POGO
PEDIATRIC ONCOLOGY GROUP OF ONTARIO

COLLABORATING FOR KIDS WITH CANCER SINCE 1983

October 27, 2011

Dr. Ann Cavoukian, PhD
Information and Privacy Commissioner of Ontario
2 Bloor Street East
Suite 1400
Toronto ON M4W 1A8

Dear Dr. Cavoukian:

The Pediatric Oncology Group of Ontario (POGO) is pleased to submit its revised report electronically in compliance with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, issued by your office on April 19, 2010.

We have also included Dr. Corin Greenberg's signed and notarized affidavit.

We would like to thank Ms Judith Goldstein, Legal Counsel from your office for her guidance and direction in clarifying questions pertaining to the manual and facilitating its completion. A special thank you must be given to POGO Senior Management, the POGO Information Technology Team, and to Ms. Kathleen Standring, (our Administrative Assistant), for all their assistance in writing, editing, reviewing and preparing this revised report.

While POGO is in compliance with the majority of the requirements as set out in the manual, we have identified the areas still to be completed and the date to be completed in Appendix 4 - Compliance Timeline.

We understand your requirement that the detailed written report and sworn affidavit submitted by POGO will be publicly available on the IPC website as well as ours. While we are comfortable posting Parts 1 to 4 of the Report and the Sworn Affidavit, we note that the public posting of Appendix 1: Privacy, Security and Other Indicators is a matter we are very concerned about given the sensitivity and security of certain information within this document. Therefore, the posted version of the Indicators document has been adapted and redacted as appropriate, to remove particularly sensitive details, such as personally identifiable information and other information that would potentially adversely impact our information security safeguards if published.

We remain confident that POGO's status will be renewed and look forward to your response.

Best regards,

Bruna DiMonte, RN, BScN
Senior Database Administrator &
Co-Privacy Officer

Madeline Riehl, MHSc
Senior Associate Research and Planning &
Co-Privacy Officer

cc.
Dr. Corin Greenberg, Executive Director, Pediatric Oncology Group of Ontario
Judith Goldstein, Legal Counsel, IPC, Ontario

480 University Avenue
Suite 1014
Toronto, Ontario
Canada M5G 1V2
tel. 416-592-1232
toll-free. 1-855-FOR POGO
(1-855-367-7646)
fax 416-592-1285
www.pogo.ca

Pediatric Oncology Group of Ontario

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

Privacy and Security Report to the Information and Privacy Commissioner of Ontario

Table of Contents

Part 2 – SECURITY DOCUMENTATION

Part 4- OGANIZATIONAL AND OTHER DOCUMENTATION

APPENDICES

Part 1- Privacy Documentation

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 advisor 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;
- to operate as a collegial alliance of specialty programs, community services, parents, survivors, and the voluntary sector;
- to 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;
- to identify, address, and resolve issues, gaps, and obstacles to state-of-the-art childhood cancer care;
- to 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;
- to bring about family-centred, coordinated, and well-integrated childhood cancer system for Ontario;
- to manage provincial programs, including the Satellite, AfterCare, and Interlink Programs, which are delivered by academic teaching and community hospitals;
- to provide and regularly renew evidence and consensus guidelines for childhood cancer control;
- to provide ongoing knowledge transfer, education, and professional updates to support best practices and raise awareness about childhood cancer;
- to stimulate scientifically credible, multi- and inter-disciplinary research that refines knowledge and supports evidence-based policy; and
- to provide essential supports for children, survivors, and families.

To support our mandate, POGO began collecting 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); and

- 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, we 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:

- evaluating, monitoring, and assuring adequate staffing levels at Ontario's tertiary cancer centres;
- 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 Pediatric Oncology Financial Assistance Program (POFAP);
- 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 frequent educational opportunities for health care professionals, including the annual POGO Symposium, Satellite Education Days, and SAVTI Education Days; and
- the POGO Research Unit (PRU), whose mandate is to: stimulate and promote pediatric oncology research; engage in collaborative multi-disciplinary investigations of childhood cancer; 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) has been 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:

- be able 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, following a second statutory review by the IPC, POGO had its status renewed on October 31, 2008. While the IPC was satisfied that POGO had practices and procedures in place that sufficiently protected the privacy of individuals whose personal health information it received and sufficiently protected the confidentiality of that information in both instances, the IPC did make certain recommendations to further enhance these practices and procedures. With respect to the recommendations made during the 2008 review to improve and bolster POGO's Privacy and Security Programs, the majority have been addressed and for the remainder of the outstanding items a timeline is attached to this document.

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

Agents

- individuals who act for, or on behalf of POGO, and who may or may not be employees of POGO and who include POGO staff, the POGO Board, researchers, volunteers, or those who are seconded employees to POGO.

Third Parties

- are agents (individuals or organizations) who provide service to or on behalf of POGO in the role of contractors or consultants.

Privacy Team

- includes the POGO Privacy Officers and administrative support personnel.

Information Technology (IT) Team

- includes the Information Systems Manager, Senior Database Administrator, and Database Administrators/Analysts/Programmers.

POGO Tertiary Pediatric Oncology Hospital Partners

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

POGO Satellite Community Hospitals

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

POGO AfterCare Adult Programs

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

Privacy and Data Security Code

- the 10 tenets of POGO's Privacy Program

Privacy and Data Security Procedures

- the 10 tenets of POGO's Privacy Program and the associated procedures.

Privacy and Security Policies and Procedures Manual

- a manual that contains all of POGO's privacy and security policies and procedures.

The Privacy Program

- refers to all of POGO's privacy program components (e.g. organizational security measures, audits, privacy impact assessments, privacy training, etc), and policies and procedures as outlined in POGO's *Privacy and Data Security Code*, *Privacy and Data Security Procedures* , and POGO's *Privacy and Security Policies and Procedures Manual.*

Prescribed Entities

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

Data Security Committee

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

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 receives and uses 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 its overarching documents, POGO's *Privacy and Data Security Code* and POGO's *Privacy and Data Security Procedures*. In addition to these overarching privacy documents, POGO's Privacy Program is further articulated in POGO's *Privacy and Security Policies and Procedures Manual*. (These three 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 evidences 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 Executive Director of POGO is ultimately accountable for ensuring compliance with the *Act* and its regulations, and for ensuring compliance with its privacy and security policies and procedures. The Executive Director reports to the Board of Directors of POGO, which is comprised of POGO tertiary pediatric hospital Program Directors, plus other selected members who contribute specific area expertise (e.g. other health care professionals, human resources, financial management, etc.).

The Privacy Program, which includes the security program, identifies the positions of the Privacy Officers as having the overall responsibility to manage the Privacy Program, and POGO's Information Systems Manager 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 two positions. POGO's Privacy Officers report to the Executive Director of POGO. POGO's Information Systems Manager reports to the Privacy Officers.

Collection of Personal Health Information

The Privacy Program describes 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 Programs and other prescribed entities), and from which it collects the information. The Privacy Program further specifies 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 states that POGO will not collect personal health information if other information will serve the intended purpose. The Privacy Program also states that POGO only collects personal health information for its stated purpose and that it collects the minimum amount of personal health information required to fulfill its stated purpose. POGO's *Privacy and Security Policies and Procedures Manual,* POGO's *Privacy and Data Security Code, and* POGO's *Privacy and Data Security Procedures* 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 Program includes the requirement to maintain a list of its data holdings of personal health information and identifies the Privacy Officers as the contacts 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 also describes 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. These policies are outlined in the POGO *Privacy and Data Security Procedures* within Principle 2 (*Identifying Purposes*) and within Principle 4 (*Limiting Collection*).

The Privacy Program also articulates 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 identifies 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 Privacy Program distinguishes 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, the POGO *Privacy and Data Security Procedures* sets 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 addresses 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 also describes 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), separation of networks, passwords, encryption, audit logs, data modification logs, backup and recovery systems.
(d) De-Identification: personal health information is de-identified, and is further de-identified by removing data fields (e.g. name, health card number, date of birth, etc.).

Inquiries, Concerns, or Complaints Related to Information Practices

The Privacy Program identifies the Privacy Officers 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 Officers 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 lodging inquiries or complaints.

The Privacy Policy 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 be 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.

The policies state that it is the responsibility of the Privacy Officers to initiate and coordinate the review process, and that in the event that proposed changes represent a material change to daily operations, the results and recommendations of the review will be forwarded to POGO's Data Security Committee for review and approval before the changes are implemented.

In undertaking the review and determining whether amendments and/or new privacy policies, procedures, and practices are necessary, POGO's Policy #7 (*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 Officers are responsible for communicating the amended or newly developed privacy policies, procedures, and practices. For staff, the Privacy Officers are guided by POGO's Policy #9 (*Staff Education and Training Policy*), which clearly stipulates that the Privacy Officers will be responsible for communicating the amended or newly developed privacy policies, procedures, and practices. The Privacy Program also identifies that the Privacy Officers are responsible for ensuring all documents available to the public and other stakeholders are current and continue to be made available to the public and other stakeholders on the POGO website.

Compliance with the *Privacy and Security Policies and Procedures Manual* is mandatory for all agents of POGO and is monitored by POGO's Privacy Officers. 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 Officers 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

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

POGO's *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, 2008) 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
5. A list of the data holdings of personal health information maintained by POGO
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 its *Privacy and Data Security Procedures*, and policies outside of the *Privacy and Data Security Code* and privacy impact assessments of data holdings containing personal health information to the public and other stakeholders.

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 type of personal health information collected
4. The organizations 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
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
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 to the transparency of policies and procedures, Principle 8 (*Openness*) states that the Executive Director 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 has policies and procedures that identify the purposes for which personal health information is collected, the nature of the personal health information that is collected, the health care custodians from whom the personal health information is 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 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 Programs and other prescribed entities).

POGO enters into data sharing agreements with its tertiary pediatric oncology hospital partners, POGO AfterCare Adult Programs, and other prescribed entities and maintains general 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 Officers monitor compliance with the terms of the data sharing agreements and other agreements and those terms are ultimately enforced by the POGO Board of Directors.

Compliance with the policies and procedures for the collection of personal health information are audited in accordance with POGO's policies and procedures in respect of POGO's Privacy Audit Program, which state that privacy audits are carried out annually at minimum by the Privacy Officers.

POGO's policies and procedures for managing privacy breaches require that agents of POGO notify the Privacy Officers 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), which have remained unchanged since that time. No additional personal health information data elements are anticipated.

In 2010, POGO secured two grants that allow POGO to retrospectively add personal health information data elements (treatment and outcome information) to the POGONIS database on the cases diagnosed in 1985 to 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 and POGO's Medical

Director, and were subsequently endorsed by the Program Directors from each of the POGO tertiary pediatric oncology hospitals.

