nature of the communication, and the Privacy Team who is responsible for the communication.

POGO requires agents to comply with the policy and its procedures and sets out that compliance will be enforced by the Privacy Officer, and also sets out the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program as well as Policy #9.1.15 (*Privacy Audits*) and sets out the frequency

with which the policy and procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with POGO's *Privacy and Data Security Code*, POGO's *Privacy and Data Security Procedures*, Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

This policy and its associated procedures are combined with Policy #9.3.1 (*Privacy and Security Training*).

2. Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training

The Privacy Team maintains a log of the attendance of agents at the initial privacy orientation and ongoing privacy training. The log sets out the name of the agent, the date that the agent attended the initial privacy orientation, and the dates that the agent attended ongoing privacy training.

3. Policy and Procedures for Security Training and Awareness

Policy #9.3.1 (*Privacy and Security Training*) requires agents of POGO to attend initial security orientation as well as ongoing security training.

The policy and procedures set out the time frame within which agents must complete the initial security orientation as well as address the frequency of ongoing security training. The policy and procedures require an agent to complete the initial security orientation prior to being given access to personal health information and to attend ongoing security training provided by POGO on an annual basis.

The Privacy Officer is the agent responsible for preparing and delivering the initial security orientation and ongoing security training. The policy and procedures further set out the process that must be followed in notifying the Privacy Officer who are responsible for preparing and delivering the initial security orientation when an agent has commenced or will commence an employment, contractual, or other relationship with POGO. This includes a discussion of the Privacy Team as the agents responsible for providing notification, the time frame within which notification must be provided, and the format of the notification.

The policy and procedures also identify the content of the initial security orientation to ensure that it is formalized and standardized. The initial security orientation includes:

- An overview of the security policies, procedures, and practices that have been implemented by POGO and the obligations arising from these policies, procedures, and practices;
- The consequences of breach of the security policies, procedures, and practices implemented;

- An explanation of the Security Program, including the key activities of the program and the Privacy Officer and the IT Team who are the agents that have been delegated day-to-day authority to manage the Security Program;
- The administrative, technical, and physical safeguards implemented by POGO to protect personal health information against theft, loss, and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification, or disposal;
- The duties and responsibilities of the Privacy Team together with the IT Team in implementing the administrative, technical, and physical safeguards put in place by POGO; and
- An explanation of Policy #9.1.16 (*Privacy Breach and Incident Management*) and the duties and responsibilities imposed on agents in identifying, reporting, containing, and participating in the investigation and remediation of information security breaches.

Policy #9.3.1 (*Privacy and Security Training*) also requires the ongoing security training to be formalized and standardized; to include role-based training in order to ensure that agents understand how to apply the security policies, procedures, and practices in their day-to-day employment, contractual, or other responsibilities; to address any new security policies, procedures, and practices and significant amendments to existing security policies, procedures, and practices; and to have regard to any recommendations with respect to security training made in privacy impact assessments, the investigation of information security breaches and the conduct of security audits including threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing, ethical hacks, and reviews of system control and audit logs.

The policy and procedures require that a log be maintained to track attendance at the initial security orientation as well as the ongoing security training and the policy and procedures identify the Privacy Team as the agents responsible for maintaining such a log and tracking attendance.

The process to be followed in tracking attendance at the initial security orientation as well as the ongoing security training is outlined, including the documentation that must be completed, provided, and/or executed to verify attendance; the Privacy Team as responsible for completing, providing, and/or executing the documentation; the agent to whom this documentation must be provided; and the required content of the documentation. The procedure to be followed and the Privacy Team who is responsible for identifying agent(s) who do not attend the initial security orientation or the ongoing security training and for ensuring that such agent(s) attend the initial security orientation and the ongoing security training is also identified, including the time frame following the date of the security orientation or the ongoing security training within which this procedure must be implemented.

The policy and procedures also outline that documentation related to attendance at the initial security orientation and the ongoing security training will be retained in POGO's secured central files and the Privacy Team is responsible for retaining this documentation.

The policy and procedures also discuss the other mechanisms implemented by POGO to raise awareness of the Security Program and the security policies, procedures, and practices implemented. The policy and procedures also discuss the frequency with which POGO

communicates with its agents in relation to information security, the method and nature of the communication, and the Privacy Officer as the agent responsible for the communication.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program as well as Policy #9.2.16 (*Security Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer together with the IT Team as the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

4. Log of Attendance at Initial Security Orientation and Ongoing Security Training

The Privacy Team maintains a log of the attendance of agents at the initial security orientation and ongoing security training. The log sets out the name of the agent, the date that the agent attended the initial security orientation, and the dates that the agent attended ongoing security training.

5. Policy and Procedures for the Execution of Confidentiality Agreements by Agents

POGO's *Privacy and Security Policies and Procedures (The Manual), Section 1 (Accountability), and* Policy #9.3.2 (*Confidentiality and Non-Disclosure Agreement*) require agents to execute a Confidentiality and Non-Disclosure Agreement in accordance with POGO's *Confidentiality Agreement Template* at the commencement of their employment, contractual, or other relationship with POGO prior to being given access to personal health information. This policy and procedures require that a Confidentiality Agreement be executed by agents, and on an annual basis, and identifies the time frame each year in which the Confidentiality Agreement is required to be executed.

The policy and procedures further identify the Privacy Team as the agents responsible for ensuring that a Confidentiality Agreement is executed with each agent of POGO at the commencement of the employment, contractual, or other relationship and thereafter on an annual basis and the process that must be followed in this regard.

In particular, the policy and procedures outline the process that must be followed in notifying the Privacy Officer each time an agent has commenced or will commence an employment, contractual, or other relationship with POGO. This includes a discussion of the agent(s) responsible for providing notification, the time frame within which notification must be provided, and the format of the notification.

The policy and procedures also outline the process that is followed by the Privacy Team in tracking the execution of Confidentiality Agreements, including the process that must be followed where an executed Confidentiality Agreement is not received within a defined period of time following the commencement of the employment, contractual, or other relationship or within a defined period of time following the date that the Confidentiality Agreement is required to be executed on an annual basis.

The policy and procedures require that a log be maintained of executed Confidentiality Agreements and identify the Privacy Team as the agents responsible for maintaining such a log. The policy and procedures also set out that documentation related to the execution of Confidentiality Agreements will be scanned and stored electronically in POGO's secured central files by the Privacy Team.

POGO requires agents to comply with the policy and its procedures and stipulates that the Privacy Officer enforces compliance, and the consequences of breaches. The policy and procedures also stipulate that compliance with the policy and its procedures and with the Confidentiality Agreement will be audited in accordance with POGO's Privacy and Audit Program which sets out the frequency with which the policy and its procedures will be audited and identifies the Privacy Officer as the agent responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify POGO at the first reasonable opportunity, in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

6. Template Confidentiality Agreement with Agents

A Confidentiality Agreement must be executed by each agent of POGO in accordance with Policy #9.3.2 (*Confidentiality and Non-Disclosure Agreement*) that addresses the matters set out below.

General Provisions

The Confidentiality and Non-Disclosure Agreement describes the status of POGO under the *Act* and the duties and responsibilities arising from this status. It also states that individuals executing the agreement are agents of POGO in respect of personal health information and outlines the responsibilities associated with this status.

The Confidentiality and Non-Disclosure Agreement also require agents to comply with the provisions of the *Act* and its regulation relating to POGO and with the terms of the Confidentiality and Non-Disclosure Agreement as may be amended from time to time.

Agents are also required to acknowledge that they have read, understood, and agree to comply with the privacy and security policies, procedures, and practices implemented by POGO and to comply with any privacy and security policies, procedures, and practices as may be implemented

or amended from time to time following the execution of the Confidentiality and Non-Disclosure Agreement.

The Confidentiality and Non-Disclosure Agreement also contains a definition of personal health information and the definition provided is consistent with the *Act* and its regulation.

Obligations with Respect to Collection, Use and Disclosure of Personal Health Information

The Confidentiality and Non-Disclosure Agreement identifies the purposes for which agents are permitted to collect, use, and disclose personal health information on behalf of POGO and any limitations, conditions, or restrictions imposed thereon.

In identifying the purposes for which agents are permitted to collect, use, or disclose personal health information, POGO ensures that each collection, use, or disclosure identified in the Confidentiality and Non-Disclosure Agreement is permitted by the *Act* and its regulation. In this regard, the Confidentiality and Non-Disclosure Agreement prohibits agents from collecting and using personal health information except as permitted in the Confidentiality and Non-Disclosure Agreement and from disclosing such information except as permitted in the Confidentiality and Non-Disclosure Agreement or as required by law.

Further, the Confidentiality and Non-Disclosure Agreement prohibits agents from collecting, using, or disclosing personal health information if other information will serve the purpose and from collecting, using, or disclosing more personal health information than is reasonably necessary to meet the purpose.

Termination of the Contractual, Employment or Other Relationship

The Confidentiality and Non-Disclosure Agreement require agents to securely return all property of POGO, including records of personal health information, and all identification cards, access cards, and/or keys, on or before the date of termination of the employment, contractual, or other relationship in accordance with Policy #9.3.4 (*Termination or Cessation of Employment or Contractual Relationship*). The Confidentiality and Non-Disclosure Agreement also stipulates the time frame within which the property of POGO must be securely returned, the secure manner in which the property must be returned, and the Privacy Team to whom the property must be securely returned.

Notification

The Confidentiality and Non-Disclosure Agreement require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) if the agent breaches or believes that there may have been a breach of the Confidentiality and Non-Disclosure Agreement, or if the agent breaches or believes that there may

have been a breach of the privacy or security policies, procedures, and practices implemented by POGO.

Consequences of Breach and Monitoring Compliance

The Confidentiality and Non-Disclosure Agreement outlines the consequences of breach of the agreement and addresses the manner in which compliance with the Confidentiality and Non-Disclosure Agreement will be enforced. The Confidentiality and Non-Disclosure Agreement further stipulates that compliance with the Confidentiality and Non-Disclosure Agreement will be audited and addresses the manner in which compliance will be audited.

7. Log of Executed Confidentiality Agreements with Agents

POGO maintains a log of Confidentiality and Non-Disclosure Agreements that have been executed by agents at the commencement of their employment, contractual, or other relationship with POGO and on an annual basis. The log includes the name of the agent, the date of commencement of the employment, contractual, or other relationship with POGO, and the dates that the Confidentiality and Non-Disclosure Agreements were executed.

8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program

Policy #9.3.3 (*Delegation of Roles and Responsibilities*) provides a job description for the position of Privacy Officer who has been delegated day-to-day authority to manage the privacy program on behalf of POGO has been developed.

The job description sets out the reporting relationship of the Privacy Officer who has been delegated day-to-day authority to manage the privacy program by the Chief Executive Officer. The job description identifies the responsibilities and obligations of the Privacy Officer in respect of the privacy program. These responsibilities and obligations include:

- Developing, implementing, reviewing, and amending privacy policies, procedures, and practices;
- Ensuring compliance with the privacy policies, procedures, and practices implemented;
- Ensuring transparency of the privacy policies, procedures, and practices implemented;
- Facilitating compliance with the *Act* and its regulation;
- Ensuring agents are aware of the *Act* and its regulation and their duties thereunder;
- Ensuring agents are aware of the privacy policies, procedures, and practices implemented by POGO and are also appropriately informed of their duties and obligations thereunder;
- Directing, delivering, or ensuring the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy;
  Conducting, reviewing, and approving privacy impact assessments;

- Receiving, documenting, tracking, investigating, remediating, and responding to privacy complaints pursuant to POGO's *Privacy and Security Policies and Procedures (the Manual)*- Principle #10 *(Challenging Compliance)*, and POGO Privacy Program, Section 7 (*Privacy Inquires, Challenges, and Complaints*);
- Receiving and responding to privacy inquiries pursuant to the Section 7 (*Privacy Inquires, Challenges, and Complaints*);
- Receiving, documenting, tracking, investigating, and remediating privacy breaches or suspected privacy breaches pursuant to Policy #9.1.16 (*Privacy Breach and Incident Management*); and
- Conducting privacy audits pursuant to Policy #9.2.16 (*Security Audits*).

9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program

A job description has been developed for the Privacy Officer and the IT Team who have been delegated day-to-day authority to manage the security program on behalf of POGO.

The job description sets out the reporting relationship of the Privacy Officer who has been delegated day-to-day authority to manage the Security Program by the Chief Executive Officer. The job description identifies the responsibilities and obligations of the Privacy Officer with respect to the Security Program. These responsibilities and obligations include:

- Developing, implementing, reviewing, and amending security policies, procedures, and practices together with the IT Team;
- Ensuring compliance with the security policies, procedures, and practices implemented together with the IT Team;
- Ensuring agents are aware of the security policies, procedures, and practices implemented by POGO and are appropriately informed of their duties and obligations thereunder together with the IT Team;
- Directing, delivering, or ensuring the delivery of the initial security orientation and the ongoing security training and fostering a culture of information security awareness together with the IT Team;
- Receiving, documenting, tracking, investigating, and remediating information security breaches or suspected information security breaches pursuant to Policy #9.1.16 (*Privacy Breach and Incident Management*); and
- Conducting security audits pursuant to POGO's Privacy and Security Audit Program together with the IT Team.

10. Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship

Policy #9.3.4 (*Termination or Cessation of employment of Contract*) requires agents, as well as their supervisors, to notify POGO of the termination of any employment, contractual, or other relationship. The policy and procedures identify the Privacy Team to whom notification must be

provided, the nature and format of the notification, the time frame within which notification must be provided, and the process that must be followed in providing notification.

The policy and its procedures also require agents to securely return all property of POGO on or before the date of termination of the employment, contractual, or other relationship. In this regard, a definition of property is provided in the policy and procedures and this definition includes records of personal health information, identification cards, access cards, and/or keys.

The policy and procedures identify the Privacy Team to whom the property must be securely returned; the secure method by which the property must be returned; the time frame within which the property must be securely returned; the documentation that must be completed, provided, and/or executed; the Privacy Team as the agents responsible for completing, providing, and/or executing the documentation; and the required content of the documentation. The procedures to be followed in the event that the property of POGO is not securely returned upon termination of the employment, contractual, or other relationship is also addressed, including the Privacy Team as the agents responsible for implementing the procedure and the time frame following termination within which the procedure must be implemented.

The policy and procedures also require that access to the premises of POGO, to locations within the premises where records of personal health information are retained, and to the information technology operational environment, be immediately terminated upon the cessation of the employment, contractual, or other relationship. The policy and procedures identify the Privacy and IT Teams as the agents responsible for terminating access; the procedure to be followed in terminating access; the time frame within which access must be terminated; the documentation that must be completed, provided, and/or executed and the Privacy Team that is responsible for completing, providing, and/or executing the documentation.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officer who is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.3.6 (*Disciplinary Action – Privacy Breach)* if an agent breaches or believes there may have been a breach of this policy or its procedures.

11. Policy and Procedures for Discipline and Corrective Action

POGO has in place a policy and associated procedure for discipline and corrective action in respect of personal health information.

POGO Policy #9.3.6 (*Disciplinary Action – Privacy Breach*) addresses the investigation of disciplinary matters, including the Privacy Officer who is responsible for conducting the investigation; the procedure that must be followed in undertaking the investigation; any documentation that must be completed, provided, and/or executed in undertaking the investigation; the Privacy Officer who is responsible for completing, providing, and/or executing the documentation; the required content of the documentation; and the Privacy Officer, the agent's Manager/Supervisor, and POGO's Chief Executive Officer to whom the results of the investigation must be reported.

The types of discipline that may be imposed by POGO and the factors that must be considered in determining the appropriate discipline and corrective action are also set out in the policy and procedures. The Privacy Officer, the agent's Manager/Supervisor and POGO's Chief Executive Officer are responsible for determining the appropriate discipline and corrective action, the procedure to be followed in making this determination, the agent(s) that must be consulted in making this determination; and the documentation that must be completed, provided, and/or executed, are also identified in Policy #9.3.6. Documentation regarding discipline and corrective action are retained in POGO's secure central files by the Privacy Team who is responsible for retaining the documentation.

Part 4 – Organizational and Other Documentation

1. Privacy and Security Governance and Accountability Framework

A Privacy and Security Governance and Accountability Framework, and POGO's Privacy Program has been established by POGO for ensuring compliance with the *Act* and its regulation, and for ensuring compliance with the privacy policies, procedures, and security-related practices implemented by POGO. POGO's Privacy Program includes POGO's *Privacy and Data Security Code and* POGO's *Privacy and Data Security Procedures (the Manual),* POGO's *Privacy and Security Governance and Accountability Framework*, POGO's Business Continuity and Disaster Recovery Plan; POGO's *Corporate Risk Management Framework*, and POGO's *Security Standards*.

POGO's Privacy Program stipulates that the Chief Executive Officer is ultimately accountable for ensuring that POGO and its agents comply with the *Act* and its regulation and comply with the privacy policies, procedures, and practices implemented.

The Privacy Officer is the agent who has been delegated day-to-day authority to manage POGO's Privacy and Security Program. The Privacy Officer is identified in POGO's Privacy Program which outlines the nature of the reporting relationship to the Chief Executive Officer. These documents also set out the responsibilities and obligations of the Privacy Officer and identify the other individuals and teams (i.e., the Data Security Committee, IT Team) that support the Privacy Officer.

POGO's Chief Executive Officer and/or delegate is accountable to the Board of Directors to whom privacy matters are reported. The Privacy Program is overseen by a Data Security Committee which is responsible to the Chief Executive Officer, which in turn, reports to the Board of Directors. POGO's Privacy Program sets out the frequency, and the method and manner by which the Board of Directors is updated with respect to the Privacy Program, the Privacy Officer who are responsible for providing such updates together with the Chief Executive Officer, and the matters with respect to which the Board of Directors is required to be updated. The Board of Directors is updated on an annual basis in a presentation format which is documented in POGO's minutes of the Board of Directors, and the training is logged in the applicable privacy training log.

The update provided to the Board of Directors addresses the initiatives undertaken by the Privacy Program, including privacy and security training and the development and implementation of privacy and security policies, procedures, and practices. It also includes a discussion of the privacy and security audits and privacy impact assessments conducted, including the results of, and recommendations arising from the privacy and security audits and privacy impact assessments and the status of implementation of the recommendations. The Board of Directors is also advised of any privacy or information security breaches and privacy complaints that were investigated, including the results of and any recommendations arising from these investigations, and the status of implementation of the recommendations.

POGO's Privacy Program, and its Privacy and Security Governance and Accountability Framework are accompanied by a privacy governance organizational chart.

These documents also set out the manner in which the Privacy Program will be communicated to agents of POGO, the method by which it will be communicated, and the Privacy Officer as the agents who are responsible for this communication.

2. Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program

POGO has established terms of reference for the Data Security Committee, Business Continuity and Disaster Recovery Teams, and the Audit, Finance and Risk Management Committee that have a role in respect of the Privacy and/or Security Program. For these committees, the terms of reference identify the membership of the committee, the chair of the committee, the mandate and responsibilities of the committee in respect of the privacy and/or the Security Program, and the frequency with which the committee meets. The terms of reference also set out to whom the committees report, the types of reports produced by the committees (if any); the format of the reports (if applicable), and to whom these reports are presented and the frequency of these reports

3. Corporate Risk Management Framework

POGO has in place 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.