In addition, POGO maintains five other databases which collect personal health information from its POGO tertiary pediatric oncology hospital partners, from POGO Satellite Community Hospitals and AfterCare Adult programs and from other prescribed entities. 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 (POFAP);
- The Interlink Community Care Nursing Program;
- Satellite service utilization; and
- AfterCare care and service delivery.

POGO's policies and procedures outline that 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 programs and other prescribed entities and the general 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 outline the purpose and obligations of each partner to achieve compliance with data collection.

In addition, the policy and procedures set out the criteria that must be considered for determining whether to approve the collection of personal health information. The criteria require 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 determining whether 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 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 and other prescribed entities or a general POGO/hospital agreements such as those it maintains with the POGO Satellite Community Hospitals and that the providers of the information 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 Executive Director 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 housed within a secured data centre with restricted access, in accordance with the policies and 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, 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 faxed, and/or encrypted electronic transfer in accordance with the policies and procedures Policy #29 (*Secure Transfer of Personal Health Information*).

Secure Return or Disposal

POGO's privacy policies and procedures identifies POGO's Privacy Officers 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 the 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 #29 (*Secure Transfer of Personal Health Information)*

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 the policies and procedures for the secure disposal of personal health information.

5. List of Data Holdings Containing Personal Health Information

POGO maintains an up-to date list of, and brief 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 that the Privacy Officers have been delegated overall responsibility 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 the Privacy Officers prepare the statements of purpose in concert with the POGO Program Manager responsible for the data holding. Once finalized, the statement of purpose is reviewed and approved by POGO's Executive Director.

The statements of purpose shall be provided to the health information custodians 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 Officers are responsible for reviewing the statements of purpose and 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 programs 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 Officers. 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 the Policy and Procedure in Respect of Privacy Audits, that policies and procedures will be audited annually or sooner if required, and that the POGO Privacy Officers are 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 #4 (*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 Privacy Officers draft 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 the prescribed entity 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, and 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 #14 (*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 a single agent 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 the Policy #16 (*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 #10 (*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* outline that the Senior Database Administrator and POGO's 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 the 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 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 sets 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 pre-determined expiry dates. At a minimum, the Privacy Officers review the expiry dates one year from the date that approval was granted.

In the *Privacy and Security Policies and Procedures Manual*, Policy #14 (*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 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 #14 (*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 Officers 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 Officers 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, if any; the Privacy Officers who are responsible for completing, providing and/or executing the documentation; the Privacy Officers to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also identifies the Privacy Officers 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 #23 (*Termination or Cessation of the Employment or Contractual Relationship*).

Secure Retention

The policy and procedures require an agent granted approval to access and use personal health information to securely retain the records of personal health information in compliance with Policy #3 (*Procedures for 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 #3 (*Procedures for 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 #40 (*Privacy Audits*).

The purpose of the audit is to ensure that agents granted such approval continue to be employed or retained by the prescribed person or prescribed entity 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 Officers as the agents 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 #4 (*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 Program Principle 5 (*Limiting Use, Disclosure and Retention*) and Policy #27 (*Process for 44 and 45 Projects*) 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 policy and its procedures and address how the POGO Privacy Officers enforce compliance and the consequences of breach. POGO policies and procedures also stipulate that compliance will be audited in accordance with Policy #40 (*Privacy Audits*), and states that policies and procedures will be audited by the Privacy Officers annually to ensure compliance with the policy and its procedures.

The policy and procedures also requires agents to notify the Privacy Officers at the first reasonable opportunity, in accordance with Policy #4 (*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 #27 (*Process for 44 and 45 Projects*) 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 #27 (*Process for 44 and 45 Projects*) clearly 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*, as the case may be. The criteria that must be considered are outlined in Policy #27 and determines 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 Officers as responsible for, and the procedure which is to be followed when making this determination

Review and Approval Process

Policy #27 (*Process for 44 and 45 Projects*) identifies the Privacy Officers and the 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 Officers, 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 Officers 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 Officers and Medical Director 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 research ethics board, and to ensure that the prescribed entity is in receipt of a copy of the decision of the research ethics board approving the written research plan.

In addition, prior to any approval of the use of personal health information for research purposes, the Privacy Officers and Medical Director responsible for determining whether to approve or deny the request ensure that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board. The Privacy Officers and Medical Director responsible also 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.

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 by the Privacy Officers with regard to the personal health information for research purposes that comply with subsections 44(6) (a) to (f) of the *Act*.

In addition, the Privacy Officers are 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* Policy #3 (*Retention, Return and Destruction*) requires 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 research ethics board.

Secure Return or Disposal

Policy #3 (*Retention, Return and Destruction*) 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 research ethics board.

If the records are required to be securely returned to another agent at POGO, Policy #3 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 Privacy Officers at POGO.

If the records of personal health information are required to be disposed of in a secure manner, Policy #3 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, must require a certificate of destruction to be provided, must identify the Privacy Officers to whom the certificate of destruction must be provided, and must identify 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 the records of personal health information securely disposed of, and the date, time 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 #16 (*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 Officers as the agents 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 #27 (*Process for 44 and 45 Projects*) requires that a log is maintained of the approved uses of personal health information for research purposes and identify the Privacy Team as responsible for maintaining such a log. The policy also outlines where written research plans, copies of the decisions of research ethics boards, 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

This section is not applicable to POGO

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 research ethics 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 data fields, elements and 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 research ethics board;
- The date, time, location, and method by which the records must be returned, disposed of, or de-identified
- 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 and time 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, 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 Procedures* and Policy #27 (*Process for 44 and 45 Projects)* identifies when and under what circumstances personal health information is permitted to be disclosed for purposes other than research (45 purposes).

POGO's *Privacy and Data Security Code and* POGO's *Privacy and Data Security Procedures* articulates 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 Officers enforce compliance and address the consequences of any breaches that may occur. Policy #40 (*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 Officers 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 #4 (*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 #27 (*Process for 44 and 45 Projects*) permits 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. 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 #27 (*Process for 44 and 45 Projects*) identifies the Privacy Officers and Medical Director 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 Officers to whom this documentation must be provided; and the required content of the documentation.

POGO's *Privacy and Data Security Procedures* and Policy #27 addresses the requirements that must be satisfied and the criteria that must be considered by the Privacy Officers and the Medical Director 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 Officers and Medical Director 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.

POGO's *Privacy and Data Security Code, and* POGO's *Privacy and Data Security Procedures* require the Privacy Officers and Medical Director 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 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*) sets out the manner in which the decision approving or denying the request for the disclosure of personal health 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.

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 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, 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 #41 (*Execution of Data Sharing Agreements*) identifies the Privacy Officers 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*, Policy #29 (*Secure Transfer of Records of PHI Submission Guidelines*) requires records of personal health information to be transferred in a secure manner.

Secure Return or Disposal

Policy #3 (*Retention, Return, and Destruction of Data)* identifies the Privacy Officers 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 Officers 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 #27 (*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 Officers who are responsible for retaining this documentation.

Where the Disclosure of Personal Health Information is not Permitted

This section does not apply to POGO.

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 #27 (Process for 44 and 45 Projects) identifies 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 *Privacy and Security Policies and Procedures Manual* and that POGO's Privacy Officers enforce compliance and address the consequences of any breach. Policy #40 (*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

Officers 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 #4 (*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 #27 (*Process for 44 and 45 Projects*) 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 #27 (*Process for 44 and 45 Projects*) identifies the Privacy Officers and Medical Director 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 #27 (*Process for 44 and 45 Projects*) addresses the requirements that must be satisfied and the criteria that must be considered by the Privacy Officers and the 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 Officers and Medical Director 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 research ethics board 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 Officers and Medical Director 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 research ethics board. The Privacy Officers 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 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 Data Security Code, and* POGO's *Privacy and Data Security Procedures*, Principle 1 (*Accountability*), requires a Researcher Agreement to be executed 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* sets out that the Privacy Officers are 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 #29 (*Secure Transfer of Records of PHI Submission Guidelines*) requires records of personal health information to be transferred in a secure manner.

Secure Return or Disposal

Policy #3 (*Retention, Return, and Destruction of Data*) identifies the Privacy Officers 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

Policy #27 (*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 research purposes is retained, and the Privacy Officers who are responsible for retaining this documentation.

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

This section does not apply to POGO.

14. Template Research Agreement

A Researcher Agreement 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 the personal health information is being disclosed by the prescribed person or prescribed entity and the purposes for which the personal health information may be used or disclosed by the researcher must be identified in the Researcher Agreement, as must 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 research ethics board 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 research ethics board.

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 research ethics board.

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 research ethics board 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 research ethics board and with the conditions, if any, specified by the research ethics board 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 #29 (*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 is also identified, including 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 research ethics board.

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 #29 (*Secure Retention of Records of Personal Health Information*) and to the written research plan approved by the research ethics board.

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 research ethics board.

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 research ethics board.

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 Privacy Officers of POGO.

In identifying the secure manner in which the records of personal health information will be returned, regard may be had to Policy #3 (*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 #3 (*Retention, Return, and Destruction of Data*) implemented by POGO.

Further, the Researcher Agreement identifies the Privacy Officers 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 #16 (*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 the time frame following the retention period set out in the Researcher Agreement within which the written confirmation must be provided and the Privacy Officers of POGO to whom the written confirmation must be provided.

Notification

At a minimum, the Researcher Agreement requires the researcher to notify the Privacy Officers, 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 Officers 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 research ethics board, 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 research ethics board 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 #41 (*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 Agreements 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 Officers who are 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 Officers 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 Officers 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 Officers who are responsible for ensuring that a Data Sharing Agreement is executed, must also be satisfied that the collection was approved in accordance with Principle 5.

Policy #41 (*Execution of Data Sharing Agreements*) also sets out that a log of Data Sharing Agreements be maintained and identifies the Privacy Officers 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.

All agents of POGO must understand that compliance will be audited in accordance with Policy #40 (*Privacy Audits*) on an annual basis or as required, and that the Privacy Officers will be responsible for conducting the audit.

POGO's policies also require agents to notify the Privacy Officers at the first reasonable opportunity, in accordance with Policy #4 (*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 #41 (*Execution of Data Sharing Agreements*) that, at a minimum, addresses the matters set out below.

General Provisions

POGO's Data Sharing Agreements describes 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 #29 (*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 Officers ensure 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 #3 (*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 Officers 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 may be had to Policy #29 (*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 #3 (*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 Officers, 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 Officers. 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 #42 (*Agreement for All 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 *Template Agreement for All Third Party Service Providers*.

The policy also identifies the Privacy Officers who are 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 Officers are identified in the policy as the agents 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 Officers are responsible for implementing this process and the time frame following termination within which this process must be implemented.

The policy and procedures also requires that a log be maintained of all agreements executed with third party service providers and identifies the Privacy Officers as 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 Officers.

POGO requires agents to comply with specific policies and procedures as outlined in each Third Party Service Agreement and set out how the Privacy Officers enforce compliance and the consequences of breach. Compliance will be audited in accordance with principles within Policy #40 (*Privacy Audits*) specific to Third Parties and will be audited by the Privacy Officers annually to ensure compliance with the policy and its procedures.

The policy and procedures also require Third Parties to notify the Privacy Officers at the first reasonable opportunity, in accordance with Policy #4 (*Privacy Breach and Incident Management*) if a third party agent 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 is 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 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.

If 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

The agreement identifies the purposes, if any, for which the third party service provider is permitted to disclose 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 disclose personal health information, POGO ensures that each disclosure identified in the agreement is consistent with the disclosures of personal health information permitted by the *Act* and its regulation. In this regard, the agreement prohibits the third party service provider from disclosing personal health information except as permitted in the agreement or as required by law, from disclosing personal health information if other information will serve the purpose and from disclosing more personal health information than is reasonably necessary to meet the purpose.

In the case of an electronic service provider that is not an agent of POGO, the agreement prohibits the electronic service provider from disclosing personal health information to which it has access in the course of providing services except as required by law. At the present time, POGO does not have an electronic service provider who is not an agent of POGO.

Secure Transfer

Where it is necessary to transfer records of personal health information to or from POGO, 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 #29 (*Secure Transfer of Records of Personal Health Information*) implemented by POGO.

In addition, where the retention of records of personal health information 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, for the purposes of the agreement, 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, 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 #3 (*Retention, Return, and Destruction of Data*) implemented by POGO.

Currently 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 currently require any third party service provider to maintain a detailed inventory of records of personal health information, in regard to such retention.

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 #29 (*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 of.

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's Policy #3 (*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

This section is not applicable to POGO.

Notification

At a minimum, the agreement requires the third party service provider to notify POGO 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 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 be auditing 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 Privacy 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 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.
- 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;
- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to the personal health information was terminated or the date by which the records of personal health information must be returned or disposed of or access terminated.

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

POGO's *Privacy and Security Policies and Procedures* and Policy #10 (*Confidentiality and Security of Data*) address linkages of records of personal health information.

These policies and procedures describe that POGO permits the linkage of records of personal health information, and the purposes for which 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 has 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 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 prescribed entities 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 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 45 prescribed entity, researcher or organization, the policy and procedures requires that the disclosure be approved pursuant to Policy #27 (*Process for 44 and 45 Projects*), and Policy #41 (*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 #27 (*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 #16 (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 requires that linked records of personal health information be retained in compliance with the Policy #3 (*Retention, Return, and Destruction of Data*) until they are de-identified and/or aggregated pursuant to the Policy #16 (*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 #3 (*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 #40 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as those 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 #4 (*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 Officers as those 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 for 45 and 44 linkage purposes. 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 #16 (*De-Identifying Personal Health Information*) and POGO's *Privacy and Data Security Procedures* , Principle 5 (*Limiting Use, Disclosure and Retention*) requires that personal health information not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose.

With respect to cell-sizes of less than five and the exceptions thereto, Policy #26 (*Small Cell*) sets out 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 provides 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 #16. 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 #16. 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 identify the mechanisms implemented to ensure that other 45 prescribed entities 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 Officers will enforce compliance and the consequences of breach. The policy and procedures stipulate that compliance will be audited in accordance with Policy #40 (*Privacy Audits*) annually, and the audit will be conducted by the Privacy officers 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 #4 (*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 #28 (*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 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.

When there are limited and specific circumstances in which privacy impact assessments are not required to be conducted 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, the policy and procedures outline the rationale why privacy impact assessments are not required. The policy and procedures further identify the Privacy Officers as those responsible for making this determination and requires them to ensure this determination and the reasons for the determination are documented.

The policy and procedures also sets out that privacy impact assessments are conducted annually. 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 Officers as the agents responsible 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 Officers as the agents 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 Officers have been delegated overall responsibility for both the privacy and security programs, and are 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 Officers as the agents 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 #40 (*Privacy Audits*) which sets out the frequency with which the policy and procedures will be audited and that the

Privacy Officers are responsible for conducting the audit, and for ensuring compliance with the policy and its procedures.

The policy and procedures also requires agents to notify POGO at the first reasonable opportunity, in accordance with the Policy #4 (*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 Officers 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 Officers as the agents 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 the Privacy Officers who are 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 #40 (*Privacy Audits*) sets 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 Officers as the agents 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 Officers as the agents 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 Officers as the agents responsible for completing, providing, and/or executing the documentation.

The Privacy Officers are identified has having been delegated overall responsibility to manage the privacy program and the security program.

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 Officers who are the agents responsible for completing, providing, and/or executing 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 Officers as the agents 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 Executive Director.

The policy and procedures further require that a log be maintained of privacy audits and identifies the Privacy Officers 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 Officers are responsible for retaining this documentation.

The policy and procedures also require the Privacy Officers responsible for conducting the privacy audit, to notify the Executive Director and Medical Director of POGO at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the Policy #4 (*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 Officers as the agents 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 #4 (*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 suspected privacy breach.

In this regard, the policy and procedures identify the Privacy Officers as the agents who must be notified of the privacy breach or suspected privacy breach and provides contact information for the Privacy Officers who must be notified. The policy and procedures further stipulates 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 Officers 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 Officers responsible for making this determination are also identified.

The policy and procedures further address when senior management will be notified, including the Executive Director. This includes a discussion of the Privacy Officers who are 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 Officers 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 Officers 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 Officers who are 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 Officers who are responsible for reviewing the containment measures; the Privacy Officers 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 Officers as the agents 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 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 Officers as the agents 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 Officers as the agents 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 Officers to whom this documentation must be provided; and the required content of the documentation.
The Privacy Officers have been delegated the overall responsibility to manage the privacy program and the security program.

The policy and procedures also identify the Privacy Officers as the agents 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 Officers as the agents responsible for completing, providing, and/or executing the documentation, 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 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 Officers who are 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 Executive Director.

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 Officers 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 #40 (*Privacy Audits*), sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as the agents 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

POGO 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 Officers 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 Officers 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 Officers as the agents responsible 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 Officers as the agents 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 requires 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 Executive Director and Privacy Officers as the agents 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 Officers as the agents 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 Officers as the agents responsible for completing, providing, and/or executing the documentation, and the required content of the documentation.

The Privacy Officers have been delegated overall responsibility 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 agents 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 Officers as the agents responsible for completing, preparing, and/or executing the documentation, 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 Officers as the agents 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 Executive Director.

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 Officers are the agents 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 Officers who are responsible for providing the notification.

Further, the policy and procedures require that a log be maintained of privacy complaints and identifies the Privacy Officers 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 Officers who are 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 #40 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and procedures and Policy #4 (*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 Officers 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 Officers directly.

The policy and procedures further establish the process to be followed in receiving and responding to privacy inquiries. This includes the Privacy Officers as the agents 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 Officers has been delegated overall responsibility 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 #40 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited, and identifies the Privacy Officers as the agents 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 #4 (*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 these overarching information security documents: POGO's *Privacy and Data Security Code*, POGO's *Privacy and Data Security Procedures* and POGO's *Privacy and Security Policies and Procedures Manual.* These documents have been implemented in relation to personal health information received by POGO under the *Act*. The Privacy Program as well as POGO's Policy #32 (*Security Standards and Procedures*) requires that steps be taken to ensure that the 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's Policy #31 (*Threat and Risk Assessment)* requires 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 #31 establishes and documents a 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 #32 (*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's Policy #31 (*Threat and Risk Assessment*) effectively addresses the threats and risks identified, is amenable to independent verification, and is 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;

- Policies and procedures for the ongoing review of the security policies, procedures, and practices implemented (policy #7: *Review of Privacy and Security Policies and Procedures*);

- Policies and procedures for ensuring the physical security of the premises (Policy #2: *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 (Policy #3: *Retention, Return, and Destruction of Data*);

- Policies and procedures to establish access control and authorization including business requirements, user access management, user responsibilities, network access control, operating system access control, and application and information access control (Policy #32: *Security Standards and Procedures* and section 3.13 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 (*Policy #32: 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 (Policy #32: *Security Standards and Procedures*);

- Policies and procedures for network security management, including patch management and change management (Policy #32: *Security Standards and Procedures);*

- Policies and procedures related to the acceptable use of information technology (Policy #33: *Acceptable Use*);

- Poli*cies and procedures for back-up and* recovery (Policy #32: *Security Standards and Procedures*);

- Policies and procedures for information security breach management (Policy #36: *Information Security Breach Management*); and

- Policies and procedures to establish protection against malicious and mobile code (Policy #32: *Security Standards and Procedures*).

The Privacy Program together with POGO's Policy #32 (*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 #32 (*Security Standards and Procedures*), and POGO's Privacy 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 is enforced by the Privacy Officers and the IT Team. Policy #4 (*Privacy Breach and Incident Management*) indicates 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 in accordance with POGO's Privacy Audit Program and identifies the Privacy Officers together with the IT Team as the agents responsible for conducting the audit and for ensuring compliance with the policy.

Policy #4 (*Privacy Breach and Incident Management*) and Policy #36 (*Information Security Breach Management*) also requires agents to notify POGO at the first reasonable opportunity, if an agent breaches or believes there may have been a breach of this policy or any of the 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 #7 (*Review of Privacy and Security Policies and Procedures*) 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 #7 (*Review of Privacy and Security Policies and Procedures*) indicates that the Privacy Officers and the IT Team will undertake the review annually and will complete it in no more than 6 months. This policy and procedures also identify the Privacy Officers together with 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 Officers as the agents 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 #7 (*Review of Privacy and Security Policies and Procedures*) indicates that the Privacy Officers 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 Officers and the IT Team will be responsible for any such amendments or additions to the policy suite. Further, the Privacy Officers are responsible for communicating the changes or additions to its agents by email and/or verbally at staff meetings. The Privacy Officers ensure that 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 Executive Director through the Privacy Officers. 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 Audit Program, compliance will be audited on an annual basis and the Privacy Officers will be responsible for conducting the audit.

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

POGO's Policy #2 (*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's Policy #14 (*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 #14 outlines the premises of POGO be divided into four 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 Officers.

Policy #14 (*Levels of Access*), like all POGO privacy and security policies, requires agents of POGO to comply with its terms. Compliance is enforced by the Privacy Officers. The policy clarifies 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 *Levels of Access* policy, compliance is audited in accordance with POGO's Privacy Audit Program on an annual basis and the Privacy Officers are responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Policy #14 (*Levels of Access*) also requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #4 (*Privacy Breach and Incident Management*) if an agent breaches or believes that there may have been a breach of this policy or its associated procedures. Any breach of this policy will lead to a review of the incident by the POGO Privacy Officers and may result in disciplinary action as per Policy #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 security 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 #14 (*Levels of Access*).