The Corporate Risk Management Framework addresses the agent(s) responsible, and the process to be followed in identifying risks that may negatively affect the ability of POGO to protect the privacy of individuals whose personal health information is received, and to maintain the confidentiality of that information. This document also includes a discussion of the agents or other persons or organizations that must be consulted in identifying the risks; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

It also addresses the agent(s) responsible, the process that must be followed, and the criteria that must be considered in ranking the risks and assessing the likelihood of the risks occurring and the potential impact if they occur. This also includes a discussion of the agents or other persons or organizations that must be consulted in assessing and ranking the risks; the documentation that must be completed, provided and/or executed in assessing and ranking the risks; the documentation that must be completed, provided and/or executed in setting out the rationale for the assessment and ranking of the risks; the agent(s) responsible for completing, providing and/or executing the

documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The Corporate Risk Management Framework also identifies the agent(s) responsible, the process that must be followed, and the criteria that must be considered in identifying strategies to mitigate the actual or potential risks to privacy that were identified and assessed, the process for implementing the mitigation strategies, and the agents or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies.

This discussion also includes identifying the agent(s) responsible for assigning other agent(s) to implement the mitigation strategies, for establishing timelines to implement the mitigation strategies, and for monitoring and ensuring that the mitigation strategies have been implemented. The Corporate Risk Management Framework further addresses the documentation that must be completed, provided and/or executed in identifying, implementing, monitoring, and ensuring the implementation of the mitigation strategies; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The Corporate Risk Management Framework also addresses the manner and format in which the results of the corporate risk management process, including the identification and assessment of risks, the strategies to mitigate actual or potential risks to privacy, and the status of implementation of the mitigation strategies, are communicated and reported. This involves identifying the agent(s) responsible for communicating and reporting the results of the corporate risk management process, the nature and format of the communication; and to whom the results will be communicated and reported, including to the Chief Executive Officer. Approval and endorsement of the results of the risk management process, including the agent(s) responsible for approval and endorsement, is also outlined.

Further, the Corporate Risk Management Framework also ensures that a corporate risk register is maintained and that the corporate risk register is reviewed on an ongoing basis in order to ensure that all the risks that may negatively affect the ability of POGO to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information continue to be identified, assessed, and mitigated.

The frequency with which the corporate risk register is reviewed, the agent(s) responsible for its review, and the process that must be followed in reviewing and amending it is also identified.

The manner in which the Corporate Risk Management Framework is integrated into the policies, procedures and practices of POGO, and into the projects undertaken by POGO and the agent(s) responsible for integration, is also addressed.

4. Corporate Risk Register

POGO has developed and maintains a corporate risk register that identifies each risk that may negatively affect the ability of POGO to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. For each risk

identified, the corporate risk register includes an assessment of the risk, a ranking of the risk, the mitigation strategy to reduce the likelihood of the risk occurring and/or to reduce the impact of the risk if it does occur, the date that the mitigation strategy was implemented or is required to be implemented, and the agent(s) responsible for implementation of the mitigation strategy.

5. Policy and Procedures for Maintaining a Consolidated Log of Recommendations

POGO has developed and implemented Policy 9.4.6 (*Consolidated Log of Recommendations*) 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 consolidated and centralized log includes recommendations made by the Information and Privacy Commissioner of Ontario to be addressed by POGO prior to the next review of its practices and procedures.

The policy and procedures also set out the frequency with which, and the circumstances in which the consolidated and centralized log will be reviewed, the agent(s) responsible for reviewing and amending the log, and the process that must be followed in this regard. The log is updated each time that a privacy impact assessment, privacy audit, security audit, investigation of a privacy breach, investigation of a privacy complaint, investigation of an information security breach or review by the Information and Privacy Commissioner of Ontario is completed, and each time that a recommendation has been addressed. Further, the consolidated and centralized log is reviewed on an ongoing basis in order to ensure that the recommendations are addressed in a timely manner.

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. POGO's Privacy and Data Security Procedures, Policy #9.1.15 (*Privacy Audits*), and POGO's Privacy Program - Section 4, (POGO's *Privacy and Security Audit Program*) also stipulate that compliance will be audited in accordance with these documents, and sets out the frequency with which the policy and procedures will be audited and the Privacy Officer as the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures also requires that agents notify POGO at the first reasonable opportunity in accordance with Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

6. Consolidated Log of Recommendations

POGO has developed and maintains 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 Information and Privacy Commissioner of Ontario.

In particular, the log sets out the name and date of the document, investigation, audit and/or review from which the recommendation arose. For each recommendation, the log sets out the

recommendation made, the manner in which the recommendation was addressed or is proposed to be addressed, the date that the recommendation was addressed or by which it is required to be addressed, and the agent(s) responsible for addressing the recommendation.

7. Business Continuity and Disaster Recovery Plan

POGO has developed and implemented a Business Continuity and Disaster Recovery Plan and associated procedures to protect and ensure the continued availability of the information technology environment of POGO in the event of short and long-term business interruptions, and in the event of threats to the operating capabilities of POGO, including natural/environmental, and technical/man-made interruptions and threats.

The Business Continuity and Disaster Recovery Plan addresses notification of the interruption or threat, documentation of the interruption or threat, assessment of the severity of the interruption or threat, activation of the Business Continuity and Disaster Recovery Plan, and recovery of personal health information.

In relation to notification of the interruption or threat, the Business Continuity and Disaster Recovery Plan identifies the agent(s) as well as the other persons or organizations that must be notified of short and long-term business interruptions and threats to the operating capabilities of POGO and the agent(s) responsible for providing such notification. The Business Continuity and Disaster Recovery Plan also addresses the time frame within which notification must be provided, the manner and format of notification, the nature of the information that must be provided upon notification, and any documentation that must be completed, provided and/or executed.

In this regard, a contact list has been developed and maintained of all agents, POGO office building contacts, third-party service providers, stakeholders, and other persons or organizations that must be notified of business interruptions and threats. The Business Continuity and Disaster Recovery Plan identifies the agent(s) responsible for creating and maintaining this contact list.

In relation to the assessment of the severity level of the interruption or threat, the Business Continuity and Disaster Recovery Plan identifies the agents(s) responsible for the assessment, the criteria pursuant to which this assessment is to be made, and the agents and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat. Further, it addresses the documentation that must be completed, provided and/or executed resulting from or arising out of this assessment; the required content of the documentation; the agent(s) to whom the documentation must be provided; and to whom the results of this assessment must be reported.

In relation to the assessment of the interruption or threat, the Business Continuity and Disaster Recovery Plan sets out the agent(s) responsible and the process that must be followed in conducting an initial impact assessment of the interruption or threat, including its impact on the technical and physical infrastructure and business processes of POGO. This includes the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be utilized in conducting the assessment; the documentation that must be completed, provided and/or executed; the agent(s)

responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of the initial impact assessment must be communicated.

The Business Continuity and Disaster Recovery Plan further identifies the agent(s) responsible for conducting and preparing a detailed damage assessment in order to evaluate the extent of the damage caused by the threat or interruption and the expected effort required to resume, recover, and restore infrastructure elements, information systems, and/or services. It further addresses the manner in which the assessment is required to be conducted; the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied, and the criteria that must be considered in undertaking the assessment; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of the assessment must be communicated.

The Business Continuity and Disaster Recovery Plan also identifies the agent(s) responsible for resumption and recovery, the procedure that must be utilized in resumption and recovery for each critical application and business function, the prioritization of resumption and recovery activities, the criteria pursuant to which the prioritization of resumption and recovery activities is determined, and the recovery time objectives for critical applications. This includes a discussion of the agents and other persons or organizations that are required to be consulted with respect to resumption and recovery activities; the documentation that must be completed, provided and/or executed; the required content of the documentation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of these activities must be communicated.

In this regard, the Business Continuity and Disaster Recovery Plan requires that an inventory be developed and maintained of all critical applications and business functions and of all hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and network settings for firewalls, routers, domain name servers, email servers and the like. The Business Continuity and Disaster Recovery Plan further identifies the agent(s) responsible for developing and maintaining the inventory, the agent(s) and other persons and organizations that must be consulted in developing the inventory, and the criteria upon which the determination of critical applications and business functions must be made.

The procedure by which decisions made and actions taken during business interruptions and threats to the operating capabilities of POGO are documented and communicated and by whom and to whom they will be communicated is also be discussed.

The Business Continuity and Disaster Recovery Plan also addresses the testing, maintenance, and assessment of the Business Continuity and Disaster Recovery Plan. This includes identifying the frequency of testing; the agent(s) responsible for ensuring that the Business Continuity and Disaster Recovery Plan is tested, maintained, and assessed; the agent(s) responsible for amending the business continuity and discovery plan as a result of the testing; the procedure to be followed in testing, maintaining, assessing and amending the Business Continuity and Recovery Plan; and

the agent(s) responsible for approving the Business Continuity and Disaster Recovery Plan and any amendments thereto.

The Business Continuity and Disaster Recovery Plan further addresses the agent(s) responsible and the procedure to be followed in communicating the Business Continuity and Disaster Recovery plan to all agents, including any amendments thereto, and the method and nature of the communication. The agent(s) responsible for managing communications in relation to the threat or interruption are also identified, including the method and nature of the communication.

Part 1 – Privacy Indicators

<table>
<tr><th>Categories</th><th>Privacy Indicators</th><th>POGO-IPC Review (2019)</th></tr>
<tr><td rowspan="2">General Privacy Policies, Procedures and Practices</td><td>▪ The dates that the privacy policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.</td><td>
<table>
<tr><th>Date</th><th>Policies Reviewed (See Appendix 1: POGO Policy Numbers and Policy Titles)</th></tr>
<tr><td>June 2017</td><td>9.1.1</td></tr>
<tr><td>August 2017</td><td>9.1.7, 9.1.10</td></tr>
<tr><td>September 2017</td><td>9.1.1, 9.1.8, 9.1.9</td></tr>
<tr><td>November 2017</td><td>9.1.24</td></tr>
<tr><td>July 2018</td><td>9.1.6, 9.1.13, 9.3.1, 9.3.2</td></tr>
<tr><td>August 2018</td><td>9.1.1, 9.1.7, 9.1.8, 9.1.14, 9.1.16, 9.2.18</td></tr>
<tr><td>October 2018</td><td>9.1.5, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.15, 9.1.22</td></tr>
<tr><td>September 2018</td><td>9.3.26</td></tr>
<tr><td>October 2019</td><td>9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.7, 9.1.20, 9.3.3</td></tr>
</table>
</td></tr>
<tr><td>▪ Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure</td><td>
<table>
<tr><th>Policy #</th><th>Policy Document/Title</th><th>If yes, reason for and nature of amendments made</th></tr>
<tr><td>Privacy and Security document #1.7 and 1.8</td><td>Privacy and Data Security Code and its Procedures</td><td>POGO's Privacy and Security Code (10 Principles) was updated as a result of the review, i.e., adding text to clarify POGO's legal authority, amplify processes regarding Limited Collection, Limited Use, Disclosure and Retention, and Safeguards

Additional review in June 2018 after 2018 External Breach and additional processes for collection, use and disclosure for internal and external 44 and 45</td></tr>
</table>
</td></tr>
</table>

	amended, a brief description of the amendments made.				purposes and security enhancements were made. IPC notified of these changes on July 25, 2018
			9.1.1	Process for 44 and 45 Projects	Added de-identified and/or aggregate sections for research purposes; amended to meet IPC Comments (August 25, 2017); added text to clarify that this document refers readers to specific privacy documents and procedures; added text to clarify the process when a data request is received; added additional text re privacy breach and audits; added definitions of 45 and 44 from the Personal Health Information Protection Act, 2004 legislation; added legislative authority of 39(1)(c); added requirement that agents must comply with the policy and procedure; and added compliance and breach clause
			9.1.2	Review of Privacy and Security Policies and Procedures	Elaborated the procedure for amending the policy, elaborated the procedure for approving amendments; added that compliance will be audited in accordance with Policy #9.1.15 Privacy Audits; added how compliance is enforced and the consequences of a breach; added agents must comply with the policy and procedure and added compliance and breach clause
			9.1.3	Transparency of Privacy Policies, Procedures and Practices	Updated wording/phrases; added how compliance is enforced and the consequences of a breach; added requirement that agents must comply with the policy and procedure; and added compliance and breach clause
			9.1.4	Collection of Personal Health Information	Added criteria for collection approval (ensure that the collection is permitted by PHIPA and that any and all conditions or restrictions set out in PHIPA have been satisfied; ensure that de-identified and/or aggregate information will not serve the identified purpose; that no more PHI is being requested than is reasonably necessary to meet the identified purpose); included the manner in which the decision and the reasons for the decision are documented; included the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated; identified agents responsible for completing, providing or executing the documentation and/or agreements; identified agents responsible for ensuring that any conditions or restrictions that must be satisfied prior to the collection of PHI have in fact been satisfied; added agents must comply with the policy and procedure and added compliance and breach clause
			9.1.5	Data Holdings Containing Personal Health Information	Added legislative authority, and noted legislative or consent-based authority. Also edited in Appendix B of the Code; added agents must comply with the policy and procedure and added compliance and breach clause
			9.1.6	Levels of Access	Added agents must comply with the policy and procedure and added compliance and breach clause
			9.1.7	Use of Personal Health Information for Research	Amended to meet IPC Comments (August 25, 2017); Amended to remove Senior Advisor Policy and Clinical Affairs, removed reference to 'external' and amended text to meet the requirements of the Manual; added agents must comply with the policy and procedure and added compliance and breach clause

		9.1.8	Disclosure of Personal Health Information for Purposes Other Than Research	Edited to address IPC comments; Removed reference to discontinued Senior Advisor role, added text to more fully reflect the IPC Manual; added short description of the "content of the documentation" requirements for the POGO Data Request; elaborated on the requirements that must be satisfied and the criteria that must be considered by the agents responsible for determining whether to approve the request for the disclosure of personal health information for purposes other than research; added the requirement that agents must comply with the policy and procedure; and added compliance and breach clause
		9.1.9	Disclosure of Personal Health Information for Research Purposes and the Executive of Research Agreements	Amended to meet IPC Comments (August 25, 2017); Amended to ensure all sections of the Manual are appropriately addressed.
		9.1.10	Execution of Data Sharing Agreements	Amended to meet IPC Comments (August 25, 2017); amended to more closely reflect the requirements of the Manual; added agents must comply with the policy and procedure and added compliance and breach clause
		9.1.11	Template Agreement with Third Party Service Providers	Amended policy to comply with the Manual as applicable. Added legislative; added agents must comply with the policy and procedure and added compliance and breach clause
		9.1.12	Linkage of Records of Personal Health Information	Added legislative authority
		9.1.13	De-Identified and Aggregate Personal Health Information	Addition of legal authority; removal of reference to discontinued Linkage system; updated process re. secure network drive and restricted access to that drive
		9.1.14	Privacy Impact Assessment Process	Added legal authority, changed employee to agent, edited text for clarity, added fuller text re breach and confidentiality; added agents must comply with the policy and procedure and added compliance and breach clause
		9.1.24	Visitor Sign-In – Audit Program	Added responsibility of POGO Privacy Program and POGO Agents; revised definitions of agents and visitors; revised process
		9.2.28	Inventory of PHI documents in secure bin	It was recommended by IPC that an inventory be completed regarding documents containing PHI that are placed in POGO's secure bin in POGO's secure data room for secure disposal. The inventory includes: the name of the POGO data holding, whether or not the document contains POGONIS patient record-level data, or POGO Data Holding Patient Registration Form/Record, or Project Number, and Signature of the person placing the document in the bin.

<table>
<tr>
<td></td>
<td>▪ Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.</td>
<td>

Policy #9.1.24 POGO Visitor Sign in – Policy created as per 2016 IPC Recommendation. Policy includes: Legislative authority, updated visitor tracking procedure, new chart to assist POGO staff in identifying who is an agent and who is a visitor, process to identify, screen and supervise visitors and documentation requirements.
Policy #9.2.28 Inventory of PHI Documents in Secure Bin. – It was recommended that an inventory be completed regarding all documents containing PHI and placed in POGO's secure bin in POGO's secure data room. The inventory includes: the name of the data holding, indicate if the documents are a POGONIS Patient Record-level Data Analysis, or POGO Data Holding Patient Registration Form/Record, or Project Number, and Signature.

</td>
</tr>
<tr>
<td></td>
<td>▪ The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.</td>
<td>
<table>
<tr><th>Date</th><th>Nature of Communication</th></tr>
<tr><td>November 2017</td><td>Met with PHI users regarding new policy to maintain an inventory of PHI placed in the secured gray bin for secure disposal. (9.2.28).</td></tr>
<tr><td>1 December 2017</td><td>Directors updated on amendments made to Privacy policies and procedures at their Board of Directors meeting. (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).</td></tr>
<tr><td>15 June 2018</td><td>Data Managers privacy re-fresher training and policies and procedures updates. (9.1.1, 9.1.4, 9.1.7, 9.1.8, 9.1.9).</td></tr>
<tr><td>24 July 2018</td><td>Briefings with agents including senior management and the Board regarding changes to policies and procedures as a result of April 2018 privacy incident (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).</td></tr>
<tr><td>26 July 2018</td><td>Email to PHI users regarding security enhancements to privacy and security policies as a result of the April privacy incident (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).</td></tr>
<tr><td>30 July 2018</td><td>Briefings with agents including senior management and the Board regarding changes to policies and procedures as a result of April 2018 privacy incident (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).</td></tr>
</table>
</td>
</tr>
</table>

10 August 2018	Email to POGO staff regarding the new Visitor Sign-In- Policy (9.1.24).
27 August 2018	Briefings with agents including senior management and the Board regarding changes to policies and procedures as a result of April 2018 privacy incident (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
28 September 2018	Interlink Community Nurses privacy training and review of privacy/PHI procedures and amendments specific to Interlink practices (9.1.21, 9.2. 29, 9.4.12).
25 January 2019	Directors updated on amendments made to Privacy policies and procedures at their Board of Directors meeting having regard to changes as a result of the privacy incident(1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
25 January 2019	Email to staff regarding updates/edits to POGO Privacy and Security Code and its Procedures (1.7).
26 January 2019	Directors updated on amendments made to Privacy policies and procedures at their Board of Directors meeting (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
30 January 2019	Email to staff regarding edits/updates to POGO privacy and security policies and procedures posted in POGO Staff Policies folder (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
18 June 2019	Reviewed updated refresher privacy training at monthly POGO staff meeting and PowerPoint was sent via email for reference (9.3.1).
October 2019	Communication sent to staff concerning visitor sign in policy and visitor sign in chart of internal and external agents (9.1.24).
September 2019	Operations Group (management team) meeting and staff meeting: PIA, confidentiality agreement (revised), revised visitor sign-in, BCDR new and refresher (9.1.14, 9.1.24, 9.4.7).
September/October 2019	Lunch and Learn on BCDR Plan for new and current staff (9.4.7).
October 23, 2019	POGO Financial Administrative Program (POGO FAP) Administration Update – October 23, 2019 – Avoiding Breaches (9.1.16) Communication sent to POGO FAP staff concerning privacy breach management protocol of internal and external agents.

	▪ Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	▪ Yes, POGO's Privacy and Security Code (10 Principles) was updated as a result of the review, i.e., adding text to clarify POGO's legal authority, amplify processes regarding Limited Collection, Limited Use, Disclosure and Retention, and Safeguards. ▪ The revised Code is on the POGO'S website.
Collection	▪ The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.	▪ 7 data holdings: 1. POGONIS (Pediatric Oncology Group of Ontario Networked Information System); 2. POGO FAP (Pediatric Oncology Financial Assistance Program) Database (*name change from POFAP*); 3. Interlink Community Cancer Nurses Database; 4. SAVTI (Successful Academic Vocational Transition Initiative (SAVTI) 5. ACTS (After Care Treatment Summary) Database; 6. Satellite Database (NEW in 2018); 7. Aftercare Database.
	▪ The number of statements of purpose developed for data holdings containing personal health information.	▪ Each of the 7 data holdings has 1 statement of purpose each.
	▪ The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the Information and Privacy Commissioner of Ontario.	▪ Seven statements of purpose for the data holdings have been reviewed annually since the last IPC review (2016/17). o POGONIS (Pediatric Oncology Group of Ontario Networked Information System); o POGO FAP (Pediatric Oncology Financial Assistance Program) Database (*name change from POFAP*); o Interlink Community Cancer Nurses Database; o SAVTI (Successful Academic Vocational Transition Initiative (SAVTI) database; o ACTS (After Care Treatment Summary) Database; o Satellite Database (NEW in 2018); o Aftercare Database.

	▪ Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the review, and a list of the amended statements of purpose and, for each statement of purpose amended, brief description of the amendments made.	Yes, the POGO Financial Assistance Program (FAP) database statement of purpose was amended as a result of the review to clarify the purpose of the PIA regarding POGO's legislative authority to carry out the POGO Financial Assistance Program (FAP), and to demonstrate that POGO has identified and mitigated privacy risks associated with this consent-based program.
Use	▪ The number of agents granted approval to access and use personal health information for purposes other than research.	▪ POGO staff: 16 in 2017, 16 in 2018, 15 in 2019 ▪ 7 - POGONIS Data Managers for each year and 1 data clerk (2017 to 2019) ▪ 20 - POGO Financial Assistance Program (FAP) Database ▪ 6 - SAVTI Database ▪ 3 - (2018) and 22 (2019) (New) Satellite Database (pilot launched in Sept 2018) ▪ 6 - users of AfterCare database ▪ 31- users of ACTS database
	▪ The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy Commissioner of Ontario.	Total: 27 ▪ 27 requests have been received.
	▪ The number of requests for the use of personal health information for research purposes that were granted and that were denied since the prior review by the	▪ Total granted: 27 ▪ No requests have been denied.

	Information and Privacy Commissioner of Ontario.	
Disclosure	▪ The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario.	Total: 35 plus ACTS users (see Note below) ▪ 8– data requests (disclosures made under section 45 of *PHIPA*) ▪ 18 – ICES projects ▪ 3 - CCO ▪ 5 - CYP-C ▪ 1 - patient request <u>Note</u>: ▪ 31 - individual users of ACTS data for clinical use (from 2017 – 2019). POGO logs access to ACTS server by users but unable to log number of requests for the disclosures made at the institution level
	▪ The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 35 requests were granted (45 purposes PHI data disclosures) ▪ None were denied.
	▪ The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied since the prior review by the	Total: 39 were granted ▪ 26 were granted (disclosures made under section 44 of *PHIPA*) ▪ 13 - CYP-C research projects ▪ None were denied.

	Information and Privacy Commissioner of Ontario.	
	▪ The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the Information Privacy Commissioner of Ontario.	▪ 26 Research Agreements have been executed for the 26 requests ▪ For CYP-C research projects, no research agreements were executed by POGO as per the blanket data sharing agreement. POGO executes project permissions with CYP-C Management Committee and receives accompanying REB approvals and related documentation from CYP-C Management Committee.
	▪ The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes since the prior review by the Information and Privacy Commissioner of Ontario.	Total: 167 received ▪ 46 - requests received for aggregate information for other purposes ▪ 95 - requests received for disclosure of aggregate information for the hospital reports for other purposes ▪ 1 – request received for the disclosure of aggregate information for other purposes for the POGO surveillance report ▪ 16 - requests received for de-identified information for other purposes ▪ 6 – requests received for disclosure of de-identified information for research purposes ▪ 3 – requests received for disclosure of aggregate information for research purposes
	▪ The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes since the prior review by the Information and Privacy Commissioner of Ontario.	▪ There were 18 agents who use de-identified data and who sign a confidentiality agreement annually for other purposes - POGO staff ▪ There were 22 persons who received de-identified data and who signed the acknowledgement within the POGO Data Request form ▪ There were 49 persons who received aggregate data and who signed the acknowledgement within the POGO Data Request form ▪ There were 258 agents who may use aggregate data for POGO presentations and written materials and who sign a confidentiality agreement annually for other purposes - POGO Internal and External Agents ▪ There were 6 agents (44 research projects) who received de-identified data who signed researcher agreements which comply with all the research agreement provisions of the Manual

		▪ There were 3 agents (44 research projects) who received aggregate data who signed researcher agreements which comply with all the research agreement provisions of the Manual ▪ There were 125 total agents (non POGO staff) who participated in POGO's Provincial Pediatric Oncology Planning exercise in March 2017 where de-identified data was disclosed to working group members who signed confidentiality agreements, which were logged.
Data Sharing Agreements	▪ The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	▪ No new Data Sharing Agreements have been executed for the purposes of collection since the prior review by the IPC. ▪ There have been 0 amendments to Data Sharing Agreements executed for the collection of personal health information since the prior review.
	▪ The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	▪ No new Data Sharing Agreements executed for the disclosure of PHI since the prior review by the IPC. ▪ 1 Amendment executed for the disclosure of PHI since the prior review by the IPC: Institute for Clinical Evaluative Science (ICES). Amendments executed April 18, 2017
Agreements with Third Party Service Providers	▪ The number of agreements executed with third party service providers with access to personal health information since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 1 ▪ 1 agreement with third party service provider whose primary purpose is to perform forensic audit

<table>
<tr>
<td>Data Linkage</td>
<td>▪ The number and a list of data linkages approved since the prior review by the Information and Privacy Commissioner of Ontario.</td>
<td>▪ 34 (Based on numbers below)
o (31) CCO-Cancer Care Ontario; CCO-PET monthly linkage since November 2016;
o (3) CCO Exchange Data (Death Clearance and Second Cancers) (April 2017; July 2018; August 2019).</td>
</tr>
<tr>
<td>Privacy Impact Assessments</td>
<td>▪ The number and a list of privacy impact assessments completed since the prior review by the Information and Privacy Commissioner of Ontario and for each privacy impact assessment:
– The data holding, information system, technology or program,
– The date of completion of the privacy impact assessment,
– A brief description of each recommendation,
– The date each recommendation was addressed or is proposed to be addressed, and
– The manner in which each recommendation was addressed or is proposed to be addressed.</td>
<td>▪ 14 privacy impact assessments have been completed since the previous review:
Individuals (9PIAs)
<table>
<tr><th>Agent (Data Holding/ Program)</th><th>Date Completed PIA</th><th>Description of Recommendation</th><th>Date Addressed or Proposed</th><th>Manner Each Recommendation Addressed</th></tr>
<tr><td>[redacted] (POGONIS, Satellite, IT)</td><td>14-Mar-19</td><td>No recommendations for 2018 – new PIA.</td><td>14-Mar-19</td><td></td></tr>
<tr><td>[redacted] Education (Program)</td><td>28-Aug-19</td><td>New program assessment:
For onsite event photos add a disclaimer in event registration and provide options for manual photo removal</td><td>28-Aug-19</td><td>Education Program Manager updated the PIA and addressed the recommendations per the below:
1. Disclaimer included at registration in Waiver form providing explicit consent that was signed by participants.

Option for photo removal by participants:

Participants were advised via the Disclaimer that they can withdraw from any photograph by contacting
POGO’s Program Assistant, Communications and Education at her</td></tr>
</table>
</td>
</tr>
</table>

							POGO email for images to be removed and not used again at POGO.
		[redacted] **(POGO Financial Assistance Program (FAP)/ Provincial Coordinator**	24-Sep-19	1. Update name of program throughout PIA. 2. Clarify type of PHI and sensitive non-PHI collected. 3. Add to PIA the process for saving of Family letters and registrations in POGO networks.	24-Sep-19	Provincial Coordinator updated the PIA with new-processes as per below- 1. Updated name of program in the PIA, "POGO Financial Assistance Program" (POGO FAP). 2. Type of PHI and sensitive non-PHI collected, was clarified and added to the PIA. 3. Agent updated PIA to reflect the accurate process for saving of Family letters and registration forms in POGO networks.	
		[redacted] **(SAVTI)**	18-Oct-19	No recommendations for 2018 – new PIA.	18-Oct-19		
		[redacted] **(Associate Medical Director)/ POGONIS/ Satellite**	10-Oct-19	No recommendations for 2018 – new PIA	10-Oct-19		
		[redacted] **(Medical Director)/ POGONIS/ AfterCare**	8-Oct-19	Add access to de-identified CCO – POGONIS Registry Linkages data to the PIA.	8-Oct-19	Privacy Officer added Medical Director's access to the CCO-POGONIS Registry Linkages data to Medical Director's PIA and the policies and procedures re. security measures in place for the access.	
		[redacted] **(AA to CEO)/ Corporate**	10-Oct-19	No recommendations for 2018 – new PIA	10-Oct-19		
		[redacted] **(Senior Clinical Program Manager/ Satellite/**	October 2019	Clarify the following items in the PIA Health service utilization data for the satellite program: 1.	October 2019	October 2019, Senior Clinical Program Manager updated the PIA for Satellite Database as per below: For Health Service Utilization Data for Satellite Program:	

		AfterCare)		Clarified type of PHI and sensitive non-PHI collected 2. Reviewed new means of secure transfer via secure FTP server. Satellite Database: New web-based application, new as of October 2018: 1.Added type of PHI and sensitive non-PHI collected POGO Satellite Program Hospital Reporting activities of Non-PHI health service measures**:** 1. Added procedures for use and disclosure of De-identified centre data and aggregate patient data for presentations 2. Noted small cell data not included		1. Agent clarified type of PHI and sensitive non-PHI collected and was updated in the PIA. 2. Agent updated the means of secure transfer of Satellite data via secure FTP server and clarified to include health service utilization data for the satellite program network. FTP server has limited access and files are retained in secured data folders on POGO network system. PIA updated accordingly given processes were updated. For Satellite Database: New web-based application: 1. Agent clarified type of PHI and sensitive non-PHI collected and was updated in the PIA. Data reports include non-small cell data regarding number of new patients seen per satellite clinic, number of clinic visits, number of inpatient discharges and average length of stay. For POGO Satellite Program Hospital Reporting activities: 1. Procedures for the use and disclosure of de-identified centre data and aggregate patient data for presentations were clarified and updated in the PIA.	

							2. Use of de-identified general patient information for the purpose of making presentations to Satellite and Tertiary centres and informing decision making re: suitability of exceptional access to specialized care, i.e. patient diagnosis, treatment plans. 3. PIA clarified and included details re. type of data included in annual reports (de-identified small cell data may be included in the reports). Reference to POGO's small cell policies and procedures included in the PIA.	
				November 2018	Removal of HealthCare, Analytics Team from PIA for AfterCare database as no longer manages AfterCare database	November 2018	PIA was updated by removing name "HealthCare, Analytics Team" throughout AfterCare database PIA due to HealthCare, Analytics Team no longer manages AfterCare database.	
				October 2019	**AfterCare Program Data:** 1. Agent to Confirm procedures for use and disclosure of aggregate health service utilization data for presentations 2. Agent to note that small cell data not included	October 2019	October 2019, Senior Clinical Program Manager updated the PIA for AfterCare Database as per below: 1) a. Agent confirmed the use and disclosure of aggregate health service utilization data for presentations and updated in the PIA. b. Agent confirmed the use of de-identified general patient information for the purpose of making presentations to Tertiary AfterCare programs and informing decision making re: suitability of exceptional access to specialized care, i.e. patient diagnosis, treatment plans.	

						c. Agent confirmed all AfterCare Program health service utilization presentation data reported is retained in the POGO Dashboard folder (which does not contain PHI) in POGO central files and has limited access. 2) PIA clarified to indicate small cell data not included in any presentation or reports. Reference to POGO's small cell policies and procedures included in the PIA.
		[redacted] **(AA to Senior Clinical Program Manager/ Satellite/ Interlink)**	October 2019	Privacy recommended new PIA to be completed by Agent to reflect restructured role which includes the processes to calculate the following metrics: Health Service Utilization (HSU) Metrics - 1. New Patients Seen 2. Total Patients Seen 3. Ambulatory Visits 4. Number of Discharges 5. Inpatient Days 6. Average Length of Stay (in Days)	October 2019	PIA was updated to reflect a restructured role by Program Assistant. Satellite Database Privacy Impact Assessment and Threat and Risk Assessment completed.
		Programs/Initiatives (4)				

		Data Holding	Date PIA Complete	Description of Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed	
		POGO Financial Assistance Program (FAP)	14-Sep-18	1. Update mitigating strategy – FAP policy and procedures to use Family registration ID and not First name and Last Initial in all emails from FAP Data Managers to POGO in order to avoid breaches. 2. Include statement regarding process of storing hard copies of letter. 3. Given new FAP claims process, update PIA to address privacy and security measures. 4. Roll out program direct deposit claim payment from POGO to all other POGO centres - now active for [redacted].	14-Sep-18	POGO FAP Program Manager provided training and communication to Data Managers for new processes and also updated the FAP PIA as per below: 1. Prior to sending emails to POGO, POGO FAP Data Managers will no longer include First name and Last Initial of patients registered and will include Family Registration IDs only. 2. Statement regarding process of storing hard copies of letter is that no hard copies of the letters are kept. Letters are PDFed and saved on secure drive with limited staff access. 3. FAP claims process addresses privacy and security measures by claim amounts verified by health care professional which is indicated under hospital to ensure accuracy for payment. 4. Include new POGO Program direct deposit claim payment process at all active POGO centres ([redacted]).	
		S2S Workshops featured on OTN webcasts (SAVTI)	3-June-19	Email to be sent to participants making them aware that workshop will be livestreamed and recorded by OTN, including their comments	3-Jun-19	Program Assistant updated the processes and PIA as per below: Email/web registration communication to participants (privacy disclaimer included in email) Communication/web registration email	

		and/or stories.		sent to participants that included details that workshop was livestreamed and recorded by OTN, including participants comments and/or stories. POGO no longer features S2S Workshops on OTN webcasts and uses Zoom Health Care Conference instead. Further information on Zoom is available upon request.
POGO Hospital Reporting (POGONIS)	5-Feb-19	POGO will not disclose Pediatric Oncology identifiable PHI data from POGONIS to the hospital partners for the purposes of the project. Add Privacy Disclaimer on the Hospital Reports.	5-Feb-19	Senior Database Administrator updated the Reports to include Privacy Disclaimer and ensured each report did not contain identifiable PHI and only aggregate data disclosed. The PIA was updated accordingly. to include the below: POGO will not disclose Pediatric Oncology PHI data from POGONIS to the hospital partners for the purposes of the project by only disclosing the data in aggregated form. Privacy Disclaimer included in each report.

Data Holdings (1)

Data Holding	Date PIA Complete	Description of Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed
[redacted] **(Satellite Program Database) Satellite Program Database Web-Based Application**	1-Sept-18	IPC Recommendation to ensure PIA's meet all requirements as per the Manual	Nov-18	New Web-Based Application Satellite Database PIA and TRA completed by Privacy Officer and Program Manager in November 2018. IPC has requested PIA and TRA and Documentation has been included in IPC Comments Round 1 for review and approval.

	▪ The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion.	▪ There have been 0 privacy impact assessments undertaken but not completed since the prior review.
	▪ The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion.	▪ None

<table>
<tr>
<td></td>
<td>

- The number of determinations made since the prior review by the Information and Privacy Commissioner of Ontario that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.

</td>
<td>

- There have been 33 determinations where a privacy impact assessment is not required to be completed (11 programs per year over 3 years).

<table>
<tr><th>Data Holding, Information System, Technology or Program</th><th>Reasons for Determination</th></tr>
<tr><td>Fundraising</td><td>Data holdings, information systems, technologies or programs do not involve the collecting, use or disclosure of personal health information.</td></tr>
<tr><td>Finance</td><td>Same as above.</td></tr>
<tr><td>Human Resources</td><td>Same as above.</td></tr>
<tr><td>Research Granting Program</td><td>Same as above.</td></tr>
<tr><td>Strategic Project Initiatives</td><td>Same as above.</td></tr>
<tr><td>Student Summer Program</td><td>Same as above.</td></tr>
<tr><td>Communications</td><td>Same as above.</td></tr>
<tr><td>Guidelines Methodologist</td><td>Same as above.</td></tr>
<tr><td>Volunteer Program</td><td>Same as above.</td></tr>
<tr><td>Conference & Educational Events</td><td>Same as above.</td></tr>
<tr><td>Administration and Reception</td><td>Same as above.</td></tr>
</table>

</td>
</tr>
<tr>
<td></td>
<td>

- The number and a list of privacy impact assessments reviewed since the prior review by the Information and Privacy Commissioner and a brief description of any amendments made.

</td>
<td>

- There are **-33** privacy impact assessments that have been reviewed and amended since the previous review.