Policy #14 (*Levels of Access*) identifies the Privacy Officers as the agents 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 #14. The Access Control Card Tracking Log is completed by the Privacy Team who is the agents to whom the documentation must be provided and includes the required content of the documentation.

Policy #14 further addresses the criteria that must be considered by the Privacy Officers 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 Officers who are responsible for making the determination; and the required content of the documentation.

Policy #14 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's Policy #2 (*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 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 #2.

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 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 #30 (*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 POGO on or before the date of termination of their employment, contractual or other relationship.

Policy #30 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 #14 (*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 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 #14 (*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 *Levels of Access* policy identifies the Privacy Officers as the agents 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 #14 (*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 is a small organization and has determined it does not require a formal visitor tracking procedure. POGO's procedure for screening and supervising visitors to the POGO premises is the responsibility of the POGO Receptionist/Administrative Assistant. This staff member receives the visitor, notifies the staff member who they are meeting, and either escorts the visitor to the staff office or the staff member comes to reception to greet the visitor. Board meetings and attendance are tracked via the corporate calendar.

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 Policy #3 (*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 must ensure 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 research ethics board. 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 Officers as the agents 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 the necessary steps 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.

Currently 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 currently require any third party service provider to maintain a detailed inventory of records of personal health information, in regard to such retention.

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

Policy #35 (*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 Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as the agents responsible for conducting an annual audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #4 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

Policy #35 (*Personal Health Information on Mobile Devices*) also sets out the circumstances in which POGO permits personal health information to be retained on a mobile device.

Personal health information may be stored on a mobile device under the following circumstances:

1. Personal health information is stored on a mobile devices for 45 purposes when data is:
   - stored on backup tape and transferred to offsite secure storage;
   - transferred to the Linkage System for analysis;
   - transported to another 45 entity for linkage purposes;
   - being collected on a mobile device; and
   - transferred to offsite affiliates conducting analysis and reporting for POGO.

2. For 44 purposes, when data is transferred to the research team. All research requirements need to be met prior to transfer.

Approval Process

Policy #35 (*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 Officers as the agents 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 Officers 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 Officers 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 Officers who are 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 requires the Privacy Officers to determine whether to approve or deny the request to ensure that the use of the personal health information has been approved pursuant to Policy #14 (*Levels of Access*).

Policy #14 also sets 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 #35 (*Personal Health Information on Mobile Devices)* requires mobile devices containing personal health information to be encrypted as per Policy #21 (*Encryption*) as well as password-protected using strong and complex passwords that are in compliance with Policy #13 (*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 IT Team who is responsible for encrypting mobile devices and for ensuring that the mandatory standardized password-protected screen saver is enabled are also identified.

Policy #35 (*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 #35 (*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. Therefore, this section is not applicable.

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

POGO has developed and implemented a guiding policy - Policy # 29 (*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 #10 (*Confidentiality and Security of Data*) *and* Policy #18 (*Secured Faxes Containing Personal Health Information/ Confidential Information*), and in respect of secure electronic transfer of personal health information, Policy #10 (*Confidentiality and Security of Data*), and Policy #21 (*Encryption*).

Section 3.13 in the POGO *Privacy and Security Policies and Procedures Manual* (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 agent transferring records of personal health information is required to document the date, time and mode of transfer; the recipient 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 are logged for all transfer of all 44 and 45 projects in the POGO Research Database and POGONIS database, for transfers of personal health information from the POGO tertiary pediatric oncology hospital partners.

Policy # 29 (*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 # 29 (*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 Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers 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 #4 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

Policy #3 (*Retention, Return, and Destruction of Data*) and Policy #12 (*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 #3 *(Retention, Return, and Destruction of Data*). The policy 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. The policy and procedures also identifies the Privacy Officers as the agents 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 researcher who is not a third party service provider, POGO's Researcher Agreement and Policy #3 (*Retention, Return, and Destruction of Data*) identify the researcher as the designated agent responsible for securely disposing of the records of personal health information; the responsibilities of the researcher 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 researcher 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 and method of secure disposal employed; and
- Bearing the name and signature of the agent(s) who performed the secure disposal.

Policy #3 (*Retention, Return, and Destruction of Data*) sets out the time frame within which, and the Privacy Officers as the agents 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 #12 (*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 #12 (*Document Shredding*).

The policy and procedures also designates the Privacy Officers as the agents 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. POGO does not create 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, numerous paper copies of electronic documents containing personal health information used for review and analysis. Following analysis these paper copies are no longer required and therefore disposed securely (placed in a 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 #42 (*Template Agreement for All Third Party Service Provider*), and identifies the Privacy Officer as the agents responsible for ensuring that the agreement has been executed prior to the transfer of records of personal health information for secure disposal.

Policy #3 *(Retention, Return, and Destruction of Data*) and Policy #12 (*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 agent(s) 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 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 POGO's Privacy Audit Program, set out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers 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 Policy #4 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

9. Policy and Procedures Relating to Passwords

Policy #13 (*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 #13.

Policy #13 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, concealing, 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 Audit Program and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers 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 Policy #4 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

POGO has developed and implemented Policy #32 (*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.

The *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 #32 (*Security Standards and Procedures*), and POGO's *Privacy and Security Policies and Procedures Manual,* Section 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 IT Team is 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.

The *Security Standards and Procedures* and POGO's *Privacy and Security Policies and Procedures Manual,* Section 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 or amended or deleted in any way. The *Security Standards and Procedures* and POGO's *Privacy and Security Policies and Procedures Manual,* Section 3 (*POGONIS Security Controls and Performance*) also set out the procedures that must be implemented in this regard and the IT Team as the agents responsible for implementing these procedures.

The *Security Standards and Procedures* and POGO's *Privacy and Security Policies and Procedures Manual,* Section 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 will 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 #4 (*Privacy Breach and Incident Management*), or Policy #36 (*Information Security Breach Management*) of an information security breach or suspected information security breach. The relationship between these two policies and their procedures is also identified.

Further, the *Security Standards and Procedures* addresses the findings arising from the review of system control and audit logs, including the Privacy Officers who are 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.

The *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 Officers 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, the *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 Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers 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 Policy #4 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

11. Policy and Procedures for Patch Management

The *Security Standards and Procedures* outline the procedures that have been developed and implemented for patch management.

The *Security Standards and Procedures* identify 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. The *Security Standards and Procedures* further discuss 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.

In circumstances where a determination is made that the patch should not be implemented, the *Security Standards and Procedures* requires that the IT Team 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, the *Security Standards and Procedures* identify the IT Team as responsible for determining the time frame for implementation of the patch and the priority of the patch. The *Security Standards and Procedures* also set 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 *Security Standards and Procedures* also set 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.

The *Security Standards and Procedures* also require 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 *Security Standards and Procedures* also stipulate that compliance will be audited in accordance with the POGO's Privacy Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The *Security Standards and Procedures* also require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #4 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

12. Policy and Procedures Related to Change Management

POGO's Policy #37 (*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 Officers as the agents 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 #37 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 #37 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 #37 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 #37 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.

The *Change Management* policy 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.

The *Change Management* policy 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 must also stipulate that compliance will be audited in accordance with POGO's Privacy Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The *Change Management* policy also requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #4 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

The *Security Standards and Procedures* were developed and implemented and includes back-up and recovery of records of personal health information.

The *Security Standards and Procedures* 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.

The *Security Standards and Procedures* 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.

The *Security Standards and Procedures* further identify the IT Team that is 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. The *Security Standards and Procedures* requires the backed-up records of personal health information to be retained in compliance with this policy, and POGO's *Privacy and Security Policies and Procedures Manual*, Section 3 (*POGONIS Security Controls and Performance*) and identifies the IT Team that is responsible for ensuring that they are retained in a secure 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. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy Audit

Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The *Security Standards and Procedures* require agents to notify POGO at the first reasonable opportunity, in accordance with Policy #4 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

14. Policy and Procedures on the Acceptable Use of Technology

POGO's Policy #33 (*Acceptable Usage*) was developed and implemented outlining the acceptable use of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by POGO.

Policy #33 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 #33 identifies the IT Team in consultation with the Privacy Officers 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 Officers as the agents to whom this documentation must be provided; and the required content of the documentation. The criteria that must be considered by the Privacy Officers for determining whether to approve or deny the request is also identified.

Policy #33 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 Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Policy #33 (*Acceptable Usage*) also requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #4 (Privacy *Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

15. Policy and Procedures In Respect of Security Audits

POGO's Privacy Audit Program was enhanced in 2010 to include some required components 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. The security audits to be developed and implemented include: threat and risk assessments; vulnerability assessments; penetration testing; and ethical hacks. Once POGO has developed and implemented all the required types of security audits, the program will hereafter be referred to as POGO's Privacy and Security Audit Program.

With respect to each security audit that is required to be conducted and currently implemented and those security audits to be developed and implemented, 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 and will identify the IT Team and Privacy Officers as the agents 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 Officers as the agents to whom this documentation must be provided; and the required content of the documentation.

The role of the Privacy Officers who have been delegated overall authority to manage the privacy and security program is identified. The IT Team have 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 Officers who are the agents 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.

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 Officers 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 Executive Director.

POGO's Privacy and Security Audit Program further requires that a log be maintained of security audits and identifies the Privacy 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 at the first reasonable opportunity, of an information security breach or suspected information security breach in accordance with Policy #4 (*Privacy Breach and Incident Management*), or Policy #36 (*Information Security Breach Management*) of an information security breach or suspected information security breach.

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 Officers who are 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's Policy #36 (*Information Security Breach Management*) was developed and implemented to 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.

Policy #36 imposes 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 Officers as the agents who must be notified of the information security breach or suspected information security breach and provides contact information for the Privacy Officers. 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 Officers as the agents to whom this documentation must be provided; and the required content of the documentation.

Upon notification, Policy #36 requires 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 Officers who are the agents 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 Executive Director will be notified. This includes a discussion of the Privacy Officers who are the agents 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 Officers 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 Officers 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 Officers, together with 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. Policy #36 also addresses any documentation that must be completed, provided and/or executed by the Privacy Officers 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 to 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, Policy #36 sets out the Privacy Officers as the agents 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 requires 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 set out the Privacy Officers as the agents 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 further identifies the Privacy Officers as the agents 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 Officers as the agents to whom this documentation must be provided; and the required content of the documentation. The role of the Privacy Officers that have been delegated overall authority to manage the privacy and security program is also identified.