Individual (11PIAs)

<table>
<tr><th>Agent (Data Holding)</th><th>Description of Recommendation</th><th>Amendments Made</th></tr>
<tr><td>[redacted]
(POGONIS, ACTS, SAVTI, POGO FA Program, IT, Interlink, Data Management, IT)</td><td>2018 - Recommended changing Low to Medium Risk on some Business Process to Low Risk given Policies and Procedures in place</td><td>PIA updated by Database Administrator to modify risk level to low for the business process of extracting data and preparing datasets for researchers given privacy and security policies and procedures in place.</td></tr>
</table>

</td>
</tr>
</table>

			2019 – Update PIA to include new processes regarding secure transfer of PHI to researchers and external agents	PIA updated by Database Administrator to include: Details added regarding secure transfer of PHI to researchers and external agents include data is stored electronically on secure servers where the access is limited for pre-authorized people. Policies and Procedures (P/P) are in place to secure and protect the data by where the data is created and viewed, by whom, when and where it is stored, logs maintained and unique study ID's created. For researcher purposes, P/P are in place to govern the transferring of record level data.
		[redacted] **(IT)**	No recommendations for 2018	No recommendations for 2018.
			2019 – No changes from previous PIA, therefore no recommendations made.	No recommendations for 2019.
		[redacted] **(POGONIS, Research/Scientist)**	2018 – Update PIA to include new processes where Data is sent via secure means (secure FTP).	Researcher updated the PIA to include: Data sent via secure means by using FTP and includes privacy policies that are in place and information practices have been implemented. Data is only sent via secure means (Secure FTP). Individual level analysis files are created and used for project specific purposes with individual identifiers limited (if any) to requirements for each project.
			2019 – No changes from previous PIA, therefore no recommendations made.	No recommendations for 2019.
		[redacted] **(SAVTI)**	No recommendations for 2018.	No recommendations for 2018.
			2019 – Update PIA to include new processes for: 1. Entering client information and storing electronically – offsite	SAVTI Counsellor updated PIA to include: 1. When entering client information and storing electronically (offsite), new steps introduced upon entering database. This includes asking

				2. Communication on behalf of clients with other agencies and providers	the user if the user wants to "proceed" prior to any electronic files are displayed. 2. In order to communication on behalf of clients with other agencies and providers, a client will read, review and sign a consent form. The client understands what PHI will be collected, used and disclosed and that other agencies and providers will review their PHI.
			HealthCare Analytics Team (Research, Clinical Programs: Satellite, AfterCare, POGONIS, Atlas) [redacted] **(Senior Healthcare Analyst & Project Manager)**	2018 - Update PIA to include new processes related to aggregated data only in the central filing system and electronic filing system.	HealthCare Analyst updated PIA to include: HealthCare Analyst team have updated retaining of information in both the central and electronic filing system. Only aggregated data is stored in the central paper filing system and electronic filing system.
				2019 – Update PIA to include new processes for Satellite Health Service Utilization Data Analyses and Reporting has been removed from PIA.	Senior Healthcare Analyst is not involved in this process and does not have access to this information any longer therefore she removed this process from the PIA.
			[redacted] **(Healthcare & Guidelines, Administration and Reception)**	No recommendations for 2018.	No recommendations for 2018.
			[redacted] **(Database Developer, IT, POGONIS, POGO** [redacted] **Program, SAVTI Interlink, ACTS)**	2018 Update PIA to include new processes for: 1. System locks-up when keyboard/mouse idle time exceeded. 2. No web access – disabled. 3. Access to POGO FTP server is via an encrypted connection. POGO FA Program manager have a dedicated, password-protected logins.	Database Developer updated the PIA to include the below; 1. When the keyboard/mouse idle time has exceeded, the system will locks-up by external access to ACTS is via encrypted connection (using Secure Socket Layer). User-authentication required.. Access attempts are logged. Idle time limits are enforced, resulting in automatic session termination. Failed access attempts result in account lock-up. System locks-up when keyboard/mouse idle time limit exceeded. 2. There is no web access and it has been disabled by the mapping application is encrypted and password-protected. Mapping application resides on a server

					located behind POGO firewall on a server restricted and enforced by permissions and security policies. Web-based access disallowed. 3. Access to POGO FTP server is via an encrypted connection and the POGO FAP manager has a dedicated password-protected logins and this includes passwords being encrypted and password-protected, and sits behind POGO firewall, patient-identifying information and passwords are NOT communicated via email.
				2019 No changes from previous PIA, therefore no recommendations made	No recommendations made for 2019.
			[redacted] **(Data Management/IT)**	2019 Update PIA to include new processes: 1. Note access level to all POGO Data Holdings access 2. Update Mitigating Strategies for creation/analysis of record level data for analysis or research to current POGO Policies/Procedures in Place	Senior Database Administrator updated the PIA to include the below: 1. Added all POGO Data Holdings that agent has access to 2. Updated Mitigating strategies by removal of Linkage system and added Policies/Procedures that are in place to govern storage of paper copies and secure transfer of data.
			[redacted] **(Research)**	2019 No changes from previous PIA, therefore no recommendations made	No recommendations made for 2019.
			[redacted] **(POGONIS/ACTS/DATA Management/IT)**	2019 Update PIA to include new processes: 1. Viewing of ACTS Patient records Record-level, patient identifiers – All PHI, diagnostic, treatment and	Pediatric Oncology Analyst updated the PIA to include the below access privileges: 1. The viewing of ACTS patient record-level, patient identifiers which includes PHI within

			outcome information of patients within ACTS database. All PHI (first and last name, HC number, date of birth, postal code, diagnosis, etc.) 2. Viewing of AfterCare Patient records – Record-level data, patient identifiers. All PHI diagnostic, treatment and outcome information of patients within AfterCare databases. All PHI (first and last name, HC number, date of birth, postal code, diagnosis etc.) 3. Data transfer through FTP server – Record-level data patient identifiers – Patient ID, name, date of birth, postal code, diagnosis, date of diagnosis, etc. All PHI (first and last name, HC number, date of birth, postal code, diagnosis, etc). All PHI (first and last name, HC number, date of birth, postal code, diagnosis, etc).	ACTS database which is secured and agent has signed a confidentiality agreement. 2. The viewing of AfterCare Patient records – record-level data, patient identifiers, including all PHI within AfterCare databases which is secured, and agents signed a confidentiality agreement. 3. Data transfer through FTP server – Record-level data with patient identifiers which is secured, and agent signed a confidentiality agreement.
		[redacted] **(SAVTI)**	2019 Update PIA to include new process: Removed "Transfer of clients files from outside of Toronto for entry into database or statistics lists".	SAVTI Counsellor updated the PIA to remove the below: This is no longer necessary for the SAVTI Program given client information is no longer transferred using paper files to POGO from hospital based counselors for initial input into the database. SAVTI no longer sends paper files because they are currently uploaded into database and it is no longer necessary to send out paper files.

Research Projects (22)

Data Holding	Date PIA Complete	Description of Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed
Research Project 157	25-Nov-2016	Recommended adding unique study number to	22-Dec-2016	

			– **POGONIS Data Holding**		dataset as a mitigation strategy for reducing possible re-identification of individual		Researcher confirmed unique study number used in dataset as a mitigation strategy for reducing possible re-identification of the individual and PIA updated to add unique study number to dataset as a mitigation strategy for reducing possible re-identification of the individual. Updated PIA signed by PI.	
			Research Project 156 – POGONIS Data Holding	22-Feb-2017	No recommendations			
			Research Project 158 – POGONIS Data Holding	6-June-2017	No recommendations			
			Research Project 161 – POGONIS Data Holding	17-Aug-2017	No recommendations			
			Research Project 167 – POGONIS Data Holding	25-Aug-2017	Recommended: 1. Add PIs who will have access to PHI to PIA 2. Add date, time and location for destruction of data to PIA		1. Added PI with access to PHI by reason for access and qualifications. 2. Added date, time and location for destruction of data by date of destruction logged in POGO's PRU database for reference. Date entered (15 years from publication) time and location. Updated PIA signed by PI	

		Research Project 159 – POGONIS Data Holding	28-Aug-2017	To include additional data abstractor information to PIA	28-Aug-2017	Included additional data abstractor information by updating the project PIA and updated PIA signed by PI.	
		Research Project 118.1 – POGONIS Data Holding	11-Sept-17	No recommendations			
		Research Project 164 – POGONIS Data Holding	17-Oct-2017	No recommendations			
		Research Project 166 – POGONIS Data Holding	17-Oct-2017	1. Provide POGO with copy of the chart abstraction form noted in the PIA		As per POGO policies for 44 research project requirements, a copy of the chart abstraction form to POGO via email and POGO reviewed abstraction form to assess requested Patient data fields.	
		Research Project 168 – POGONIS Data Holding	28-Nov-2017	No recommendations			
		Research Project 165 – POGONIS Data Holding	28-May-18	No recommendations			
		Research Project 169 –	29-Jan-18	No recommendations			

		POGONIS Data Holding					
		Research Project 170 – POGONIS Data Holding	31- Jan-18	Add time of destruction of data to PIA	6-Feb-18	Researcher added time of destruction of data to PIA form and PI signed updated PIA form.	
		Research Project 171 (Part 1) – POGONIS Data Holding	4-Jul-18	No recommendations			
		Research Project 177 – POGONIS	10-Oct-18	No recommendations			
		Internal 45 Analysis Research Project – POGONIS	Feb -19	1. External PI and Research Coordinator will be required to sign POGO Confidentiality form. 2. Data will be transferred using secure POGO FTP. 3. External PI and Research Coordinator will be required to create secure folder to store data and set up limited access to the folders 4. POGO Privacy Officer will conduct audit at the end of the project	Feb-19	1. External PI and Research Coordinator signed POGO Confidentiality form 2. Data transferred using Secure POGO FTP 3. Coordinator created secure folder to store data and set up limited access to folders 4. POGO Privacy Officer will conduct audit at the end of the project	
		Research Project 171 (Part 2) – POGONIS	18-June-19	Add Programmer/ Biostatisticians who will have access to de identified dataset	18-Jun-19	PIA updated to included Programmer/ Biostatisticians who will obtain access to de-identified dataset. Updated PIA signed by PI.	

		Research Project 178 – POGONIS	1-Feb-19	No recommendations		
		Research Project 179 – POGONIS	19-Jul-19	No recommendations		
		Research Project – 180 – POGONIS	16-April-19	Given ongoing project, added new CO PIs to new PIA	16-Apr-19	New CO PIs added to PIA. Updated PIA signed by PI.
		Research Project 182 – POGONIS	18-Jul-19	No recommendations		
		Research Project 183 – POGONIS	2-Aug-19	No recommendations		

Privacy Audit Program

- The dates of audits of agents granted approval to access and use personal health information since the prior review by the Information and Privacy Commissioner of Ontario and for each audit conducted:
  4. A brief description of each recommendation made,
  5. The date each recommendation was addressed or is proposed to be addressed, and
  – The manner in which each recommendation was addressed or is

2017

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Internal Program Area Reviews				
FINANCE - POGO Financial Assistance Program (FAP) Direct Deposit - POGO wished to pay families directly as opposed to payment coming from hospitals. The benefit is that families associate	1. [redacted] -June 2016 2. [redacted] - Nov 2014 3. [redacted] - Oct 2017 4. [redacted]	1. Via letter, notify families that this change was going to occur 2. Collect banking info 3. Communicate with Program Administrators re the change 4. POGO Finance administered the change	1. [redacted] - Sept 2016 2. [redacted] - Feb 2015 3. [redacted] - Dec 2017 4. [redacted] - Oct 2018	1. Each family registered for the program was notified via letter of the changes in payment method. 2. POGO FAP Manager communicated with each family to obtain banking information 3. POGO FAP Manager communicated the change with each Hospital Program Administrator

	proposed to be addressed.	funds coming from POGO. Streamlines POGO financial process and process for families. 1. [redacted] families first to be paid directly from POGO 2. [redacted] brought on second 3. [redacted] brought on third 4. [redacted] currently being transitioned to POGO payment	- Apr 2018			4. POGO Finance Department updated internal financial processes to enable administration of the change in payment to families
		PPOP and Privacy – Audit the Redcap Survey developed for surveying [redacted] committee members	Jun-17	1. POGO to obtain license for REDCap software 2. Working group to Create a survey to ensure the privacy and security of member responses for working group. 3. The responses to survey should be anonymized and confidential, and should not be retained.	Jun-17	1. POGO purchased REDCap software to be used for surveys 2. PPOP Working Group lead worked with Privacy Team Administrative Assistant to create Red Cap survey tool. 3. Survey respondents notified that surveys would be anonymized and keep confidential 4. POGO Organizational Improvements committee to develop guidance documents regarding survey software to be used for confidential information at POGO (in development)

		POGO Financial Assistance Program (FAP) – Review/update Consent Form	Sep-17	1. POGO FAP to create a new/revised POGO Financial Assistance Program (FAP) Consent Form. 2. Update/replace current declaration, streamline and add new text in the "by completing this form, I understand' section. 3. POGO FAP Coordinator to communicate changes to the Consent form to the Hospital Program Administrators. 4. POGO FAP to use new consent form for all new families requesting registration in the program.	Jan-18	1. Privacy Officer worked with Provincial POGO Financial Assistance Program (FAP) Coordinator and Legal Counsel via in-person meetings, and teleconferences. 2. New Consent form created to include applicable changes to the POGO FAP consent form. 3. POGO Financial Assistance Program (FAP) Coordinator emailed all Hospital Program Administrators the new Consent forms to use. 4. Hospital Program Administrators provided new consent form to all new families registered in the program.
		POGO Financial Assistance Program (FAP) – Update POGO Financial Assistance Program (FAP) – PIA	Sep-17	Complete/update POGO Financial Assistance Program (FAP) - PIA to meet the requirements as per the IPC Manual.	Jan-18	POGO Privacy Officer worked with Provincial POGO Financial Assistance Coordinator and Legal Counsel by via in-person meetings and teleconferences to make applicable changes.

2017

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
External Privacy Compliance Reviews (10% of PRU Projects)				
[redacted] **et. al –** An updated comparison of two population-based pediatric cancer registries in Ontario (Project #165)	Jan-17	No recommendations made as no changes to the PIA were made and processes remain as indicated in PIA.	Jan-19	Audit letter sent to PI on January 24, 2019.

2018

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Internal Program Area Reviews				
POGONIS – Data/IT POGONIS logins for Satellite Application Server	Sep-18	Recommendations for Tertiary Centre Satellite Coordinators using new Satellite database: 1. No direct connection from Satellite centre computers to POGONIS database. 2. Limit connection time to POGONIS only when using patient search feature. 3. Limit connection type from Satellite application to	Oct-18	Recommendations addressed: 1. Satellite application is located in separate server from POGONIS server with strict user access and functionality. A simple view (read-only) was created in POGONIS to facilitate patient search look-up only by the Satellite application. 2. Satellite application disconnects from POGONIS immediately after patient look-up is completed. 3. POGONIS database does not accept external connections

				POGONIS application via internal POGO servers. 4. Limit access to the POGONIS patient file using temporary connection via the Satellite application. 5. Audit all activity - successful login and logout. 6. New Satellite database PIA and Threat and Risk assessment completed by Privacy Officer and Database Developer.		4. A simple view (read-only) was created in POGONIS to facilitate patient search look-up only by the Satellite application. 5. POGONIS maintains a log of all successful and unsuccessful attempt and these logs are reviewed bi-weekly by POGO Database Administrator. 6. Database Developer and Privacy Officer completed a PIA and Threat and Risk Assessment for the new Satellite Database.
		POGO Financial Assistance Program (FAP) i) Consent Form, ii) POGO Financial Assistance (FAP) Program PIA (NOTE; *REVISION/ UPDATES CONTINUED INTO 2018*)	Sep-17	1) Create new/revised POGO Financial Assistance Program (FAP) Consent Form. Replace current declarations, and streamline contents of consent form and add new text in the 'by completing this form, I understand' section. 2) Complete POGO Financial Assistance Program (FAP) PIA to meet the requirements as per the IPC Manual.	Jan-18	Recommendations addressed: 1) Privacy worked with Provincial Program Financial Assistance Coordinator and legal counsel (via in-person meetings, and teleconferences) to address recommendations by replacing current declarations, and streamline contents of consent form and add new text in the 'by completing this form, I understand' section. Provincial Program Financial Assistance Coordinator distributed the new consent form to the FAP Data Managers for use with families.2) Provincial Program Financial Assistance Coordinator updated FAP PIA to include the new consent version.
		SAVTI – Revise SAVTI Consent Form – Consent-based program	Jan-18	1) Expand section on 'I understand that…'; Update SAVTI Counsellors; Streamline Diagnostic Information section; Add 'I also agree (optional)	Feb-18	Recommendations addressed: 1) Privacy worked with Provincial SAVTI Coordinator and legal counsel to (via in-person meetings and teleconferences) to address recommendations by updating the SAVTI Consent Form to expand

				section; and add address and URL.		section on 'I understand that…' section; Update SAVTI Counsellors names and affiliations; streamline Diagnostic Information section; add 'I also agree…' (optional) section and add address and POGO website URL. Provincial SAVTI Coordinator distributed the new consent form to the other provincial SAVTI Counsellors for use with clients.
			Satellites – Edit/revise End User Agreement for New Satellite Database	Oct-18	1) Revise reference to privacy breach and add POGO to activate Policy #9.1.16 in the event of a breach.	Oct-18	Recommendations addressed: 1) Privacy Officer worked with Senior Clinical Program Manager to address recommendation by updating text in clause highlighting POGO's breach policy #9.1.16 and its procedure to notify the POGO Privacy Officers. Senior Clinical Program Manager to use this updated Satellite User Agreement for all new Satellite Database Users.

2018

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
External Privacy Compliance Reviews (10% of PRU Projects)				
[redacted] – Colorectal cancer screening in Childhood Survivors (Project #170)	22-Feb-19	1) PI recommended retaining the cohort dataset for seven years therefore PIA updated. 2) With regards to future manuscripts, recommended including the suggested POGO acknowledgment noted in the Researcher Agreement - Section 7.4.	22-Feb-10	Recommendations addressed: 1) Audit letter sent to PI on February 25, 2018 indicating agreed change for date of retention/destruction to August 2025. New date of destruction entered in POGO PRU database in the project file. 2) POGO Privacy Officers amended the Researcher Agreement, Section 7.4 to include POGO acknowledgement for use in all future manuscript produced by researcher who have been disclosed POGO data.

				Signed Researcher Agreement.		

2019

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Internal Program Area Reviews				
Interlink – Interlink Program	25-Jun-19	1. Reviewed which Interlink nurses use Iron Keys to transfer PHI information and other mobile devices. 2. Reviewed purpose of use. 3. Ensured Acceptable Usage form signed by Interlink Nurses.	25-Jun-19	Recommendations addressed: 1) Reviewed Iron Keys usage with Interlink Nurses at Privacy Training session on June 25, 2019. 2) Privacy Officer confirmed the purpose of the use with the applicable Interlink Nurse 3) Privacy Officer ensured the Acceptable Usage form was completed and signed accordingly.
POGO Financial Assistance Program (FAP) – Financial Assistance Program (FAP) [redacted] site	21-Mar-19	Audit conducted at site visit on March 24, 2018 by POGO Privacy Officer for 2 new [redacted] Haem/Onc Resource Navigators who will assist with POGO FAP program: 1. Confirmed the mandatory privacy and information security training received by the 2 new Resource Navigator positions at [redacted]. 2. Ensured secure office arrangements of 2 new staff. 3. Discussed process to maintain the privacy and confidentiality of family information when reviewing	4-Apr-19	1. Audit report generated by Privacy Officer for Provincial Coordinator, POGO FAP. 2. POGO Privacy training given May 21, 2019. 3. Access privileges removed on 23 Sept 2019 by POGO Database Developer. Database Developer also confirmed and removed access privileges for all individuals who no longer enter data into FAP database. 4. On March 21, 2019, reviewed process to be followed by Resource Navigator when families request access to their family file in the POGO FAP database. 5. POGO Privacy Officer and IT/System Analyst audited [redacted] external agents who have access to the POGO FAP database and removed one agent's access privileges.

				individual family files at their desk with family member present. 4. Scheduled POGO privacy training for 2 new staff. 5. Reviewed current listing of [redacted] staff who have access to POGO FAP database and removed access privileges for one SickKids staff.		
		SAVTI – Good documentation guidelines for POGO staff	2-Aug-19	Request received from law firm requesting SAVTI client information. It was noted that SAVTI client information held third party information (i.e. name of third party) that should have been titled as i.e. "Counsellor" and not name of "Counsellor". Privacy Office created a document for all POGO staff to create good documentation guidelines when taking notes on clients/patients of POGO.	2-Aug-19	1. Guideline reviewed by CEO on Sept 17, 2019 and sent out to SAVTI Provincial Coordinator on Sept 23, 2019. 2. Final Guidelines document completed November 14, 2019 and sent out to Provincial SAVTI Counsellors. Counsellors are using guidelines when documenting client visits.
		POGO Privacy website page	2-May-19	Updated POGO's Privacy brochure and POGO's Challenge and Inquiries website, specifically documenting new Associate Privacy Officer and updated POGO brand.	2-May-19	Brochure and website has been updated due to new Associate Privacy Officer hire and updated brand for POGO.
		Updated PIA Template	19-Sep-19	Updated PIA form with helpful links for staff use.	19-Sep-19	PIA form has been updated with helpful links for staff when filling out PIA's.
		2019:				

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
External Privacy Compliance Reviews (10% of PRU Projects)				
[redacted] SAVTI/ Transition to Meaningful Activity for Childhood Cancer Survivors: Understanding the Role of SAVTI (Project #85)	11-June-2019	Given Phase 2 of the project started, Privacy Officer recommended review of all PIAs, Consent Forms, Confidentiality Agreements of Research Team and REB re-approval letters.	18-June-2019	During privacy training session, PO requested all updated documentation for the project to be sent to POGO PO. PI submitted: 1. REB re-approval letters 2. Signed and updated PIA 3. Given it is a consent-required research project, all consent forms approved by REB at each SAVTI centre requested and filed 4. Confidentiality agreement obtained from PI
[redacted]. Genetic Contribution to the Development of Subsequent Malignant Neoplasms in Childhood Cancer Survivors: an Ontario Population-Based Nested Case-Control Study (Project #171)	3-June-2019	Given one PI and one Co-PI were relocating from Ontario prior to project completion, the following recommendations were made: 1. All PHI and sensitive data elements were de-identified and a de-identified data analysis file to be created 2. POGO Scientist to review SAS code to ensure no PHI or sensitive data present in code to be disclosed to PI and Co-PI 3. POGO Scientist and Senior Database Administrator & Privacy Officer to conduct final review of de-identified data analysis file	20-Aug-2019	Each recommendation addressed via meeting with PIs on June 3, 2019 and completed by 20-August 2019. 1. All PHI and sensitive data elements were de-identified and de-identified data analysis file created. 2. POGO Scientist reviewed SAS code to ensure no PHI or sensitive data present in code. 3. POGO Scientist and Senior Database Administrator & Privacy Officer conducted final review of de-identified data analysis file. 4. Ontario PI sign off on amended Researcher Agreement with new Schedule, amended PIA, and amended analysis process document on 18-June-2019. 5. REB amendment signed 29-May-2019 and forwarded to POGO on 18-June-2019. 6. PIA amended to include additional project team members and signed off by PI on 4-July-2019. 7. POGO IT transferred de-identified data analysis file via secure FTP process on August

				4. Remaining Ontario PI to sign off on amended Researcher Agreement with new Schedule, amended PIA, and amended analysis process document 5. REB amendment signed 29-May-2019 to be requested and filed at POGO. 6. Amend project PIA to include additional team members and have PI sign. 7. POGO IT to transfer de-identified data analysis file via secure FTP process. 8. Ensure Privacy receives confirmation from POGO Scientist that SAS code and 3 files reviewed and all PHI is de-identifed and saved in project folder. 9. Ensure Privacy receives confirmation that files securely sent using FTP and saved in project folder.		20, 2019 and on Sept 23, 2019. 8. Confirmation email received from POGO Scientist that SAS code was reviewed and de-identified files (3) reviewed and confirmed no PHI recorded in the SAS code and de-identified files. Email of 8-Aug-2019 saved in project folder. 9. Confirmation email received from POGO Database Administrator that files sent securely via FTP to non-Ontario PIs and saved in project file.	
		[redacted] Treatment Outcome of **Low** Grade Gliomas in Children (Project #180)	4- April-2019	Recommendations made: 1. Ensure all REB re-approvals are sent to POGO PO. 2. Add to PIA the additional data to be requested on cause of death.		1. REB approvals sent to POGO Office on 27-June-2019. 2. PIA updated to add the addition cause of death information required. PIA resigned by PI.	
	▪ The number and a list of all other privacy audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:	**2017: Other Privacy Audits** 2 Topic Reviews audits have been completed.					

– A description of the nature and type of audit conducted,
– The date of completion of the audit,
– A brief description of each recommendation made,
– The date each recommendation was addressed or is proposed to be addressed, and

▪ The manner in which each recommendation was addressed or is proposed to be addressed.

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Topic Reviews				
Privacy Program – Review and update Researcher Agreement to ensure up-to-date and compliant with PHIPA	Oct-17	Add new definitions, edit others definitions, add applicable policies, edit use and disclosure clauses, edit clauses re security and destruction, and edit report section re researcher requirements.	Nov-17	Privacy Team reviewed and updated the Researcher Agreement to include requirements of the IPC Manual as follows: 1. Edited and Included new definitions e.g. aggregate data; retention period. 2. Updated the researcher requirements for process for use and disclosure 3. Updated clauses for security and destruction
Data Request form updates – Revise POGO Data Request Form to require persons or organizations to which de-identified and/or aggregate information will be disclosed, to acknowledge and agree, in writing that that they will not use the information alone or with other information to identify an individual as per the Manual on page 24.	Mar-18	Edit Data Request Form to include the following statement and sign-off by researchers prior to data being released. "I/We will not use the de-identified and/or aggregate information provided by POGO, either alone or with other information, to identify an individual. I/We will not attempt to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge".	Mar-18	Recommendations addressed to meet IPC recommendation. Privacy Team and IT Team edited Data Request Form. Privacy Team reviewed and updated the Data Request form to meet the IPC recommendations by including: 1. The statement and sign-off feature for requesters to complete prior to data being releases on the Data Request form. 2. IT team implemented the change in the electronic Data request form and tested the new functionality of the form 3. Data Management/IT team retains all copies of the completed Data Request form in the project specific folder in the POGO network for Privacy team reference when requested.

2017: Other Privacy Audits

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Internal Privacy and Security Policies and Procedure Review				

(See section **General Privacy Policies, Procedures and Practices –** amendments made to existing privacy policies and procedures as a result of the review.)

2018: Other Privacy Audits

4 Topic Reviews audits have been completed.

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Topic Reviews				
Confidentiality Agreements Privacy Program – POGO Confidentiality Agreements	Nov-18	1. New CEO requested review of current Internal and External Confidentiality Agreements.	Jan-19	1. Privacy Team worked with POGO counsel to review and further edit and finalize the Internal and External Confidentiality Agreements.
Human Resources Database Privacy – Human Resources Database	Nov-18	1. HR to ensure new addition to database (to calculate employee's next change in vacation status) should maintain restricted/limited access to ensure security of data.	Nov-18	1. Recommendations addressed. HR and Privacy worked with POGO's Database Developer to ensure the changes were accurate and effective and restricted access maintained.

		Volunteer Committee Agreement Privacy – Development of an agreement for 'External Volunteer Committee Members'	Nov-18	1. Privacy to draft agreement to require committee members to understand and agree to maintain the security of information/data that may be shared at various POGO meetings.	Feb-19	1. Privacy Team drafted new Volunteer Committee Agreements, reviewed by Director, Finance and Administration and sign-off by CEO.	
		Relationship Agreement Privacy - Development of a Relationship Agreement to enable POGO to share quality indicator initiative proprietary information with APPHON	Nov-18	1. Privacy to draft new agreement that requires members to agree to ensure they maintain the security of information/data that may be shared at various POGO/APPHON meetings.	Feb-19	1. Recommendation addressed. Privacy Team drafted new agreement. Reviewed by Sr. Healthcare Analyst and Project Lead, Director Finance and Administration, and CEO, and finalized for implementation.	

2018: Other Privacy Audits

15 Internal Privacy and Security Policies and Procedure Reviews have been completed

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Internal Privacy and Security Policies and Procedure Review				
9.1.6 Levels of Access Audit Program	July-18	Add legislative authority text. Privacy Officer and IT team recommended post 2018 External Breach that	July-18	1. Privacy Team reviewed IPC Manual and changed the policy and procedure accordingly.

					POGO further strengthened a number of its security policies/procedures and controls regarding PHI to mitigate against similar incidents from occurring in the future. IT Team reviewed policies to ensure levels of access for all data remain applicable.			
			9.1.13 De-identified and Aggregate PHI Audit Program	July-18	Add legislative authority; remove reference to Linkage System no longer used; update process re. secure network drive and restrict access to S: drive.	July-18	1. Privacy Officer addressed by changing the policy and its procedures. 2. Sr. Database Administrator and IT Team reviewed new policy and procedure. 3. Privacy Officer communicated with POGO Internal Agents changes in policy.	
			9.1.1 Process for 44 and 45 Projects Audit Program	Aug-18	Add text to clarify this document 'refers readers to specific privacy documents and procedures, add text to clarify the process when a data request is received; add additional text re privacy breach and audits.	Aug-18	1. Privacy Team reviewed IPC Manual and changed the policy and its procedures accordingly. 2. Privacy Officer communicated with POGO Internal Agents changes in policy.	
			9.1.7 Use of PHI for Research Audit Program	Aug-18	Amend to remove Senior Advisor Policy and Clinical Affairs, remove reference to 'external', and amend text to include "Tracking Approved Uses of Person Health Information for Research" to further meet the requirements of the Manual.	Aug-18	1. Privacy Team reviewed IPC Manual and changed the policy and its procedures accordingly. 2. Privacy Officer communicated with POGO Internal Agents changes in policy.	

		9.1.8 Disclosure of PHI for Purposes Other Than Research Audit Program	Aug-18	Edit further to include "The Privacy Team tracks receipt of the executed written acknowledgments and are responsible for setting out the procedures that must be followed and the documentation that must be completed" to meet requirements of the IPC Manual.	Aug-18	1. Privacy Team reviewed IPC Manual and changed the policy and its procedures accordingly. 2. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.1.14 Privacy Impact Assessment Process Audit Program	Aug-18	Add legislative authority, change employee to agent, edit text for clarity, add fuller text re breach and confidentiality.	Aug-18	Privacy Officer updated policy by adding legislative authority which includes changing the name "employee" to the name "agent", edited for clarity of policy, added detailed text, specifically for breach and confidentiality in the policy. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.1.16 Privacy & Incident Management Audit Program	Aug-18	Add definition of agent, edit text and process for greater clarity.	Aug-18	Privacy Officer updated policy by adding definition of agent, edited text and process for greater clarity; added legislative authority; edited the steps and added detail regarding the process/steps involved with Discovery and Notification, Containment, Investigation, and Documentation; added requirement and detail re an Action Log, deleted Appendix A and edited the order in Flowcharts 1 and 2; deleted Flowchart 3. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.1.9 Disclosure of PHI for Research	Oct-18	Amend further to include additional requirements for the Review and Approval	Oct-18	Privacy Officer amended further in the policy to include additional requirements for the Review and Approval Process where the	

		Purposes & the Execution of Research Agreements Audit Program		Process where the Disclosure of PHI is permitted and where not permitted for research to ensure all sections of the Manual are appropriately addressed.		Disclosure of PHI is permitted and where not permitted for reach to ensure all sections of the Manual are appropriately. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.1.10 Execution of DSAs Audit Program	Oct-18	Amend further to list the POGO policies and procedures related to collection and disclosure to be reviewed prior to the execution of DSAs to more closely reflect the requirements of the IPC Manual.	Oct-18	Privacy Officer amended further in the policy to list the POGO policies and procedures related to collection and disclosure to be reviewed prior to the execution of DSA's to more closely reflect the requirements of the IPC Manual. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.1.11 Template for Agreements with Third Party Service Providers Audit Program	Oct-18	Amended to include additional requirements for secure disposal to further comply with the IPC Manual.	Oct-18	Privacy Officer amended in the policy to include additional requirements for secure disposal to further comply with the IPC Manual. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.1.5 Data Holdings Containing PHI Audit Program	Oct-18	Add legislative or consent-based authority text.	Oct-18	Privacy Officer amended in the policy and added legislative and consent based authority text and complied with the IPC manual. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.1.12 Linkage of Records of PHI Audit Program	Oct-18	Add legislative authority text.	Oct-18	Privacy Officer added legislative authority text in the policy and complied with the IPC Manual. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.1.22 POGO Financial Assistance Program (FAP)	Oct-18	Add authority is consent-based, change POFAP to 'the Program'.	Oct-18	Privacy Officer added authority that is consent-based in the policy, and changed the program name "POFAP" to "the Program".	

Audit Program				Privacy Officer communicated with POGO Internal Agents changes in policy.
Policy #9.3.4 Termination or Cessation of Employment or Contractual Relationship	July-2018	It was recommended by Privacy Officer and the CEO to review policies and procedures as a result of the external breach.	July-2018	Privacy Officer added to policy review of all devices, including USB keys at the end of employment and attestations. Privacy Officer communicated with POGO Internal Agents changes in policy. Privacy Officer reported amendments to the IPC on July 25, 2018 letter.
Policy # 9.3.1 Privacy and Security Training	July 2018	It was recommended by the Privacy Officer and CEO to review policies/procedures been as a result of the external breach.		Edited policy for 2016 review and once again in July 2018. Amendments reported to the IPC on July 25, 2018 letter. Privacy Officer communicated with POGO Internal Agents changes in policy. Privacy Officer edited policy for 2016 review and July 2018.

2019: Other Privacy Audits

6 Topic Review audits have been completed.

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Topic Reviews				
Researcher Agreement - Researcher Agreement for Project #179	10-Jun-19	Privacy Officer of PI's Organization [redacted] requested updates to POGO Researcher Agreement. POGO requested review by legal counsel. Legal counsel recommended updates and added definition (Process or processing); added to	4-Sep-19	Privacy Officer reviewed changes with lawyers on July 17, 2019. Research Agreement for Project #176 signed August 29, 2019. Privacy Officer updated 3.3 template. Researcher Agreement on September 4, 2019.

				section of privacy breach management and revised wording in Article 8, liability and indemnification. POGO Privacy Officer revised 3.3 Researcher Agreement template accordingly.			
		Privacy Website Policy – POGO Privacy Website	31-Jul-19	1. Updated and revised Privacy Website Policy for patients/clients. 2. Created Access and Request form for POGO Privacy Website.	31-Jul-19	1. Updated and revised Privacy Website Policy for patients/clients. 2. Created Access and Request form for POGO Privacy Website. 3. Communication Manager will communicate this update to POGO internal agents.	
		Consent Form to Use Photograph/ Video	28-Aug-19	Updated consent from and added client can withdraw at any time and remove photo from POGO.	28-Aug-19	Updated consent form and added client can withdraw at any time and remove photo from POGO.	
		Confidentiality Agreements – Privacy Program – POGO Confidentiality Agreements	Nov-18	1. Amendments requested of Internal and External Confidentiality Agreement by new CEO. 2. Privacy Officer drafted modified structure and provided to legal counsel for review and comment to ensure compliance with PHIPA regulations. 3. For Internal agents Confidentiality Agreement, review required of definition of Confidential Information. 4. For External agent Confidentiality Agreement, "duty of confidence" amended to require external	18-Sep-19	Final version approved by CEO on Sept 18, 2019. New Internal Agreement discussed with staff at Staff Meeting on September 17, 2019.	

				agent's compliance with specific POGO policies as referenced in the POGO's privacy code (link provided to POGO website) but not POGO procedures.		
		Committee Participation Agreements – Privacy Program/Organizational Improvements – Committee Participation Agreements	Mar-19	1. Privacy Officer drafted Committee Participation Agreement as requested by new CEO to be used for all stakeholders who are not agents but participate in POGO. Committee and their work 2. Consulted with CCO regarding their Volunteer Participation Agreement. 3. Ensured all applicable laws FIPPA and PHIPA included in agreement as well as definition of Confidential Information and reference to POGO Privacy and Security Code.	Not completed - ongoing review by Operation Committee to be completed by Dec 2019	1. Initial review with POGO Senior Executive on Mar 14, 2019 and updates made accordingly. 2. Second review on June 11, 2019 and updates made accordingly. 3. Presentation to the Operations Committee on August 13, 2019 requesting review and comment to be provided by Sept 30, 2019. 4. Once consolidated review received, final approval by CEO and then each POGO Committee Chair will circulate to their POGO Committee Members for review and signage.
		MSUR (Satellite) – Satellite Program Database/Member Site User Registration	22-Aug-18	PO initial review to ensure the MSUR complies to PHIPA 2004 requirements as it applies to new Satellite Program Database features and to be signed as Satellite database users Confidentiality Agreement. Review required by Satellite Database Project Team. Final review of MSUR by PO once Satellite Program database upgrade completed.	20-Sep-19	POGO Senior Clinical Program Manager and Program Assistant notified MSUR has been finalized. Distribution to Satellite Site Database Users for review and signage will be completed by POGO Senior Clinical Program Manager. Privacy Team will received completed forms and log according to IPC requirements.

2019 : Other Privacy Audits

10 Internal Privacy and Security Policies and Procedure Review has been completed.

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Internal Privacy and Security Policies and Procedure Review				
Policy #9.3.26 Working Remotely Policy – formerly Working Remotely, currently "Remote Access"	23-Jul-19	1. Privacy Officer and HR Manager to draft a new and separated Flexible Work Arrangements policy with a recommended link to Policy #9.3.26. 2. Privacy Officer changed name for policy to Remote Access to comply with IPC Manual recommendations. 3. CEO recommended review of policy by Privacy Officer to remove references to Flexible working arrangements and to strictly adhere to remote access policy, procedures and practices.	23-Sep-19	1. Flexible Work Arrangements policy drafted by Privacy and HR 2. Privacy edited title from "Remote Working Guidelines" to "Remote Access" as per the recommendation of the IPC Manual. 3. Removed all references to "flexible work arrangements: and only included "remote access". Privacy Officer communicated with POGO Internal Agents changes in policy.
Policy #9.1.16 Privacy Breach and Incident Management	June 2019	1. CEO recommended Privacy Officer to re-format structure of the policy; enhance agent definitions; modify flowchart.	Still in draft	1. Privacy Officer made revisions as per CEO recommendations. Awaiting final approval by CEO.

		Privacy and Security Training Presentation	April 2019	1. Given new position of Associate Privacy Officer at POGO, the Privacy Officer recommended the new Associate Privacy Officer review and recommend updates to the Privacy and Security Training presentation slides.	June 2019	1. Privacy presentation updated inclusion of required components completed April 2019. 2. Privacy Officer and CEO approved revisions to the Privacy and Security Training Presentation in June 2019.
		Policy #9.3.3 Delegation of Roles and Responsibilities	October 2019	1. Privacy Officer recommended review of roles given changes to POGO staff and roles.	October 2019	1. Privacy Officer reviewed and edited policy. Privacy Officer communicated with POGO Internal Agents changes in policy.
		Privacy documents #1.7 and #1.8 Privacy and Data Security Code and Procedures	October 2019	1. Recommended by the Privacy Officer to review the Privacy and Data Security Code and its procedures to ensure up to date processes for collection, use and disclosure in place.	October 2019	1. Privacy Officer reviewed and edited the Privacy and Data Security Code and its procedures.
Privacy Breaches	▪ The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	▪ There have been 22 notification of privacy breaches or suspected privacy breaches since the prior review.				

	▪ With respect to each privacy breach or suspected privacy breach: – The date that the notification was received, – The extent of the privacy breach or suspected privacy breach, – Whether it was internal or external, – The nature and extent of personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the health information custodians or any other organizations, – The date that the investigation was commenced. The date that the investigation was completed, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and	▪ Please see table below.

	– The manner in which each recommendation was addressed or is proposed to be addressed.	