The policy also identifies the Privacy Officers as the agents 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 Officers as the agents to whom the documentation must be provided; and the required content of the documentation.

Policy #36 also addresses 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 agent(s) 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 of the investigation must be communicated, including the Executive Director.

Further, the policy requires that a log be maintained of information security breaches and identifies the Privacy 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 Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers as the agents 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.

The policy and procedures set 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 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 Officers are 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 Officers who are 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 agent(s) responsible for providing notification to the Privacy Officers, 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 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 Officers have 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 agents 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 #4 (*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.

The policy and procedures set 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 Officers, and also sets out the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with Policy #40 (*Privacy Audits*) and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers 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 POGO's *Privacy and Data Security Code*, POGO's *Privacy and Data Security Procedures,* Policy #4 (*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 (*Privacy and Security Training*).

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

POGO 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 (*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 Officers are the agents 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 Officers 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 Officers together with 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 agents in implementing the administrative, technical, and physical safeguards put in place by POGO; and

- An explanation of Policy #4 (*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.

The policy and procedures also require 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 Officers as the agents 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 Policy #40 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers 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 #4 (*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 (*Privacy and Security Training*).

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

POGO 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 P*rivacy and Security Policies and Procedures Manual,* Policy #5 (*Confidentiality and Non-Disclosure Agreement*) requires agents to execute a Confidentiality and Non-Disclosure Agreement in accordance with the 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 on an annual basis and identify the time frame

each year in which the Confidentiality Agreement is required to be executed.

The policy and procedures further identifies 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 Officers 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 stored electronically and in hard copy in POGO's secured central files and hard copy by the Privacy Team.

POGO requires agents to comply with the policy and its procedures and stipulates that the Privacy Officers enforce compliance, and the consequences of breach. 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 Policy #40 (*Privacy Audits*) and sets out the frequency with which the policy and its procedures will be audited and identifies the Privacy Officers 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 #4 (*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 #5 (*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 requires 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 #30 (*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 requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #4 (*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

A job description for the position of Privacy Officers who have 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 Officers who have been delegated day-to-day authority to manage the privacy program by the Executive Director. The job description identifies the responsibilities and obligations of the Privacy Officers 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 Manual, S*ection #7 (*Privacy Inquires, Challenges, and Complaints*)
- Receiving and responding to privacy inquiries pursuant to the POGO's *Privacy and Security Policies and Procedures Manual,* Section #7 (*Privacy Inquires, Challenges, and Complaints*);
- Receiving, documenting, tracking, investigating, and remediating privacy breaches or suspected privacy breaches pursuant to Policy #4 (*Privacy Breach and Incident Management)*; and
- Conducting privacy audits pursuant to the Policy #40 (*Privacy Audits*).

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

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

The job description sets out the reporting relationship of the Privacy Officers who have been delegated day-to-day authority to manage the security program by the Executive Director. The job description identifies the responsibilities and obligations of the Privacy Officers 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 #4 (*Privacy Breach and Incident Management*); and

- Conducting security audits pursuant to Policy #40, (*Privacy Audits*) together with the IT Team.

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

The policy and procedures require 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 Policy #40 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers who are 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 #4 (*Privacy Breach and Incident Management*) and Policy #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's *Privacy and Security Policies and Procedures Manual*, Policy #6 (*Disciplinary Action – Privacy Breach*) addresses the investigation of disciplinary matters, including the Privacy Officers who are 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 Officers who are responsible for completing, providing, and/or executing the documentation; the required content of the documentation; and the agent(s) 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 agent(s) 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 #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 Governance and Accountability Framework

A privacy governance and accountability framework, POGO's Privacy Program, which includes security, has been established by POGO for ensuring compliance with the *Act* and its regulation, and for ensuring compliance with the privacy policies, procedures, and practices implemented by POGO.

POGO's Privacy Program stipulates that the Executive Director 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 Officers are the agents who have been delegated overall authority to manage POGO's privacy program. The Privacy Officers are identified in POGO's Privacy Program, which outlines the nature of the reporting relationship to the Executive Director. These documents also set out the responsibilities and obligations of the Privacy Officers and identify the other individuals, committees, and teams that support the Privacy Officers.

POGO's Executive Director 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 Executive Director, who in turn, reports to the Board of Directors. POGO's Privacy Program sets out the frequency with which and the method and manner by which the Board of Directors is updated with respect to the Privacy Program, the Privacy Officers who are responsible for providing such updates together with the Executive Director, 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 and documented in POGO's minutes of the Board of Directors.

The update provided to the Board of Directors addresses the initiatives undertaken by the Privacy Program including privacy training and the development and implementation of privacy policies, procedures, and practices. It also includes a discussion of the privacy audits and privacy impact assessments conducted, including the results of, and recommendations arising from the privacy audits and privacy impact assessments and the status of implementation of the recommendations. The Board of Directors is also advised of any privacy 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 is accompanied by a privacy governance organizational chart.

POGO's Privacy Program also sets out the manner in which the program will be communicated to agents of POGO, the method by which it will be communicated, and the Privacy Officers as the agents responsible for this communication.

POGO's Privacy Program is a combination of POGO's *Privacy and Data Security Code*, POGO's *Privacy and Data Security Procedures*, and POGO's *Privacy and Security Policies and Procedures Manual.*

2. Security Governance and Accountability Framework

POGO's Privacy Program, which includes security, has been established, and ensures compliance with the *Act* and its regulation as well as compliance with the security policies, procedures, and practices implemented by POGO.

POGO's Privacy Program stipulates that the Executive Director is ultimately accountable for ensuring the security of personal health information and for ensuring that POGO and its agents comply with the security policies, procedures, and practices implemented.

The Privacy Officers who have been delegated overall authority to manage the security program are identified in the Privacy Program and report directly to the Executive Director. POGO's Privacy Program also sets out the responsibilities and obligations of other individuals, committees, and teams (i.e., the Data Security Committee and IT Team) that support the Privacy Officers.

The role of the Board of Directors in respect of the security program is also addressed. The Privacy Program sets out the frequency with which and the method and manner by which the Board of Directors is updated with respect to the security program, the Privacy Officers who are responsible for providing updates, 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 by the Privacy Officers in the form of a presentation, and documented in the minutes of the Board of Directors.

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

The Privacy Program is accompanied by a security governance organizational chart.

The Privacy Program, which includes security, also sets out the manner in which the program will be communicated to agents of POGO, the method by which it will be communicated, and the agent(s) responsible for this communication.

POGO's Privacy Program is a combination of POGO's *Privacy and Data Security Code*, POGO's *Privacy and Data Security Procedures*, and POGO's *Privacy and Security Policies and Procedures Manual.*

3. 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 that has a direct role in respect of the Privacy Program, and which includes security. For this committee, 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 that this committee reports to the Executive Director. Meeting minutes are utilized to review, update, create privacy and security policies and procedures, and to provide updates to the Board of Directors.

4. Corporate Risk Management Framework

POGO plans to develop and implement a comprehensive and integrated corporate risk management framework to identify, assess, mitigate, and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received, and to maintain the confidentiality of that information.

The corporate risk management framework will address 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 will also include 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 will also address 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 will also include 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 will also identify 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 will include 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 will further address 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 will also address 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 will involve 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 Executive Director. Approval and endorsement of the results of the risk management process, including the agent(s) responsible for approval and endorsement, will also be outlined.

Further, the corporate risk management framework will also ensure that a corporate risk register be maintained and that the corporate risk register be 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 will be reviewed, the agent(s) responsible for its review, and the process that must be followed in reviewing and amending it will also be identified.

The manner in which the corporate risk management framework will be integrated into the policies, procedures and practices of POGO, and into the projects undertaken by POGO and the agent(s) responsible for integration will also be addressed.

5. Corporate Risk Register

POGO will develop and maintain 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 shall include 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.

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

POGO will develop and implement a policy and associated procedures requiring a consolidated and centralized log to be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits, and the investigation of privacy breaches, privacy complaints, and security breaches. The consolidated and centralized log will include recommendations made by the Information and Privacy Commissioner of Ontario that will be addressed by POGO prior to the next review of its practices and procedures.

The policy and procedures will 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 will be 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 will be 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 #40 (*Privacy Audits*), and POGO's Privacy and Security Policies and Procedures Manual, Section 4, (*POGO's Privacy 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 Officers 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 Policy #4 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

7. Consolidated Log of Recommendations

POGO will develop and maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches, and reviews by the Information and Privacy Commissioner of Ontario.

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

8. Business Continuity and Disaster Recovery Plan

A policy and associated procedures will be developed and implemented by POGO 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, human, environmental, and technical interruptions and threats.

The business continuity and disaster recovery plan will address 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 will identify 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 will also address 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 will be developed and maintained of all agents, service providers, stakeholders, and other persons or organizations that must be notified of business interruptions and threats. The business continuity and disaster recovery plan will identify 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 will identify the agent(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 will address 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 will set 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 will include 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 will further identify 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 will further address 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 will also identify 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 will include 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 will require 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 will further identify 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 will be documented and communicated and by whom and to whom they will be communicated will also be discussed.

The business continuity and disaster recovery plan will also address the testing, maintenance, and assessment of the business continuity and disaster recovery plan. This will include identifying the frequency of testing; the agent(s) responsible for ensuring that the business continuity and disaster recovery discovery 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 discovery 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 will further address 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 will also be identified, including the method and nature of the communication.