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
27-Jan-17	1 email containing PHI sent to 2 recipients on 27-Jan-17.	Internal	Patient information (PHI)	N/A	Double delete all copies of the email.	27-Jan-17	27-Jan-17	27-Jan-17	8-Feb-17	All agents permanently deleted all copies of email and were informed of POGO policy. All agents sent a privacy presentation for reference.
8-Feb-17	1 email containing PHI sent to 40 recipients.	Internal	Patient information (PHI)	N/A	All copies of the email have been double deleted.	8-Feb-17	8-Feb-17	8-Feb-17	8-Feb-17	All agents permanently deleted all copies of email and were informed of POGO policy. All agents sent a privacy policy reminder for reference.
19-Apr-18	[redacted] x POGO	External	Patient information (PHI)	19-Apr-18	PHI – POGO Data – complete hard drive wipe from [redacted] and an erase method was used. The method was supervised by the [redacted] Desktop Support Analyst and Supervisor.	13-Aug-18	19-Apr-18	19-Apr-18 to 13-Aug-18	May 2018	POGO CEO, Privacy Officer and POGO IT reviewed existing privacy and security policies and processes for potential update as follows: 1) Departing employees will be required to execute an additional confidentiality undertaking an attestation that confirms they do not have any PHI

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
					Data Security Firm retained – 3rd party forensic to obtain USB keys and perform the forensic audit work on personal laptop and USB keys. Data Security Firm completed their investigation with confidence that the files were contained and no further access, duplication or dissemination beyond [redacted] and personal laptop and USB keys. Secure deletion was completed on July 4, 2018. Affidavit from agent has been received.					in their possession and that they have returned all POGO data that was in their possession. 2) Regarding access to secure file storage drives and monitoring user behavior with respect to PHI file storage, POGO has a) Completed decommissioning of our former model of file storage for research ("Linkage System"). All research folders (PHI files) are now located on a secure storage server with limited access b) Blocked ability to use USB and other external storage devices for those with access to PHI c) Reviewed and enhanced access restrictions to PHI files in our dedicated network drive containing PHI files d) Disabled accessing home computer local drive from POGO Remote Desktop Connection

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
										session and has disabled copying and pasting of documents from POGO network to home computer for all PHI users. e) Continued to monitor researcher computers on a quarterly basis by the Privacy Officer or IT designate 4) Employee privacy training reviewed and updated as follows: a) All new employees receive privacy training within two days of their employment start date. All employees receive annual privacy training. b) POGO Privacy Officer completed additional training with agents who have access to PHI between July 24, 2018 and July 26, 2018 to review. c) POGO Privacy Officer reviewed data security information/update at POGO Staff meeting on July 17, 2018

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressedor Proposed Manner
28-Jun-18	1 email containing patient name and number sent to 1 recipient on June 28 2018.	Internal	Patient information (PHI)	N/A	All copies of the email have been double deleted.	28-June-18	N/A	28-Jun-18	28-Jun-18	All agents permanently deleted all copies of email.
20-Aug-18	1 email containing name of deceased patient sent to 1 recipient on 20-Aug-18.	Internal	Patient information (PHI)	N/A	All copies of the email have been double deleted.	20-Aug-18	N/A	20-Aug-18	20-Aug-18	All agents permanently deleted all copies of email.
24-Sep-18	1 email containing POGO Family number, full patient name and relapse date sent to I recipient on 24-Sep-18.	Internal	Patient information (PHI)	N/A	All copies of the email have been double deleted.	24-Sep-18	N/A	24-Sep-18	24-Sep-18	All agents permanently deleted all copies of email.
9-Nov-18	1 email containing patient information including name and financial assistance registration information sent to 3	Internal	Patient information (PHI)	NA.	All copies of the email have been double deleted.	7-Nov-18	N/A	7-Nov-18	7-Nov-17	All agents involved permanently deleted all copies of email.

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressedor Proposed Manner
	recipients on 7-Nov-18.									
17-Dec-18	2 emails containing PHI sent to 1 recipient on 17-Dec-18.	Internal	Patient information (PHI)	N/A	All copies of the email have been double deleted.	17-18-Dec-18	N/A	18-Dec-18	17-18-Dec-18	All agents involved permanently deleted all copies of email.
18-Dec-18	1 email containing PHI sent to 1 recipient on 18-Dec-18.	Internal	Patient information (PHI)	N/A	All copies of the email have been double deleted.	18-Dec-18	N/A	18-Dec-18	18-Dec-18	All agents involved permanently deleted all copies of email.
9-Jan-19	Agenda containing PHI sent via email to POGO Provincial Pediatric NeuroOncology Clinical Rounds attendees.	Internal	Patient information (PHI)	10-Jan-2019	All copies of both emails have been double deleted from sender and all recipients.	9-Jan-19	N/A	9-Jan-19	10-Jan-2019 23-Jan-2019	All agents involved permanently deleted all copies of email. Investigation regarding using [redacted] FTP for sending agendas were discussed with [redacted] NeuroOnc Oncologist - Chair of NeuroOnc rounds As of October 2019, [redacted] no longer uses POGO FTP to circulate meeting material.
16-Jan-19	2 emails containing PHI were sent to 1 recipient at	Internal	Patient information (PHI)	N/A	All copies of both emails have been double deleted from	16-Jan-19	N/A	16-Jan-19	16-Jan-19	All agents permanently deleted all copies of email.

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
	POGO on January 16				sender and recipient.					
26-Mar-19	1 email containing PHI was sent from Social Worker to Provincial Coordinator, POGO Financial Assistance Program (FAP).	Internal	Patient Name and Family situation	N/A	All copies of both emails have been double deleted from sender and recipient.	26-Mar-19	N/A	26-Mar-19	26-Mar-19	All agents permanently deleted all copies of email. Reminder not to use POGO Family ID # in emails, not names.
12-Apr-19	Research project file containing PHI for Hospital 1 was inadvertently sent in secure FTP fashion to Hospital 2 Co-PI	Internal	Patient Information (PHI)	15-Apr-2019	Double deletion of the unopened file securely sent to hospital. Written confirmation from recipient of double deletion.	12-Apr-19	15-Apr-19	12-Apr-19	12-Apr-19	Hospital Co-PI permanently deleted the unopened file and sent confirmation of this to POGO Research Fellow and copied POGO Privacy Officer. POGO Privacy Officer sent a message to Hospital 1 Co-PI that their file was accidently sent to Hospital 2 Co-PI but that it was not opened and permanently deleted.
17-Apr-19	Lost Cell Phone	Internal	Hospital contacts and 2 emails that may have contained PHI.	N/A	Phone has been through a remote wipe from Exchange Server, phone has been reported lost to Bell and deactivated,	17-Apr-19	17-Apr-19	18-Apr-19	17-Apr-19	Agent reported phone lost to Manager/Director and Privacy Office. Phone was wiped, reported to Bell as lost; password protected and had limited information. Manager spoke to the individual

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
					phone was already password protected when phone was lost and had limited information.					asking him to return the phone to POGO (April 22, 2019). No response as of yet. On April 29, 2019, the individual contacted Manager with his address in order to pick up the phone and Manager asked for next steps. Director stated Network Analyst purchased a new phone on April 27, 2019 and the phone is set up for use. Director is comfortable with not coordinating pick up of the phone, having the individual discard the phone and thanking the individual for his assistance. Therefore, the Privacy Officer is satisfied with the breach remediation steps taken place and the report is now closed.
2-May-19	Email sent from [redacted] to POGO FAP Coordinator and copy to one other [redacted] Social Workers with a patient	Internal	Patient name for referral and exception request to POGO Financial Assistance Program.	N/A	Double deletion of the email sent to [redacted] from POGO Financial Assistance Program. Written confirmation	2-May-19	N/A	3-May-19	3-May-19	All agents permanently deleted all copies of email. Reminder to use POGO Family ID number in emails, not names.

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
	name to POGO Financial Assistance Program.				from recipient of double deletion.					
3-July-19	Email from staff member for a hotel request from [redacted] with child name instead of adult's name.	Internal	Patient name for referral and exception request to POGO Financial Assistance Program.	N/A	Double deletion of the email sent to [redacted] from POGO Financial Assistance Program. Written confirmation from recipient of double deletion.	3-Jul-19	N/A	3-Jul-19	3-Jul-19	All agents permanently deleted all copies of email. Reminder to use adult name and not child's name.
12-July-19	Accommodation request was sent using child's name instead of parent.	Internal	POGO Financial Assistance Program		Double deletion of the email sent to Social Worker from POGO Financial Assistance Program. Written confirmation from recipient of double deletion.	12-Jul-19	N/A	12-Jul-19	12-Jul-19	Agent permanently deleted all copies of email. Reminder to use adult name and not child's name.
23-Jul-19	1 email containing PHI was sent to 1 recipient at POGO on 23-July-2019.	Internal	Patient Information		All copies of both email have been double deleted from sender and recipient.	23-Jul-19	N/A	23-Jul-19	23-Jul-19	All agents permanently deleted all copies of email.
26-Jul-19	During a SAVTI, Survivor 2 Survivor webcast,	External	Correspondence for webcast	Yes	Webcast has not been archived by OTN. Webcast has been deleted,	29-July-19	26-July-2019	29-Jul-19	30-Jul-19	Webcast has been deleted from OTN archive and cache. Administrative Assistant will prepare a "Tips and Tricks" to

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
	facilitator inadvertently showed his email inbox to participants by flipping between the presentation and his email inbox.				as well as the cache.					reminder facilitators to close all email inbox, social media, etc. to prevent a privacy breach.
22-Aug-19	Accommodation request was sent using child's name instead of parent.	Internal	POGO Financial Assistance Program (FAP)		Double deletion of the email sent to Social Worker from POGO Financial Assistance Program. Written confirmation from recipient of double deletion.	22-Aug-19	N/A	27-Aug-19	27-Aug-19	Agent permanently deleted all copies of email. Reminder to use adult name and not child's name. POGO FAP will implement a communication plan to remind staff of tips and tricks for PHI. Called hotel partner main contact and reservation contact. Explained the situation Asked them to double delete all emails containing patient name from inbox, sent box and deleted items box and confirmed completion of this. Therefore, hotel double deleted the email.

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendation & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressedor Proposed Manner
										Email was also sent to follow up on conversation and to once again confirm all steps of double deletion were completed.
22-Aug-19	Accommodation request was sent using child's name instead of parent and sent to hotel for reservation.	External	Financial Assistance Program (FAP)		Double deletion of the email sent to Social Worker from POGO Financial Assistance Program (FAP). Written confirmation from recipient of double deletion.	22-Aug-19	22-Aug-19	27-Aug-19		Agent permanently deleted all copies of email. Reminder to use adult name and not child's name was included in email instructions.
20-Sep-19	Accommodation request was sent using child's name instead of parent and sent to hotel for reservation	Internal	Financial Assistance Program (FAP)		Double deletion of the email sent to Nurse from POGO Financial Assistance Program (FAP). Written confirmation from recipient of double deletion	23-Sep-19	23-Sep-19	23-Sept-19		Agent permanently deleted all copies of email. Reminder to use adult name and not child's name was included in email instructions. Given frequency of similar breaches, POGO FAP implemented a communication plan to remind staff of tips and tricks for PHI.

Privacy Complaints	▪ The number of privacy complaints received since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 0 privacy complaints received.
	▪ Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint investigated: – The date that the privacy complaint was received, – The nature of the privacy complaint, – The date that the investigation was commenced, – The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation, – The date that the investigation was completed, – A brief description of each recommendation made,	▪ N/A

	– The date each recommendation was addressed or is proposed to be addressed, – The manner in which each recommendation was addressed or is proposed to be addressed, and – The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.	
	▪ Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint not investigated: – The date that the privacy complaint was received, – The nature of the privacy complaint, and –The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.	▪ N/A

Part 2 – Security Indicators

Categories	Security Indicators	POGO 2019	
General Security Policies and Procedures	▪ The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.	**Date**	**Policies Reviewed (See Appendix 1: POGO Policy Numbers and Policy Titles)**
		February 2017	9.2.20
		June 2017	9.2.7
		November 2017	9.2.28
		August 2018	9.2.7, 9.2.15, 9.2.18
		October 2018	9.2.2, 9.2.4
		January 2019	9.2.1, 9.2.59.2.8, 9.2.9, 9.2.17, 9.2.19, 9.2.20, 9.2.26,9.2.27
		September 2019	9.2.6, 9.2.7, 9.2.9
		October 2019	9.2.28

- Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.

Policy #	Policy Document/Title	If yes, reason for and nature of amendments made
9.2.2	Ongoing Review of Security Policies, Procedures and Practices	Added legislative authority.
9.2.4	Threat and Risk Assessment	Added legislative authority.
9.2.5	Physical/Office Security	Added legislative authority, edited sections to more closely align with policy 9.2.18 - Confidentiality and Security of Data.
9.2.7	Personal Health Information on Mobile Devices	Added level of access granted; added legal authority, changed ED to CEO, deletion of floppy drives and CDs and removal of Linkage System.
9.2.15	Acceptable Usage	Addition of legal authority; new pre-approved and prohibited resources added; addition of remote access restrictions.
9.2.18	Confidentiality and Security of Data	Removed Linkage System, added legislative authority, added visitor sign-in, added use of secure gray bin for shredding, added reference to policy 9.3.4, edited wording for clarity.
9.2.19	Document Shredding	Added legislative authority, and added reference to secure gray bin in POGONIS
9.2.28	Inventory of PHI Placed in Secure Gray Bin	Policy created as per IPC recommendation to develop an inventory of PHI going into the gray bin.

- Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.
  - N/A

- The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and

Date	Nature of Communication
November 2017	Met with PHI users regarding new policy to maintain an inventory of PHI placed in the secured gray bin for secure disposal (9.2.28).

	procedure communicated to agents, the nature of the communication.	**1 December 2017**	Directors updated on amendments made to Privacy policies and procedures at their annual Board of Directors meeting (9.2.2, 9.2.4, 9.2.5, 9.2.7, 9.2.15, 9.2.18, 9.2.19, 9.2.28).	
		15 June 2018	Data Managers privacy re-fresher training and policies and procedures (9.1.1, 9.1.4, 9.1.7, 9.1.8, 9.1.9).	
		24 July 2018	Briefings with agents including senior management and the Board regarding changes to policies and procedures as a result of April 2018 privacy incident (9.2.2, 9.2.4, 9.2.5, 9.2.7, 9.2.15, 9.2.18, 9.2.19, 9.2.28).	
		26 July 2018	Email to PHI users regarding security enhancements to privacy and security policies as a result of the privacy incident (9.2.2, 9.2.4, 9.2.5, 9.2.7, 9.2.15, 9.2.18, 9.2.19, 9.2.28).	
		30 July 2018	Briefings with agents including senior management and the Board regarding changes to policies and procedures as a result of April 2018 privacy incident (9.2.2, 9.2.4, 9.2.5, 9.2.7, 9.2.15, 9.2.18, 9.2.19, 9.2.28).	
		10 August 2018	Email to POGO staff regarding the new Visitor Sign-In Policy (9.1.24).	
		27 August 2018	Briefings with agents including senior management and the Board regarding changes to policies and procedures as a result of April 2018 privacy incident (9.2.2, 9.2.4, 9.2.5, 9.2.7, 9.2.15, 9.2.18, 9.2.19, 9.2.28).	
		24 September 2019	Technical safeguards for outgoing emails: POGO's IT/Systems Analyst implemented new email security addition on the firewall that detects and emails containing the following sensitive information (personal health card number, Ontario; bank account details, Canada; bank routing numbers, Canada; credit or debit card numbers, Canada; social insurance numbers, Canada). These filters will be blocked all outgoing emails and senders will get notification of blocked emails (9.2.1, 9.2.2, 9.2.3).	
		28 September 2018	Interlink Community Nurses privacy training and review of privacy/PHI procedures and amendments specific to Interlink practices (9.1.21, 9.2. 29, 9.4.12).	
		25 January 2019	Directors updated on amendments made to Privacy policies and procedures at their annual Board of Directors meeting having regard to changes as a result of the privacy incident (9.2.2, 9.2.4, 9.2.5, 9.2.7, 9.2.15, 9.2.18, 9.2.19, 9.2.28).	
		25 January 2019	Email to staff regarding updates/edits to POGO Privacy and Security Code and its Procedures (1.7).	

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>26 January 2019</td><td>Directors updated on amendments made to Privacy policies and procedures at their annual Board of Directors meeting (9.2.2, 9.2.4, 9.2.5, 9.2.7, 9.2.15, 9.2.18, 9.2.19, 9.2.28).</td></tr>
<tr><td>30 January 2019</td><td>Email to staff regarding edits/updates to POGO privacy and security policies and procedures posted on POGO website in POGO staff policies (9.2.2, 9.2.4, 9.2.5, 9.2.7, 9.2.15, 9.2.18, 9.2.19, 9.2.28).</td></tr>
<tr><td>15 March 2019</td><td>New hires asked to sign code of conduct (9.3.8).</td></tr>
<tr><td>18 June 2019</td><td>POGO staff reviewed updated refresher privacy training in monthly staff meeting and PowerPoint was sent via email for reference (9.3.1).</td></tr>
<tr><td>October 2019</td><td>Communication sent to staff concerning visitor sign in policy and visitor sign in chart of internal and external agents (9.1.24).</td></tr>
</table>
</td></tr>
<tr><td></td><td>▪ Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.</td><td>▪ POGO's Privacy and Data Security Code was updated and made available on POGO's website in December 2018 as a result of the review.</td></tr>
<tr><td>Physical Security</td><td>▪ The dates of audits of agents granted approval to access the premises and locations within the premises where records of personal health information are retained since the prior review by the Information and Privacy Commissioner and for each audit:
– A brief description of each recommendation made,
– The date each recommendation was addressed or is proposed to be addressed, and
– The manner in which each recommendation was addressed or is proposed to be addressed.</td><td>
<table>
<tr><th>Date of Audit of Agents</th><th>Date Each Recommendation Was Addressed</th><th>Recommendations Arising from Audit</th><th>The manner in which each recommendation was addressed</th></tr>
<tr><td>November 2016</td><td>December 2016</td><td>No recommendations</td><td>No updates</td></tr>
<tr><td>September 2017</td><td>September 2017</td><td>Audit new POGO staff: Acceptable Use forms and key card access.</td><td>Acceptable Use Forms

No recommendations were made.

Reviewed with each POGO staff. Acceptable Use forms updated if required.</td></tr>
<tr><td>May 2018</td><td>November 2018</td><td>Audit new POGO staff: Acceptable Use forms and key card access.</td><td>Acceptable Use Forms

No recommendations were made.

Reviewed with each POGO staff.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>Acceptable Use forms updated if required.</td></tr>
<tr><td>January 2019</td><td>July 2019</td><td>Audit new POGO staff: Acceptable Use forms and key card access.</td><td>Acceptable Use Forms

Reviewed with each POGO staff. Acceptable Use forms updated if required.</td></tr>
<tr><td>June 2019</td><td>June 2019</td><td>Review Iron Keys usage with Interlink Nurses and update Acceptable Use form accordingly.</td><td>Given Iron Keys are no longer used by Interlink Nurses, the Acceptable Use forms was updated</td></tr>
<tr><td>August 2019</td><td>December 2019</td><td>1. Establish new policy and procedure for visitor sign-in given new POGO reception area coverage.
2. Complete all staff education about the new policy and procedure</td><td>1. New policy and procedure established and developed a Visitor Sign in Chart for staff. (See Appendix 2: Visitor Sign in Chart)

2. Email sent to POGO Staff regarding the new Visitor Sign-in policy.</td></tr>
</table>
</td><td></td></tr>
<tr><td>Security Audit Program</td><td>▪ The dates of the review of system control and audit logs since the prior review by the Information and Privacy Commissioner of Ontario and a general description of the findings, if any, arising from the review of system control and audit logs.</td><td colspan="2">
<table>
<tr><th>Type of Security Audit</th><th>Frequency</th></tr>
<tr><td>Review of all Security Policies and Procedures</td><td>Annually by POGO Privacy Officer and IT team.</td></tr>
<tr><td>POGO System/Security Audits</td><td>Biweekly on Monday by POGO System Administrator (77 audits in total over a period of 3 years).

See Appendix 3: POGO System Review 2016 – 2019</td></tr>
</table>
</td><td></td></tr>
</table>

		POGONIS Security Audit	Biweekly on Tuesday by POGO Database Administrator. (73 audits in total over a period of 3 years) See **Appendix 4: POGO POGONIS Security Audit Review**
		Threat and Risk Assessments of POGO IP Addresses ○ **Vulnerability** ○ **Penetration** ○ **Ethical Hacks**	Annually or with scheduled system changes; conducted POGO System Administrator and reviewed by POGO Privacy Officer. (106 audits in total over a period of 3 years)

- The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:
  - A description of the nature and type of audit conducted,
  - The date of completion of the audit,
  - A brief description of each recommendation made,
  - The date that each recommendation was addressed or is proposed to be addressed, and
  - The manner in which each recommendation was addressed or is expected to be addressed.

- **There were 256 security audits completed since the prior review, excluding policy reviews.**
- **3 - Audits completed due to the 2018 External Breach.**

2016:

Security Audits	Review Date	Findings/ Recommendations	Date Addressed or Proposed	Manner Each Recommendation Addressed or Proposed Manner
POGONIS Security Audit (Note: non-suspicious findings are not listed)				
POGONIS production database biweekly review, POGONIS production environment, application server named PCRTERM.	Dec 16, 2016	An Excel file found in PCRTERM C: drive, named Review_List.xls. No PHI included.	Dec 16, 2016	Although there was not any PHI data in it, an email has been sent to local administrators to remind that files should not be stored in here. File has been deleted.
POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)				

		Remote Desktop Connection	Nov 21, 2016	Remote Users could see "Network" icon in Windows Explorer.	Nov 21, 2016	"Network" has been removed from Windows Explorer Navigation Pane on PCRTERM server by Registry editing.

2017: Other Security Audits

1 Internal Security Policies and Procedure Review has been completed.

Security Audits	Review Date	Findings/ Recommendations	Date Addressed or Proposed	Manner Each Recommendation Addressed or Proposed Manner
Internal Security Policies and Procedure Review				
9.2.28 Inventory of PHI – documents in secure bin – Audit Program – IPC Recommendation	Nov-17	2016 IPC Recommendation	Nov-17	Included content suggested by IPC.
POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)				
Firewall	23-Jan- 17	[redacted] users couldn't access POGO ACTS from part of hospital computers	23-Jan-2017	[redacted] hospital external IP range has been updated on Cisco Firewall.
File Server	10-Jul-2017	1. Administrator credentials were cached on one workstation and allowed user to connect to file server as domain administrator	10-July-2017	1. POGO Domain Administrator credentials removed from workstation. POGO IT confirmed internal agent/ workstation does not have access to POGO PHI data holdings.

		Proxy Server	24-Jul-2017	Proxy CA certificate was about to expire.	24-July-2017	Certificate has been regenerated on Web protection Sophos UTP proxy.
		Email Servers	25-Jul-2017	GeoTrust recommended regenerate SSL certificates for stronger security	25-July-2017	Exchange and ACTS SSL certificate has been regenerated, following GeoTrust recommendations.
		Email Servers	5-Sep-2017	SPF DNS record was missing for POGO email server	5-Sept-2017	Sender Policy Framework (SPF) has been updated on POGO mail server
		POGONIS Security Audit (Note: non-suspicious findings are not listed)				
		POGONIS – POGONIS Application	Jul-17	No changes to application in 2017, annual review of users and access privileges conducted, no recommendations required.	Jul-17	

2018: Other Security Audits

4 Internal Security Policies and Procedure Review has been completed.

Security Audits	Review Date	Findings/ Recommendations	Date Addressed or Proposed	Manner Each Recommendation Addressed or Proposed Manner
Internal Security Policies and Procedure Review				
9.2.2 Ongoing Review of Security Policies, Procedures and Practices	Oct-18	Add legislative authority.	Oct-18	1. Policy updated with approved legislative authority by Privacy Officer. Privacy Officer communicated with POGO

		Audit Program				Internal Agents changes in policy.	
		9.2.7 PHI On Mobile Devices **Audit Program Review re: 2018 External Breach**	Aug-18	Add legal authority, change ED to CEO, delete reference to floppy drives and CDs, and remove reference to Linkage System.	Aug-18	1. Policy reviewed and updated by Privacy Officer, Senior Database Administrator and System and Network Analyst with approved legal authority, updates of Internal Agent titles and removal of hardware (floppy drives and CDs) and system processes (Linkage System) no longer in use at POGO. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		9.2.15 Acceptable Use **Audit Program Review re: 2018 External Breach**	Aug-18	Privacy Officer and CEO recommended review of policy to include addition of legal authority; new pre-approved and prohibited resources added; addition of remote access restrictions as result of 2018 External Breach.	Aug-18	1. Policy reviewed and updated by Privacy Officer, Senior Database Administrator and System and Network Analyst to include approved legal authority; addition of new pre-approved and prohibited listing of resources and addition of remote access restrictions. Privacy Officer communicated with POGO Internal Agents changes in policy. 2. IPC notified of review and update of this policy on July 25, 2018.	

		9.2.18 Confidentiality of Data **Audit Program Review re: 2018 External Breach**	Aug-18	Remove Linkage System, add legislative authority, add visitor sign-in, add use of secure gray bin for shredding, add reference to Policy #9.3.*4 Termination or Cessation of Employment or Contractual Relationship*, edit policy for clarity.	Aug-18	1. Policy reviewed by Privacy Officer, Senior Database Administrator and System and Network Analyst to add approved legislative authority; remove Linkage System process; add visitor sign-in and the use of secure gray bin for shredding of PHI documents and added references to Policy #9.3.4. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		2018					
		POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)					
		Remote Desktop Connection	2-Jan-2018	RD Gateway SSL certificate was about to expire	2-Jan-2018	RD Gateway SSL certificate has been renewed	
		https/SSL POGO Internet services	26-Feb-2018	Google and DigiCert recommended to replace SSL certificates to meet new security requirements	26-Feb-2018	Webmail, ACTS and REDCap SSL certificate are replaced, according to Google and DigiCert requirements	
		Firewall	26-Mar-2018	Repetitive scanning attack from address [redacted] IP address	26-Mar-2018	[redacted] IP address has been denied access to all POGO external resources	
		Firewall	9-Apr-2018	Repetitive scanning attack from address [redacted] IP address	9-Apr-2018	[redacted] IP address has been denied access to all POGO external resources	

Firewall	21-May-2018	Repetitive scanning attack from address [redacted] IP address	21-May-2018	[redacted] IP address has been denied access to all POGO external resources
https/SSL POGO Internet services	18-June-2018	Google and DigiCert recommended to replace SSL certificates to meet new security requirements	18-June-2018	transfer.pogo.ca SSL certificate has been replaced following Digicert and Google recommendations
File access	13-Aug-2018	PHI users should be blocked from using USB external shortage	13-Aug-2018	PHI users have been blocked from using USB external storage by new Domain Policy
https/SSL POGO Internet services	19-Nov-2018	1. Using TLS protocol versions lower than 1.2 should be eliminated for POGO Internet services 2. POGO gate.pogo.ca reviewed and TLS 1.1 remains acceptable given many client computers did not support TLS 1.2 and could not use this service if TLS 1.1 was disabled at this time.	19-Nov-2018	1. TLS 1.2 protocol was implemented for webmail.pogo.ca; acts.pogo.ca; redcap.pogo.ca; transfer.pogo.ca 2. Ongoing review of gate.pogo.ca TLS version by POGO IT is requested

2018

Security Audit	Review Date	Findings/Recommendations	Date Addressed or Proposed	Manner Each Recommendation Addressed or Proposed Manner
POGONIS Security Audit (Note: non-suspicious findings are not listed)				
POGONIS production database biweekly review, audit log at database level (select * from	March 27, 2018	1. Object update in database by POGO Database administrator 2. Satellite application user security access limitations, user	March 27, 2018	1. LOGON_TRIGGER was updated on March 27, 2018 by POGO Database Administrator [redacted] to allow connections from SERVER[redacted] for Satellite

		dba_audit_trail where to_char(timestamp ,'yyyy-mm-dd hh:mi:ss')>'2018-03-13 00:00:00' order by timestamp;)		activity auditing and logging mechanisms to be confirmed prior to Object update		database new application lookup to POGONIS. 2. Satellite application user security access limitations, user activity auditing and logging mechanisms to be confirmed by POGO Database Administrator
		POGONIS production database biweekly review	June 19, 2018	Database auditing failure after upgrade from Oracle 11g to 12c on June 7, 2018. No actions were seen in audit log within period (June 7-June 19 2018)	June 19, 2018	Auditing re-configured. The table [redacted] was renamed as [redacted] and the user login information is ensured that is being collected in this table
		POGONIS production database biweekly review	July 3, 2018	None. Ensured that the auditing is in place since the previous review on June 19, 2018	July 3, 2018	None. Continue to monitor
		POGONIS production database biweekly review - part "Check physical database backups"	Septemb er 11, 2018	Obsolete Archive logs were not deleted after the backup, which may cause server disk space issues and the database, may stop working	September 11, 2018	Obsolete Archive logs were manually purged, and auto purging re-configured in the database backup scripts Monitored closely to ensure that obsolete archive logs are again being purged automatically, and server disk free space is back in normal ranges
		POGONIS production database biweekly review	September 25, 2018	None. Ensured that the backups continue to be running properly	September 25, 2018	None. Continue to monitor the backups, obsolete archive files are auto-purged, and the disk space is in normal ranges

2019: Other Security Audits

4 Internal Security Policies and Procedure Review has been completed.

		Security Audits	Review Date	Findings/ Recommendations	Date Addressed or Proposed	Manner Each Recommendation Addressed or Proposed Manner
		Internal Privacy and Security Policies and Procedure Review:				
		Policy #9.2.6 Retention, Return and Destructions **Audit Program**	September 2019	Review policy to ensure continued compliance with IPC Manual and review procedures to ensure current applicable data destruction processes in place. Edit section 3. Researcher agreement section to include disclosure process to Principle Investigator/s and deletion of data destruction process B as CD/DVDs are no longer used for data transfers.	September 2019	1. Policy reviewed and updated by Privacy Officer to ensure all components for IPC Manual included in the policy and section 3. Researcher Agreement, updated data disclosure/transfer and data destruction processes. Privacy Officer communicated with POGO Internal Agents changes in policy.
		Policy #9.2.7 Mobile Devices **Audit Program**	September 2019	1. Privacy Officer recommended annual review of policy with IT Team. 2. Additional information on how data is transferred via encrypted mobile devices and FTP server to be added 3. Include process for POGO's consent	September 2019	1. Privacy Officer review policy with IT Team and 2. updated policy to add indications and procedure on secure transfer via encrypted mobile devices and FTP server and 3. To add the secure transfer processes for the consent based data holdings. Privacy Officer communicated with POGO

				based data holdings (Interlink and SAVTI).		Internal Agents changes in policy.	
		Policy #9.2.9 Secure Transfer of Records of Personal Health Information **Audit Program**	September 2019	Privacy Officer to review policy to 1. ensure continued compliance with IPC Manual; 2. to review procedures to ensure current applicable secure transfer processes in place, and 3. Delete Secure bonded courier as a mode of transfer from policy.	September 2019	1.Privacy Officer reviewed policy and confirmed policy in compliance with IPC Manual and 2. confirmed all current approved secure transfer processes in place listed in policy and 3. deleted secure bonded courier as a mode of transfer from policy. Privacy Officer communicated with POGO Internal Agents changes in policy.	
		Policy #9.2.28 Inventory of PHI Placed in Secure Grey Bin **Audit Program**	October 2019	1. Privacy Officer to review policy to ensure continued compliance with IPC Manual. 2. Include PHI abbreviations in policy introduction; 3. Include compliance and breach notification clause as per IPC Manual requirements.	October 2019	1. Privacy Officer reviewed and confirmed policy in compliance with IPC Manual; 2. updated policy to include PHI abbreviations; and; 3. Include compliance and breach notification clause as per IPC Manual requirements. Privacy Officer communicated with POGO Internal Agents changes in policy.	

		2019				
		POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)				
		Firewall	Sept 16, 2019	Repetitive scanning attack from address [redacted] IP address.	Sept 16, 2019	[redacted] IP address has been denied access to all POGO external resources.
		Web Proxy Server	May 2019	Decommissioned 2 former servers.	June 2019	New Web Proxy Server commissioned with new security device available. Device also acts as the front end scanning of all emails both inbound and out for viruses and spam plus monitoring the security of the websites that are browsed by internal agents. Implementation communicated with internal agents in October 2019.
		Email Server	September 2019	New firewall with enhanced security.	September 2019	Sophos firewall feature implemented to block outgoing emails that contain sensitive information e.g. personal health card numbers, SIN, bank account details, bank routing numbers, credit or debit card numbers. Senders will receive notification of blocked email. Implementation of

						these blocks communicated with internal agents in October 2019.
		Back end server applications	July 2019	Migration of Applications and installation of Microsoft System Centre Operations Manager.	July 2019	Microsoft System Center Configuration Manager is now operating in the new environment providing the distribution of antivirus updates, plus remote control software update management, software distribution, as well as maintain an inventory of hardware and software. Implementation of these blocks communicated with internal agents in October 2019.
		POGONIS Security Audit (Note: non-suspicious findings are not listed)				
		POGONIS production database biweekly review, audit log at database level (select * from dba_audit_trail where to_char(timestamp,'yyyy-mm-dd hh:mi:ss')>'2019-01-02 00:00:00' order by timestamp;)	January 15, 2019	No recent records in the database audit since previous review on 2019-Jan-02; this needs to be investigated.	January 15, 2019	Further troubleshooting in the auditing setup. Re-configured and server logs are reviewed in the operation system level. No suspicious actions found.

		POGONIS production database biweekly review, audit log at database level (select * from dba_audit_trail where to_char(timestamp,'yyyy-mm-dd hh:mi:ss')>'2019-01-15 00:00:00' order by timestamp;)	January 22, 2019	None. Ensured that the auditing is in place since the previous fix on Jan 18, 2019.	January 22, 2019	None. Continue to monitor.

2019

2 Topic Reviews audits have been completed.

Programs	Review Date	Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed Or Proposed Manner
Topic Reviews				
Research Data folders - Research - Review of users and access of program folders in POGO drive.	19-Mar-19	Access to folders on the staff drive was further restricted.	18-Mar-19	System administrators reviewed access and limited the folders containing sensitive information to solely the program manager and the system administrator.

		POGONIS – Data/IT POGONIS platform upgrade to Windows 16 or later and database version upgrade to Oracle 18	2-Jul-19	1. POGO IT recommended upgrade given MS 2008 will no longer provide security patches after December 2019. 2. AIM (Third party provider for POGONIS) notified of POGO's request to upgrade platform and database version to maintain security. 3. AIM to test POGONIS in Windows 19 and Oracle 18 and confirm that the upgrade testing had no issues prior to POGO IT proceeding with upgrades 4. POGO IT to implement the upgrade by the end of 2019.	By end of 2019	1. POGO Network/System Analyst prepared POGO network and servers for upgrade to MS Windows 16 to ensure security patches are up to date. 2. POGO IT informed AIM re. upgrades and requirement to test POGONIS 3. AIM confirmed testing of POGONIS for upgrades with no issues 4. POGO Database Administrator Began testing POGONIS for upgrades but put on hold due to pandemic and remote work environment for POGO office staff and POGONIS Data Mangers (final stage of implement-ation proposed to be completed in Fall 2020).
Information Security Breaches	▪ The number of notifications of information security breaches or suspected information security breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	▪ No known information security breaches				
	With respect to each information security breach or suspected information security breach: – The date that the notification was received, – The extent of the information security breach or suspected information security breach,	▪ Not applicable				

	– The nature and extent of personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented – The date(s) that notification was provided to the health information custodians or any other organizations, – The date that the investigation was commenced, – The date that the investigation was completed, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	

Part 3 – Human Resources Indicators

Categories	Human Resources Indicators	POGO 2019
Privacy and Security Training and Awareness	▪ The number of agents who have received and who have not received initial privacy and security orientation since the prior review by the Information and Privacy Commissioner of Ontario.	Total: 290 ▪ In 2016, 4 agents ▪ In 2017, 82 agents ▪ In 2018, 104 agents ▪ In 2019, 100 agents ▪ Since the prior review, there have been no agents that have not received initial privacy orientation
	▪ The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial privacy and security orientation and the scheduled date of the initial privacy and security orientation.	▪ Not applicable, since all new agents have received initial privacy orientation
	▪ The number of agents who have attended and who have not attended ongoing privacy and security training each year since the prior review by the Information and Privacy Commissioner of Ontario.	2016 (October to December): o 4 agents received ongoing privacy and security training o 2 Volunteers received ongoing privacy and security training o 1 Researcher received ongoing privacy and security training o 1 POGONIS Data Manager received privacy and security training o 0 agent did not receive privacy training 2017: o 82 agents in total received ongoing privacy and security training o 42 Internal Agents received ongoing privacy and security training o 15 Board of Directors received ongoing privacy and security training o 10 Volunteers received ongoing privacy and security training

Categories	Human Resources Indicators	POGO 2019
		○ 2 Students received ongoing privacy and security training ○ 9 Researchers received ongoing privacy and security training ○ 1 After Care staff received ongoing privacy and security training ○ 3 POGO Finance Assistance staff received ongoing privacy and security training ○ 15 agents did not receive privacy and security training 2018: ○ 104 agents in total received ongoing privacy and security training ○ 41 Internal Agents received ongoing privacy and security training ○ 16 Board of Directors received ongoing privacy and security training ○ 3 Volunteers received ongoing privacy and security training ○ 12 Interlink Community Cancer Nurses received ongoing privacy and security training ○ 2 POGONIS Data Manager received privacy and security training ○ 2 Students received ongoing privacy and security training ○ 6 Researchers received ongoing privacy and security training ○ 18 Satellite Nurses received privacy and security training ○ 6 POGO Finance Assistance staff received ongoing privacy and security training ○ 2 agents did not receive privacy training 2019: ○ 100 agents in total received ongoing privacy and security training ○ 40 Internal Agents received ongoing privacy and security training ○ 16 Board of Directors received ongoing privacy and security training ○ 1 Volunteer received ongoing privacy and security training ○ 14 Interlink Nurses received ongoing privacy and security training ○ 2 Students received ongoing privacy and security training ○ 8 Researchers received ongoing privacy and security training

<table>
<tr><th>Categories</th><th>Human Resources Indicators</th><th>POGO 2019</th></tr>
<tr><td></td><td></td><td>

3 SAVTI counsellors received privacy and security training
15 Satellite Nurses received privacy and security training
1 POGONIS Data Managers received privacy and security training

0 agents did not receive privacy and security training

</td></tr>
<tr><td></td><td>

The dates and number of communications to agents by the prescribed entity in relation to privacy and security since the prior review by the Information and Privacy Commissioner of Ontario and a brief description of each communication.