Appendix 1: Privacy, Security, and Other Indicators

Part 1 – Privacy Indicators

Categories	Privacy Indicators	POGO
General Privacy Policies, Procedures and Practices	▪ 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.	▪ See attached: **Appendix 1a: POGO Privacy Policy Log**. ▪ Appendix 1a: "POGO Privacy & Security Policy Log" has been revised to include each date that the privacy & security policies and procedures were reviewed. This was not POGO's practice in the past, but we will begin and continue to log each time a policy is reviewed and amended.
	▪ 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 amended, a brief description of the amendments made.	▪ All changes have been or will be made as requested by the IPC as per their April 2010 Manual (see Appendix 4) or from the 2008 IPC recommendations (see Appendix 5) or past IPC health orders. ▪ This was not POGO's practice in the past, but Appendix 1a has been revised to include a column where each policy and communication amendment can be described including the date of, and reason for each amendment.
	▪ 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.	▪ 16 new privacy policies have been developed as requested by the IPC as per their April 2010 Manual or from the 2008 IPC recommendations or past IPC health orders. ▪ Policy 24: Credit Card Use – Fundraising and Events. POGO collects and processes credit card information for payment of POGO events and

Categories	Privacy Indicators	POGO
		activities. To ensure security of the card information, POGO has established processes to ensure that a limited number of individuals have access to the card information and it is secured until the information is destroyed. ▪ Policy 25: Interlink Patient Care Plan. Interlink Community Nurses are governed by POGO privacy policies. Interlink nurses ensure their working care plans are properly secured while travelling outside of the hospital. ▪ Policy 26: Small Cell. In order to protect the confidentiality of personal health information, POGO only publishes aggregated data. Furthermore, to protect against inadvertent disclosure of personal health information, generally no data is disclosed with five or less observations per cell ("small cell data"). ▪ Policy 27: Process for 44 and 45 Projects. To ensure POGO is compliant with PHIPA, 2004 and its Regulation 329/04, as well as POGO hospital data sharing agreement requirements, guidelines have been established to ensure that projects follow the appropriate process when undertaken for analysis (45) or research (44) purposes. ▪ Policy 28: Privacy Impact Assessment Process. POGO employs a number of different privacy and security risk identification tools, including privacy impact assessments (PIAs). PIAs are integral to the fulfillment of POGO's key

Categories	Privacy Indicators	POGO
		commitment to privacy and security management. PIAs ensure that privacy and security principles are taken into account during the design, implementation, and evolution of a program, initiative, process, or system. POGO conducts both internal program and external research project PIAs. ▪ Policy 29: Secure Transfer of Records of Personal Health Information Submission Guidelines. This policy is designed to ensure the secure transfer of records to and from POGO. ▪ Policy 30: Termination or Cessation of Employment or Contractual Relationship. This policy is designed to ensure the secure return of all property of POGO on or before the date of termination of employment or contractual relationship. ▪ Policy 31: Threat and Risk Assessment. This policy addresses POGO's comprehensive threat and risk assessment process for all information security assets, including personal health information. ▪ Policy 32: Security Standard and Procedures. This policy outlines the comprehensive information security program that consists of industry standard administrative, technical, and physical safeguards. ▪ Policy 33: Acceptable Usage Policy. This policy outlines procedures related to the acceptable use

Categories	Privacy Indicators	POGO
		of information technology. ▪ Policy 34: Consolidated Log of Recommendations. This policy addresses a consolidated and centralized log to be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy complaints and privacy and security breaches, and reviews by the IPC. ▪ In Appendix 1a, Policy 34's status has been corrected to indicate it has been created and implemented. ▪ Policy 35: Personal Health Information on Mobile Devices. POGO follows strict security measures to protect any personal health information stored on mobile devices by using encryption software. ▪ Policy 36: Information Security Incident Management Process. This policy outlines the procedures for information security breach management and reporting. ▪ Policy 37: Change Management. This policy governs the approval or denial of a request for a change to the operational environment at POGO and the process to be followed. ▪ Policy 38: Monitoring Anti-Virus/Spam Updates. This policy outlines the procedures undertaken by the POGO IT Team to monitor anti-virus and anti-spam updates.

Categories	Privacy Indicators	POGO
		▪ Policy 39: Monitoring Software Updates. This policy outlines the procedures for the monitoring of software updates for the operating systems (OS) and the application systems used by POGO.
	▪ 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.	▪ Updated Policy 18 (Secured Faxes), PIAs and Confidentiality Agreements were discussed at POGO Staff meetings in April, May, and June of 2008). ▪ Email to POGO Staff re: How to Auto Lock Your Computer on April 23, 2009 ▪ Email to POGO Staff re: Shredding of Personal Health Information on May 13, 2009 ▪ Updated Policy 18 (Secured Faxes) was emailed to POGO Staff and Interlink nurses on October 5, 2010. ▪ Updated Policy 21 (Encryption) was emailed to POGO Staff on October 4, 2010. ▪ Staff education/update to be scheduled for November/December 2011. ▪ Policy 25: Interlink Patient Care Plan was circulated via email to Interlink nurses on May 27, 2010. ▪ Policy 26: Small Cell was communicated to agents via the POGO Privacy Newsletter, Winter/Spring 2010, which was emailed to

Categories	Privacy Indicators	POGO
		POGO affiliates on May 20, 2010. ▪ Newly updated/drafted policies (27-42) will be communicated to POGO staff via email once they have been finalized.
	▪ 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.	▪ Updated newsletter distributed to POGO Staff in April 2008 ▪ Updated newsletter distributed to POGO Staff and select committees and individuals in June 2009 and posted on the POGO website ▪ Updated newsletter distributed to POGO Staff and select committees and individuals in November 2010 and posted on the POGO website ▪ Documents available to the public are posted on the POGO website and updated when changes and modification are made (e.g. Privacy Code was updated on April 29, 2010).
Collection	▪ The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.	▪ 4 data holdings: Pediatric Oncology Group of Ontario Networked Information System (POGONIS), POFAP (Pediatric Oncology Financial Assistance Program) Data, Interlink Community Cancer Nurses Database, and the Successful Academic, Vocational Transition Initiative (SAVTI) Database. All 4 data holdings listed contain personal health information and are all maintained by POGO. In terms of consent, the POFAP, Interlink and

Categories	Privacy Indicators	POGO
		SAVTI databases receive consent from the individual to whom the personal health information relates. The POGONIS database contains PHI that is collected from the POGO Tertiary centres without the consent of the individuals to whom the PHI relates pursuant to section 45 of the Act.
	▪ The number of statements of purpose developed for data holdings containing personal health information.	▪ Each of the 4 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.	▪ The statements of purpose for all 4 data holdings were reviewed December 2010. See Appendix 3: POGO Data Holdings for statements of purpose.
	▪ Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made.	▪ Upon request by the POGO Co-Privacy Officers, the SAVTI database was added to the list of POGO Data Holdings in December 2010. The purpose of the SAVTI database is for reporting de-identified academic or vocational outcomes to the Ministry of Education. The data collection will be used for evaluation purposes: retrospective study and longitudinal study in the future.

Categories	Privacy Indicators	POGO
Use	▪ The number of agents granted approval to access and use personal health information for purposes other than research.	▪ POGO staff: 8 in 2008, 9 in 2009, and 9 in 2010 ▪ 7 Data Managers for each year ▪ 2 Artificial Intelligence in Medicine, Inc. (AIM) staff for each year ▪ Atlas authors/collaborators: 15 in 2008 (note: no PHI used by them in 2008), 19 in 2009 and 19 in 2010. ▪ 3 requests received (1 from ICES for the Atlas project, 2 from CCO for the Atlas project and enhanced death clearance). ▪ Atlas authors/collaborators are agents of POGO, thus this is a use of PHI and not a disclosure and therefore is reflected in the privacy indicators related to use.
	▪ 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.	▪ 6 requests have been received, with 1 yet to receive data, and 1 pending approval.
	▪ 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 Information and Privacy Commissioner of Ontario.	▪ 5 requests have been granted, 1 request is pending approval, and 0 have been denied.

Categories	Privacy Indicators	POGO
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.	▪ Atlas authors/collaborators are agents of POGO, thus this is a use of PHI and not a disclosure and therefore is reflected in the privacy indicators related to use.
	▪ 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.	▪ See Use.
	▪ The number of requests received for the disclosure of personal health information for research purposes since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 7 requests received, with 1 yet to receive data, and 1 pending approval.
	▪ 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 Information and Privacy Commissioner of Ontario.	▪ 6 requests have been granted, 1 request is pending approval, and 0 have been denied.
	▪ 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.	▪ 6 Research Agreements have been executed, as each research project must sign a Research Agreement.

Categories	Privacy Indicators	POGO
	▪ 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.	▪ 59 requests received for aggregate information for other purposes. ▪ 6 requests for de-identified 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.	▪ No agreements were executed for external persons who received aggregate information, as agreements are not required for aggregate data requests. ▪ 21 confidentiality agreements + other required privacy documents (i.e. REB, PIA and Data Request form) were executed for the 7 requests for de-identified information for research purposes. ▪ All staff who use aggregate and/or de-identified data sign a confidentiality agreement annually for 45 purposes.
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.	Five Data Sharing Agreements ▪ CCO/POGO in 2008 ▪ CCO/POGO in 2010 ▪ ICES/POGO amendment in 2009 ▪ UHN/POGO in 2009 ▪ POGO/SickKids POGONIS Backfill in 2010

Categories	Privacy Indicators	POGO
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.	▪ 3 (Artificial Intelligence in Medicine, Inc., Metafore, and Iron Mountain)
Data Linkage	▪ The number and a list of data linkages approved since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 2 (CCO and ICES)
Privacy Impact Assessments	▪ 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.	See attached: Appendix 1b: Privacy Indicator.Summary of PIAs.2010 Review
	▪ 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.	See note above.
	▪ 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.	See note above.

Categories	Privacy Indicators	POGO
	▪ 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.	See note above.
	▪ 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.	See note above.
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: – 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.	See attached: Appendix 1c: Privacy Indicator. Audits Completed.2010 Review. Appendix 1c has been amended where applicable to clearly indicate how the audit recommendations protect the privacy of individuals. An annual audit will be added to review staff, researchers, and affiliates' approved access and use of personal health information and determine whether access and use continues to be required.

Categories	Privacy Indicators	POGO
	▪ 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: – 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.	See attached: Appendix 1c: Privacy Indicator. Audits Completed.2010 Review.
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.	See attached: Appendix 1d: Privacy Indicator. Privacy Breaches 2010 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	

Categories	Privacy Indicators	POGO
	– 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.	
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, – 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	

Categories	Privacy Indicators	POGO
	– 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.	

Part 2 – Security Indicators

Categories	Security Indicators	POGO
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.	▪ See General Privacy Policies, Procedures, and Practices section. ▪ Appendix 1a: "POGO Privacy & Security Policy Log" has been revised to include each date that the privacy & security policies and procedures were reviewed and a column where each policy and communication amendment can be described. This was not POGO's practice in the past but we will begin, and continue to log this information.
	▪ 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.	
	▪ 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.	
	▪ 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 procedure communicated to agents, the nature of the communication.	
	▪ 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.	

Categories	Security Indicators	POGO
Physical Security	▪ 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.	▪ An approval audit is currently completed when: ▪ new staff/researchers require access to personal health information ▪ staff/researchers request a change in their access level ▪ physical restructuring of the POGO office takes place ▪ staff/researchers end their employment/affiliation with POGO. ▪ A more detailed audit log will be developed and implemented in 2011. This log will be audited annually by the POGO Co-Privacy Officers.
Security Audit Program	▪ 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. ▪ 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.	▪ From July 2008 to December 2009, POGO with the assistance of Artificial Intelligence in Medicine, Inc. (AIM) implemented an upgrade of POGONIS to a more secure platform. ▪ The security features of the new platform are detailed in 3.13 POGONIS Security Controls and Performance, specifically sections 3 to 6 detailing the Operational and Technical Security Controls. ▪ During the period July 2008 to December 2009, as part of the implementation plan, POGO routinely tested the new platform to ensure all security system controls were implemented and functioning as indicated in the above document. Only one identified issue identified in the early stages of implementation which was rectified by

Categories	Security Indicators	POGO
		AIM with a new build completed in December 2008. ▪ In early 2010, audit logs for both the POGO network environment and the POGONIS database system started to be reviewed by the IT Team. This occurs routinely each week, as outlined in our security standards and procedures document. ▪ In September 2010, upon reviewing the POGONIS Data Modification Audit Logs, a failure was noted by the IT Team and rectified by AIM with the new build completed in January 2011. ▪ Since the threat and risk assessment completion in June 2008, POGO has implemented the following security control recommendations: 1. Disable the VPN access afterhours; (completed March 2011) 2. Implement the configuration standards of the network devices that have been developed by the IT Team; (completed March 2011) 3. Complete the implementation of all documented firewall controls developed by the IT Team; (To be completed by November 2011). 4. Complete the implementation of the documented VPN rules. See item 3.

Categories	Security Indicators	POGO
		▪ Currently, POGO does not document the security audits completed in the exact manner specified by the IPC in this document. POGO will begin documenting as required all audits that identify an issue and yield recommendations to be addressed.
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, – 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.	▪ Not applicable.

Part 3 – Human Resources Indicators

Categories	Human Resources Indicators	POGO
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.	▪ In 2008, 7 new agents. ▪ In 2009, 16 agents. ▪ In 2010, 13 new 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.	▪ In the past, ongoing formal privacy training was not mandatory for agents although agents were invited to all formal privacy training sessions. Agents were updated on changes/modifications to policies and procedures via email and staff meetings. See the General Privacy Policies, Procedures, and Practices section for a list of updated items that POGO agents were notified of via staff meetings or emails. ▪ Since December 2010 policy#5 was amended such that agents are required to participate in ongoing privacy training.
	▪ The dates and number of communications to agents by the prescribed entity in relation to privacy and security	▪ In 2008, 4 communications regarding privacy. The information recorded regarding the 2008

Categories	Human Resources Indicators	POGO
	since the prior review by the Information and Privacy Commissioner of Ontario and a brief description of each communication.	communications are as follows: (1) in March, Co-Privacy Officers updated POGO on New Fax Policy; (2) in April POGO Privacy Newsletter was distributed; (3) in April the New Fax Policy presented at POGO Staff meeting; and (4) in April the Co-Privacy Officers presented to the POGO Board. ▪ In 2009, 9 communications regarding privacy. The information recorded regarding the 2009 communications are as follows: (1) On April 23, email to POGO Staff re: How to Auto Lock Your Computer; (2)On May 13, Email to POGO Staff re: Shredding of PHI;(3) On June 25, POGO Privacy Newsletter distributed; (4)On September 1, email to POGO Interlink Nurses re: Faxing Stats to Confidential Fax; (5)On October 1, email to POGO Interlink Nurses re: Expense Forms and Patient's Initials; (6)in December, Privacy Discussion with POGO Interlink Nursing Team; (7) On October 1, discussed policy re: email at Staff meeting; (8) On June 16, discussed POGONIS/Privacy in case of fire at Staff meeting; and (9) On January 20, discussed meeting of privacy officers. ▪ In 2010, 10 communications regarding privacy. The information recorded regarding the 2010 communications are as follows: (1) On June 4, an email sent re: limiting access to folders; (2) On September 15, an email sent re: POGO staff folders; (3) On November 10, email sent re: shredding cart in POGONIS; (4) On October 19,

Categories	Human Resources Indicators	POGO
		email sent re: sharing work space; (5) On December 21, Privacy update at Staff meeting; (6) On February 16, Privacy update at Staff meeting; (7) On May 20, POGO Privacy Newsletter distributed; (8) On October 4, an email sent re: Encryption Policy; (9) On October 5, an email sent re: Updated Fax Policy; (10) On December 17, Privacy Presentation to the POGO Board. ▪ This was not POGO's practice in the past but we will begin, and continue to log the exact date and description of each communication.

Categories	Privacy Indicators	POGO
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.	▪ 115 agents have executed Confidentiality Agreements in 2009 and 128 staff/affiliates in 2010. ▪ 0 agents have not executed Confidentiality Agreements (2010) as their work/data analysis had not begun. ▪ All agents will sign an agreement at the commencement of their relationship with POGO and prior to the release of personal health information (Atlas data). ▪ Please note that Atlas authors/collaborators are considered POGO agents.
	▪ 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.	▪ 0 Atlas authors have not executed Confidentiality Agreements (2010). Note: 7 outstanding Atlas authors have now executed an agreement and prior to the release of personal health information (Atlas data).
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 their employment, contractual or other relationship with the prescribed person or prescribed entity.	▪ 23

Part 4 – Organizational Indicators

Categories	Organizational Indicators	POGO
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.	▪ Under development.
	▪ 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.	
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.	▪ Under development.
	▪ 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.	

Appendix 1a: POGO Privacy & Security Policy Log

Note: Following the 2010/2011 IPC Review, we will begin and continue to log each time a policy is reviewed, as well as describe each amendment made to both the policy and any communication materials available to the public.

Policy #	Policy Subject	Policy Section	Issued By	Effective Date	2008 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2009 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2010 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2011 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material[1]	Date & Nature of communication to agents
1	Access to Records by the Public	Privacy & Security	Data Security Committee	Jun-05		See Footnote 1		See Footnote 1	October 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
2	Physical/Office Security	Privacy & Security	Data Security Committee	Jun-05		See Footnote 1		See Footnote 1		See Footnote 1	See Footnote 2	
3	Retention, Return, and Destruction of Data	Privacy & Security	Data Security Committee	Aug-05		See Footnote 1	October 2009 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1	December 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	Amended Data Destruction form 20-Sept-11, no change in team	
4	Privacy Breach	Privacy & Security	Data Security Committee	Jul-05		See Footnote 1	October 2009 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1		See Footnote 1	See Footnote 2	
5	Confidentiality Agreement	Privacy & Security	Data Security Committee	Feb-05	April 2008 Changes were made as requested from the 2008 IPC recommendations.	Discussed at POGO Staff meetings in April, May and June of 2008		See Footnote 1	December 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
6	Disciplinary Action - Privacy Infractions	Privacy & Security	Data Security Committee	Jun-05		See Footnote 1	October 2009 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1		See Footnote 1	See Footnote 2	
7	Review of Privacy and Security Policies and Procedures	Privacy & Security	Data Security Committee	Jun-05		See Footnote 1		See Footnote 1	November 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
8	Delegation of roles and responsibilities	Privacy & Security	Data Security Committee	Jun-05	April 2008 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1		See Footnote 1		See Footnote 1	See Footnote 2	
9	Privacy and Security Training	Privacy & Security	Data Security Committee	Jun-05		See Fotnote 1		See Footnote 1	December 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	

Policy #	Policy Subject	Policy Section	Issued By	Effective Date	2008 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2009 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2010 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2011 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material[1]	Date & Nature of communication to agents
10	Confidentiality and Security of Data	Privacy & Security	Data Security Committee	Jun-05	April 2008 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1		See Footnote 1	October 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
11	Ethics Review Process for POGO	Privacy & Security	Data Security Committee	Jun-05		See Footnote 1	October 2009 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1	October 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
12	Document Shredding	Privacy & Security	Data Security Committee	Jun-05		See Footnote 1	July 2009 Changes have been made as requested from the 2008 IPC recommendations.	Emailed updated policy to POGO Staff May 2009	October 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
13	Password	Privacy & Security	Data Security Committee	Jun-05		See Footnote 1		See Footnote 1	October 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
14	Levels of Access	Privacy & Security	Data Security Committee	May-05		See Footnote 1		See Footnote 1		See Footnote 1	See Footnote 2	
16	De-Identifying Personal Health Information	Privacy & Security	Data Security Committee	Jan-07		See Footnote 1	July & October 2009 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1	October 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
17	Telephone Messages Containing Personal Health Information	Privacy & Security	Data Security Committee	Aug-06		See Footnote 1		See Footnote 1	October 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
18	Secured Faxes (Containing Personal Health Information/Confidential Information)	Privacy & Security	Data Security Committee	Aug-06	April 2008 Changes have been made as requested from the 2008 IPC recommendations.	Discussed at POGO Staff meetings in April, May and June of 2008	October 2009 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1	October 2010 Changes have been made as requested by the IPC April 2010 Manual	Emailed updated policy to POGO Staff and Interlink nurses on October 5, 2010	See Footnote 2	
19	E-mail	Privacy & Security	Data Security Committee	Mar-07		See Footnote 1	October 2009 Changes have been made as requested from the 2008 IPC recommendations.	See Footnote 1		See Footnote 1	See Footnote 2	
20	Spam E-mail	Privacy & Security	Data Security Committee	Mar-07		See Footnote 1		See Footnote 1		See Footnote 1	See Footnote 2	
21	Encryption	Privacy & Security	Data Security Committee	May-08		See Footnote 1		See Footnote 1	September 2010 Changes have been made as requested by the IPC April 2010 Manual	Emailed updated policy to POGO staff on October 4, 2010	See Footnote 2	
22	Presentation Release Form	Privacy & Security	Data Security Committee	May-08		See Footnote 1		See Footnote 1		See Footnote 1	See Footnote 2	

Policy #	Policy Subject	Policy Section	Issued By	Effective Date	2008 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2009 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2010 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2011 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material[1]	Date & Nature of communication to agents
23	Exit Interview	Privacy & Security	POGO Administration	Jun-07		See Footnote 1		See Footnote 1	December 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
25	Interlink Patient Care Plan	Privacy & Security	POGO Privacy Program	May-10					Effective May 2010	The policy was circulated via email to Interlink Nurses on May 27, 2010	See Footnote 2	
26	Small Cell	Privacy & Security	POGO Privacy Program	Jun-10					Effective June 2010 POGO Privacy Newsletter, winter/spring 2010 updated to include information re: small cell data	POGO Privacy Newsletter, Winter/Spring 2010 was emailed to POGO affiliates on May 20, 2010	See Footnote 2	
27	Process for 44 and 45 Projects	Privacy & Security	Data Security Committee	Sep-10					October 2010 Changes have been made as requested by the IPC April 2010 Manual	See Footnote 1	See Footnote 2	
28	Privacy Impact Assessment Process	Privacy & Security	Data Security Committee	Oct-10						See Footnote 1	March 2011 - Present The Policy has been reviewed as per the April 2010 Manual and the policy will be amended to reflect the PIA Guidelines for the Ontario PHI Protection Act.	
29	Secure Transfer of Records of Personal Health Information Submission Guidelines	Privacy & Security	Data Security Committee	Dec. 2010					New policy created to formalized the secure transfer of PHI which was orginally included in Policy #10 as requested by the IPC April 2010 Manual	Communicated with staff and researchers at the time of secure transfer	See Footnote 2	
30	Termination or Cessation of Employment or Contractual Relationship	Privacy & Security	POGO Administration	Dec-10					New policy created to distinguish between termination and exit interview which were combined in Policy #23 as requested by the IPC April 2010 Manual	Formally and informally with program managers at time of termination of staff member	See Footnote 2	
31	Threat and Risk Assessment	Privacy & Security	POGO Administration	Dec. 2010					New policy to formalize practice since 2008 to meet IPC April 2010 Manual	See Footnote 1	See Footnote 2	
32	Security Standards & Procedures	Privacy & Security	POGO Administration	Dec. 2010					New policy to formalize POGO Security Standards and Procedures from 1997 as requested by IPC April 2010 Manual	See Footnote 1	See Footnote 2	