</td><td>

In addition to Parts 1 (Privacy) and 2 (Security) above where POGO indicates communication regarding new and amended policies and procedures for Privacy and Security, please see the additional 34 communication in the chart below:

<table>
<tr><th>Date</th><th>Nature of Communication</th></tr>
<tr><td>December 2017</td><td>Winter Research/Privacy Newsletter distributed to POGO staff and agents, which included highlighting of new policies and procedures (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).</td></tr>
<tr><td>February 2017</td><td>Communication to staff to review new and amended privacy policies (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).</td></tr>
<tr><td>February 2017</td><td>Communication to staff to new and amended privacy policies (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).</td></tr>
<tr><td>February 2017</td><td>Staff meeting – review of policies and accessibility compliance (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28, 9.3.24).</td></tr>
<tr><td>February 2017</td><td>Communication to staff to complete AODA training (9.3.1).</td></tr>
<tr><td>February 2017</td><td>Staff Privacy Training completed (9.3.1).</td></tr>
<tr><td>January 2017</td><td>Board Privacy Training Completed (9.3.1).</td></tr>
<tr><td>January 2017</td><td>Communication to Interlink nurses to sign annual Confidentiality Agreement (9.3.2).</td></tr>
<tr><td>January 2017</td><td>Communication to staff to sign annual Confidentiality Agreement (9.3.2).</td></tr>
</table>
</td></tr>
</table>

Categories	Human Resources Indicators	POGO 2019	
		22 Nov 2018	Follow-up written communication to POGO partner Health Information Custodians (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		29 October 2018	Communication to POGO staff requesting clarification regarding their use of Drop Box and USB keys (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		September 2018	Communication to staff regarding IT changes related to data incident (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		September 2018	Communication to staff regarding IT changes related to data incident (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		August 2018	Research/Privacy Newsletter distributed to POGO staff and agents, which included highlighting of new policies and procedures (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		August 2018	Communication to staff regarding IT changes related to data incident. (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		10 Aug 2018	Briefings with Senior Management team regarding the privacy incident and security measures (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		26 July 2018	Briefings with Staff at POGO staff meeting regarding the privacy incident and security measures (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		25 July 2018	POGO telephone notification to POGO partner Health Information Custodians regarding privacy incident (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).

Categories	Human Resources Indicators	POGO 2019	
		17 July 2018	Briefings with Senior Management team regarding the privacy incident and security measures (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		17 July 2018	Briefings with Staff at POGO staff meeting regarding the privacy incident and security measures (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		July 2018	Communication to staff and administrative assistants concerning increased data security action related to external storage devices (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		July 2018	Communication to Operations Group and all staff meeting to discuss and provide recommendations on security enhancements for PHI users (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		27 June 2018	Provided an update briefing for the POGO Board of Directors regarding the privacy incident(1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		27 June 2018	Provided an update briefing for the POGO Board of Directors regarding the privacy incident (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		11 May 2018	Briefed the POGO Board of Directors regarding privacy incident that POGO learned of on March 26, 2018 (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		8 May 2018	Briefings with Ops Committee regarding the privacy incident and security enhancements (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		January 2018	Communication to staff to sign annual Confidentiality Agreement (9.3.2).
		August 2019	Communication to staff to complete annual review of PIA's (9.1.14).
		May 2019	Communication to staff regarding sending PHI and email policies (1.7, 1.8, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.1.11, 9.1.12, 9.1.13, 9.1.13, 9.1.14, 9.24, 9.2.28).
		January 2019	Communication to staff to sign annual Confidentiality Agreement (9.3.2).

Categories	Human Resources Indicators	POGO 2019	
		October 2019	Communication to POGO FAP staff to not include child's name, but to include parent's name in the email. Including a child's name in an email as opposed to the parent's name is viewed as a breach (9.1.16).
		September 2019	Communication to staff to complete BCDR Lunch and Learn, specifically for new staff and a refresher for current employees (9.4.7).
		September 2019	Communication to staff to sign annual Confidentiality Agreement (9.3.2).
		October 2019	Communication to staff to complete BCDR Lunch and Learn, specifically new staff and a refresher for current employees (9.4.7).
Confidentiality Agreements	▪ The number of agents who have executed and who have not executed Confidentiality Agreements each year since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 5 agents executed Confidentiality Agreements in 2016 between November and December ▪ 104 agents executed Confidentiality Agreements in 2017 ▪ 78 agents executed Confidentiality Agreements in 2018 ▪ 31 agents (external) required to sign a Confidentiality Agreement annually and who did not do so in 2018. Privacy Team processes to ensure compliance were reviewed and updated. ▪ 129 agents executed Confidentiality Agreements in 2019 (100% compliance)	
	▪ The date of commencement of the employment, contractual or other relationship for agents that have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.	▪ All, but 1 agent who have not yet signed a confidentiality agreement have signed an initial confidentiality agreement in the previous year(s) as required per POGO Policies and Procedures. All agents must execute confidentiality agreements by December 2019.	
Termination or Cessation	▪ The number of notifications received from agents since the prior review by the Information and Privacy Commissioner of Ontario related to termination of	▪ 19 notifications from agents that included staff and summer students.	

Categories	Human Resources Indicators	POGO 2019
	their employment, contractual or other relationship with the prescribed person or prescribed entity.	

Part 4 – Organizational Indicators

Categories	Organizational Indicators	POGO (2019)
Risk Management	▪ The dates that the corporate risk register was reviewed by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	▪ Corporate Risk Register reviewed by Director of Finance and Administration: 1. February 12, 2018 2. September 18, 2019 ▪ POGO Board of Directors: 1. September 20, 2018 2. September 20, 2019
	▪ Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.	▪ Annual updates by all Program Managers for program-specific risk reviews and assessments. ▪ The Board of Directors reviewed the highest priority organizational risks, as well as discussing the strategies in place to mitigate the identified areas of concern. ▪ As no new program specific risks were identified that relate to collection, use and disclosure of personal health information, no amendments were made to the corporate risk register.
Business Continuity and Disaster Recovery	▪ The dates that the business continuity and disaster recovery plan was tested since the prior review by the Information and Privacy Commissioner of Ontario.	▪ The plan was tested on June 2017 via a table top business interruption scenario (Business Resumption Team) and again on June 2018. ▪ 3 actual disruptions to POGO business occurred on December 16, 2018, April 10, 2019 and June 1, 2019: due to technological/man-made interruptions.

Categories	Organizational Indicators	POGO (2019)
	▪ Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.	September 2019 • Updated Phone Tree • Program Managers are required to update their contact lists every 6 months in hard copy and on web, and updates are added to the full plan August 2018 Testing resulted in updating/streamlining the Process for Notifications (Internal and External), and roles and responsibilities. Other ongoing updates included: • the Phone Tree due to new or departing staff • re-organization of programs • new CEO letter as preamble to the Plan • Program Managers are required to update their contact lists every 6 months in hard copy and on web, and updates are added to the full plan. • minor editing and formatting changes August 2017 • Updated Phone Tree June 2017 • Tabletop testing completed with BCDR Resumption Team; No changes to plan made. March 2017 • Maintenance of BCDR Plan

Appendix 1: Listing of POGO Policy Numbers and Titles

POGO Polices – Policy Numbers and Policy Titles (IPC 2020)
9.1 Privacy Policies

Policy Number	Policy Title
9.1.1	Process for 44 and 45 Projects
9.1.2	Review of Privacy and Security Policies and Procedures
9.1.3	Transparency of Privacy Policies, Procedures and Practices
9.1.4	Collection of Personal Health Information
9.1.5	Data Holdings Containing Personal Health Information
9.1.6	Levels of Access Policy
9.1.7	Use of Personal Health Information for Research
9.1.8	Disclosure of Personal Health Information for Purposes Other than Research
9.1.9	Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements
9.1.10	Execution of Data Sharing Agreements
9.1.11	Template for Agreement with Third Party Service Providers
9.1.12	Linkage of Records of Personal Health Information
9.1.13	De-Identifying Personal Health Information
9.1.14	Privacy Impact Assessment
9.1.15	Privacy Audits
9.1.16	Privacy Breach and Incident Management
9.1.17	Privacy Inquires, Challenges and Complaints
9.1.18	Access to Records by the Public
9.1.19	Ethics Review Process for POGO
9.1.20	Privacy and Security Policies for Ontario Telemedicine Network
9.1.21	Interlink Patient Care Plan
9.2.22	POGO Financial Assistance Program
9.1.23	The POGO School and Work Transitions program Mobile Phones and Personal Health Information
9.1.24	POGO Visitor Sign-In

9.2 Security Policies

Policy Number	Policy Title
9.2.1	Information Security Policy
9.2.2	Ongoing Review of Security Policies, Procedures and Practices
9.2.3	Security Standards and Procedures
9.2.4	Threat and Risk Assessment
9.2.5	Physical-Office Security Policy
9.2.6	Retention, Return and Destruction of Data
9.2.7	Personal Health Information on Mobile Devices
9.2.8	Access to POGO Email on Personal Mobile Devices
9.2.9	Secure Transfer of Records of Personal Health Information
9.2.9	Secure Transfer of Records of Personal Health Information external use
9.2.10	Password
9.2.11	Maintaining Reviewing System Control and Audit
9.2.13	Change Management
9.2.15	Acceptable Usage
9.2.17	Information Security Incident Management Process Policy
9.2.18	Confidentiality and Security of Data
9.2.19	Document Shredding
9.2.20	Secured Faxes
9.2.21	Encryption
9.2.22	Telephone Messages Containing Personal Health Information
9.2.24	Anti-Virus Spam
9.2.26	Access to POGONIS on Weekends
9.2.27	Small Cell
9.2.28	Inventory of Personal Health Information in secure bin

9.3 Human Resources Policies

Policy Number	Policy Title
9.3.1	Privacy and Security Training Policy
9.3.2	Confidentiality and Non-Disclosure Agreement
9.3.3	Delegation of Roles and Responsibilities
9.3.4	Termination or Cessation of Employment or Contractual Relationship
9.3.6	Disciplinary Action- Privacy Breach
9.3.26	Remote Access

9.4 Organizational Policies

Policy Number	Policy Title
9.4.1	Privacy Governance and Accountability Framework
9.4.3	Terms of Reference for Committees with Roles with Respect to the Privacy and Security Program
9.4.4	Corporate Risk Management Framework
9.4.5	Corporate Risk Register
9.4.6	Consolidated Log of Recommendations
9.4.7	Business Continuity and Disaster Recovery Plan
9.4.9	Presentation Release Form
9.4.10	Email Policy
9.4.12	BCDR Plan Essential Services
9.4.13	Gift Acceptance Policy

Appendix 2: Visitor Sign in Chart

Internal Agents – Do not need to sign in
• Employees • Students on Placement and Office Volunteers • Seconded Employees
External Agents – Do not need to sign in
• POGO Board Members • Researchers (only those who have a research agreement and have signed a confidentiality agreement with POGO) • Committee/Sub-committee Members (only those who have signed a confidentiality agreement) • POGO Interlink Nurses • POGO Counsellors • POGO Satellite Nurse Coordinators • POGO Satellite Clinic Nurses • POGONIS Data Managers • POGO Financial Assistance Data Managers • POGO AfterCare Data Managers • Members of the POGO Corporation
Visitors – Do need to sign in. Those who are not Agents, include:
• An individual who is attending a meeting or visiting, even if they will only be in the boardroom • Government Personnel • POGO Transitions Program Clients/Parents/Family Members (These visitors need only sign in using their initials; a POGO Counsellor will sign their own name on behalf of their Visitor) • Consultants (even if they have signed a non-disclosure and/or POGO's confidentiality agreement) • Guest Speakers • Job Candidates • Committee/Sub-committee Members (only those who have not signed a confidentiality agreement) • Researchers (only those who do NOT have a research agreement and have NOT signed a confidentiality agreement with POGO)

Appendix 3: POGO System Review 2016-2019

POGO System/Security Audits

Biweekly on Monday by POGO System Administrator
(77 audits in total over a period of 3 years)

Date	Firewall	Domain Controllers	Email servers	RDP server	RDP Gateway	FTP server	File servers	Backup Server	AV and Software Updates server	UPSs	Virtual Hosts	Proxy Servers	Network switches	POGO Website
	Syslog server logs	Windows Event Logs	Windows Event Logs and Antivirus alerts	Windows Event Logs	Windows Event Logs	Windows Event Logs and FTP server logs	Windows Event Logs	Windows Event Logs and Backup server alerts	SCCM server alerts	UPS alerts	Windows Event Logs and HP logs	System Console and email alerts	Network switches alerts	Wordfence plug-in alerts
2016-11-07	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2016-11-21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2016-12-05	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2016-12-19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-01-09	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-01-23	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-02-06	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-02-20	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-03-06	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-03-20	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-04-03	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-04-17	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-05-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-05-15	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Date	Firewall	Domain Controllers	Email servers	RDP server	RDP Gateway	FTP server	File servers	Backup Server	AV and Software Updates server	UPSs	Virtual Hosts	Proxy Servers	Network switches	POGO Website
	Syslog server logs	Windows Event Logs	Windows Event Logs and Antivirus alerts	Windows Event Logs	Windows Event Logs	Windows Event Logs and FTP server logs	Windows Event Logs	Windows Event Logs and Backup server alerts	SCCM server alerts	UPS alerts	Windows Event Logs and HP logs	System Console and email alerts	Network switches alerts	Wordfence plug-in alerts
2017-05-29	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-06-12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-06-26	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-07-10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-07-24	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-08-07	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-08-21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-09-05	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-09-18	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-10-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-10-16	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-10-30	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-11-13	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-11-27	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-12-04	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2017-12-18	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-01-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-01-15	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-01-29	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-02-12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-02-26	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Date	Firewall	Domain Controllers	Email servers	RDP server	RDP Gateway	FTP server	File servers	Backup Server	AV and Software Updates server	UPSs	Virtual Hosts	Proxy Servers	Network switches	POGO Website
	Syslog server logs	Windows Event Logs	Windows Event Logs and Antivirus alerts	Windows Event Logs	Windows Event Logs	Windows Event Logs and FTP server logs	Windows Event Logs	Windows Event Logs and Backup server alerts	SCCM server alerts	UPS alerts	Windows Event Logs and HP logs	System Console and email alerts	Network switches alerts	Wordfence plug-in alerts
2018-03-12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-03-26	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-04-09	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-04-23	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-05-07	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-05-21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-06-04	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-06-18	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-07-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-07-16	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-07-30	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-08-13	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-08-27	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-09-10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-09-24	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-10-08	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-10-22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-11-05	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-11-19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-12-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2018-12-31	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Date	Firewall	Domain Controllers	Email servers	RDP server	RDP Gateway	FTP server	File servers	Backup Server	AV and Software Updates server	UPSs	Virtual Hosts	Proxy Servers	Network switches	POGO Website
	Syslog server logs	Windows Event Logs	Windows Event Logs and Antivirus alerts	Windows Event Logs	Windows Event Logs	Windows Event Logs and FTP server logs	Windows Event Logs	Windows Event Logs and Backup server alerts	SCCM server alerts	UPS alerts	Windows Event Logs and HP logs	System Console and email alerts	Network switches alerts	Wordfence plug-in alerts
2019-01-14	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-01-28	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-02-11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-02-25	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-03-11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-03-25	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-04-08	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-04-22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-05-06	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-05-20	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-06-03	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-06-17	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-07-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-07-15	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-07-29	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-08-12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-08-26	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-09-09	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-09-23	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-10-07	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2019-10-21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Appendix 4: POGO POGONIS Security Audit Review

POGONIS Security Audit

Biweekly on Tuesday by POGO Database Administrator (73 audits in total over a period of 3 years)

Date	Review Period		
2016-11-08	2016-10-19	through	2016-11-08
2016-11-25	2016-11-08	through	2016-11-25
2016-12-16	2016-11-25	through	2016-12-16
2017-01-09	2016-12-16	through	2017-01-09
2017-01-17	2017-01-09	through	2017-01-17
2017-01-31	2017-01-17	through	2017-01-31
2017-02-14	2017-01-31	through	2017-02-14
2017-03-06	2017-02-14	through	2017-03-06
2017-03-24	2017-03-06	through	2017-03-24
2017-04-28	2017-03-24	through	2017-04-28
2017-05-24	2017-04-28	through	2017-05-24
2017-06-06	2017-05-24	through	2017-06-06
2017-06-20	2017-06-06	through	2017-06-20
2017-07-04	2017-06-20	through	2017-07-04
2017-07-18	2017-07-04	through	2017-07-18
2017-08-01	2017-07-18	through	2017-08-01
2017-08-15	2017-08-01	through	2017-08-15
2017-08-29	2017-08-15	through	2017-08-29
2017-09-12	2017-08-29	through	2017-09-12
2017-09-26	2017-09-12	through	2017-09-26
2017-10-17	2017-09-26	through	2017-10-17
2017-10-24	2017-10-17	through	2017-10-24

Date	Review Period		
2017-11-08	2017-10-24	through	2017-11-08
2017-11-21	2017-11-08	through	2017-11-21
2017-12-05	2017-11-21	through	2017-12-05
2017-12-20	2017-12-05	through	2017-12-20
2018-01-02	2017-12-20	through	2018-01-02
2018-01-16	2018-01-02	through	2018-01-16
2018-01-30	2018-01-16	through	2018-01-30
2018-02-13	2018-01-30	through	2018-02-13
2018-02-27	2018-02-13	through	2018-02-27
2018-03-13	2018-02-27	through	2018-03-13
2018-03-27	2018-03-13	through	2018-03-27
2018-04-10	2018-03-27	through	2018-04-10
2018-04-24	2018-04-10	through	2018-04-24
2018-05-09	2018-04-24	through	2018-05-09
2018-05-23	2018-05-09	through	2018-05-23
2018-06-05	2018-05-23	through	2018-06-05
2018-06-19	2018-06-05	through	2018-06-19
2018-07-03	2018-06-19	through	2018-07-03
2018-07-17	2018-07-03	through	2018-07-17
2018-08-23	2018-07-17	through	2018-08-23
2018-08-28	2018-08-23	through	2018-08-28
2018-09-11	2018-08-28	through	2018-09-11
2018-09-25	2018-09-11	through	2018-09-25
2018-10-09	2018-09-25	through	2018-10-09
2018-10-23	2018-10-09	through	2018-10-23
2018-11-06	2018-10-23	through	2018-11-06
2018-11-20	2018-11-06	through	2018-11-20
2018-12-04	2018-11-20	through	2018-12-04

Date	Review Period		
2018-12-18	2018-12-04	through	2018-12-18
2019-01-02	2018-12-18	through	2019-01-02
2019-01-15	2019-01-02	through	2019-01-15
2019-01-22	2019-01-15	through	2019-01-22
2019-01-29	2019-01-22	through	2019-01-29
2019-02-12	2019-01-29	through	2019-02-12
2019-02-26	2019-02-12	through	2019-02-26
2019-03-13	2019-02-26	through	2019-03-13
2019-03-26	2019-03-13	through	2019-03-26
2019-04-09	2019-03-26	through	2019-04-09
2019-04-23	2019-04-09	through	2019-04-23
2019-05-07	2019-04-23	through	2019-05-07
2019-05-22	2019-05-07	through	2019-05-22
2019-06-04	2019-05-22	through	2019-06-04
2019-06-18	2019-06-04	through	2019-06-18
2019-07-03	2019-06-18	through	2019-07-03
2019-07-16	2019-07-03	through	2019-07-16
2019-08-08	2019-07-16	through	2019-08-08
2019-08-14	2019-08-08	through	2019-08-14
2019-08-27	2019-08-14	through	2019-08-27
2019-09-11	2019-08-27	through	2019-09-11
2019-09-24	2019-09-11	through	2019-09-24
2019-10-08	2019-09-24	through	2019-10-08