Policy #	Policy Subject	Policy Section	Issued By	Effective Date	2008 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2009 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2010 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material	Date & Nature of communication to agents	2011 Date Reviewed/Reason & Description of Amendment to Policy & Communication Material[1]	Date & Nature of communication to agents
33	Acceptable Usage Policy	Privacy & Security	POGO Administration	Sep-07		See Footnote 1		See Footnote 1	Modified Dec 2010 to include IPC requirements April 2010 Manual	Originally included in orientation manuals for new staff, training sessions	See Footnote 2	
34	Consolidated Log of Recommendations	Privacy & Security	POGO Administration	Dec. 2010					Policy has been drafted to satisfy IPC requirements April 2010 Manual	See Footnote 1	See Footnote 2	
35	PHI on Mobile Devices	Privacy & Security	POGO Administration	Sept. 2004		See Footnote 1		See Footnote 1	Modified Dec 2010 to include IPC requirements April 2010 Manual	See Footnote 1	See Footnote 2	
36	Information Security Incident Management Process	Privacy & Security	POGO Administration	Dec. 2010					Moified Dec 2010 to include IPC requirements April 2010 Manual	See Footnote 1	See Footnote 2	
37	Change Management	Privacy & Security	POGO Administration	Dec-10					New policy to formalize POGO Security Standards and Procedures from 1997 as requested by IPC April 2010 Manual	See Footnote 1	See Footnote 2	
38	Monitoring Anti-Virus/Spam Updates	Privacy & Security	POGO Administration	Dec-10					New policy to formalize POGO Security Standards and Procedures from 1997 as requested by IPC April 2010 Manual	See Footnote 1	See Footnote 2	
39	Monitoring Software Updates	Privacy & Security	POGO Administration	Dec-10					New policy to formalize POGO Security Standards and Procedures from 1997 as requested by IPC April 2010 Manual	See Footnote 1	See Footnote 2	
41	Execution of Data Sharing Agreements	Privacy & Security	POGO Administration	Dec. 2010					New policy to satisfy IPC requirements April 2010 Manual	See Footnote 1	See Footnote 2	
42	Template Agreement for All Third Party Service Providers	Privacy & Security	POGO Administration	Dec-10					New policy to satisfy IPC requirements April 2010 Manual	See Footnote 1	Added IPC requirements 22-Sept-11	
	Footnotes:											
1	All policies and any amendments are communicated to agents through privacy orientation, ongoing training or staff meetings. The dates of communication to agents are documented in POGO's privacy training log and staff meeting minutes.											
2	Review of all policies occurs in Sept./Oct. and amendments will be made to policies and communicated to staff by June of following year (as per Policy # 7)											

Appendix 1b: Privacy Indicator Summary of PIAs 2010 Review
List of Privacy Impact Assessments Completed Since 2008
44 Projects

Project Number	Data Holding, Information System, Technology or Program	Date Completed PIA	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner	Comments
Project 21	POGONIS	8-May	See Appendix 1c for recommendations arising from the researcher project's audit	See Appendix 1c	See Appendix 1c for recommendations addressed relating to the researcher project's audit	
Project 71	POGONIS	March-11	PIAs were completed with Privacy Officers and research team - no rec's	N/A	N/A	
Project 72	POGONIS	December-09	PIAs were completed with Privacy Officers and research team - no rec's	N/A	N/A	
Project 73	POGONIS	January-10	PIAs were completed with Privacy Officers and research team - no rec's	N/A	N/A	
project 75	POGONIS	March-11	PIAs were completed with Privacy Officers and research team - no rec's	N/A	N/A	
Proejct 79	POGONIS	March-11	PIAs were completed with Privacy Officers and research team - no rec's	N/A	N/A	
Project 82	POGONIS	June-10	PIAs were completed with Privacy Officers and research team - no rec's	N/A	N/A	
Project 91	POGONIS	June-11	PIAs were completed with Privacy Officers and research team - no rec's	N/A	N/A	
Project 92	POGONIS	February-11	PIAs were completed with Privacy Officers and research team - no rec's	N/A	N/A	

N/A = As this is a collaborative process whereby POGO's Privacy Coordinators work directly with POGO's agents to ensure accurate and complete Privacy Impact Assessments, the details of amendments that may have been made during the course of this process are not available.

Appendix 1b: Privacy Indicator Summary of PIAs 2010 Review
List of Privacy Impact Assessments Completed Since 2008
45 Purposes

Name of Staff Member	Data Holding, Information System, Technology or Program	Date Completed PIA	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
A, M	POGONIS, Research	January, 2007 and reviewed/ accepted January 2011	N/A	N/A	N/A
B, H	Atlas Project	June, 2010	De-identified record level data is currently transferred outside of the POGONIS room via an unsecured USB key for the purposes of manipulation and analysis. USB key is locked back in room after use. **Recommendation:** De-identified record level data will be transferred via IronKey.	March, 2011	De-identified record level data transferred outside of the POGONIS room will be transferred via IronKey.
B, C	Clinical Programs (Satellite, AfterCare)	April, 2010	N/A	N/A	N/A
B, N	Research, Clinical Programs (Satellite, AfterCare), POGONIS, Atlas	June, 2010	De-identified record level data is currently transferred outside of the POGONIS room via an unsecured USB key for the purposes of manipulation and analysis. USB key is locked back in room after use. **Recommendation:** De-identified record level data will be transferred via IronKey.	March, 2011	De-identified record level data transferred outside of the POGONIS room will be transferred via IronKey.

Name of Staff Member	Data Holding, Information System, Technology or Program	Date Completed PIA	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
C, H	Administration: Medical Director, Corporate	April, 2008	N/A	N/A	N/A
D, B	POGONIS, Privacy	December, 2010	N/A	N/A	N/A
D, B	SAVTI	June, 2010	N/A	N/A	N/A
G, S	IT, POGONIS	January, 2011	N/A	N/A	N/A
G, M	Research, Clinical Programs (Satellite, AfterCare), POGONIS, Atlas	February, 2007 and reviewed /accepted January 2011	N/A	N/A	N/A
H, V	IT, POGONIS	June, 2010	N/A	N/A	N/A
M, E	Backfill into POGONIS at SickKids	August, 2011	N/A	N/A	N/A
P, H	IT, POGONIS	January, 2011	N/A	N/A	N/A
P, J	POGONIS, Research	July, 2010	N/A	N/A	N/A
P, S	POFAP	February, 2010	N/A	N/A	N/A
S. L, L	Interlink	June, 2010	N/A	N/A	N/A
W, B	SAVTI	May, 2010	N/A	N/A	N/A

N/A = As this is a collaborative process whereby POGO's Privacy Coordinators work directly with POGO's agents to ensure accurate and complete Privacy Impact Assessments, the details of amendments that may have been made during the course of this process are not available.

Appendix 1b: Privacy Indicator Summary of PIAs 2010 Review

List of Privacy Impact Assessment Undertaken But Not Completed Since 2008

Name of Staff Member	Proposed Date of Completion

Appendix 1b: Privacy Indicator Summary of PIAs 2010 Review

List of Privacy Impact Assessments Not Undertaken Since 2008 But Which Will Be Completed

45's

Name of Staff Member	Proposed Date of Completion
R, P	2011
S, K	2011
M, D	2011

List of Privacy Impact Assessments Not Undertaken Since 2008
But Which Will Be Completed
44's

Name of Staff Member	Proposed Date of Completion
S, F	2011
L, N	2011

Appendix 1b: Privacy Indicator Summary of PIAs 2010 Review

Determinations Made Since 2008 That A Privacy Impact Assessment is Not Required

Name of Staff Member	Data Holding, Information System, Technology or Program	Reasons for Determination
A, R	Fundraising	Data holdings, information systems, technologies or programs do not involve the collecting of personal health information.
A, J	Fundraising	Same as above.
B, P	Student	Same as above.
B, M	Administration	Same as above.
B, E	Finance	Same as above.
B, S	Administration	Same as above.
B, C	Human Resources	Same as above.
B, L	Fundraising	Same as above.
B, L	Administration	Same as above.
B, H	Fundraising	Same as above.
C, M	Volunteer	Same as above.
C, H	Research	Same as above.
C, C	Special Events & Community Outreach	Same as above.
C, A	Administration	Same as above.
C, M	Volunteer	Same as above.
d l R, G	Volunteer	Same as above.
D, J	Communications	Same as above.
D, E	Administration	Same as above.
E, M	Administration	Same as above.
F, P	Administration	Same as above.
F, J	Educational Events	Same as above.
F, M	Student	Same as above.
G, M	Administration	Same as above.
G, L	Finance	Same as above.
G, B	Finance	Same as above.
G, S	Volunteer	Same as above.
G, C	Administration	Same as above.
G, E	Administration	Same as above.
J, C	Volunteer	Same as above.
J, C	Conference & Educational Events	Same as above.
K, S	Student	Same as above.

Name of Staff Member	Data Holding, Information System, Technology or Program	Reasons for Determination
K, I	Finance	Same as above.
K, G	Reception	Same as above.
L, D	Administration	Same as above.
L, J	Student	Same as above.
L,	Research	Same as above.
L, C	Research	Same as above.
M, J	Fundraising	Same as above.
N, B	Volunteer	Same as above.
R, M	Research, Human Resources, Privacy, Corporate	Same as above.
S, T	Volunteer	Same as above.
S, K	Volunteer	Same as above.
S, A	Student	Same as above.
S, M	Administration	Same as above.
S, M	Volunteer	Same as above.
S, T	Research Fellowship	Same as above.
S, S	Fundraising	Same as above.
T, B	Reception	Same as above.
T, C	Volunteer	Same as above.
T, F	Volunteer	Same as above.
U, N	Student	Same as above.
V, C	Fundraising	Same as above.
W, M	Fundraising	Same as above.
Y, V	Fundraising	Same as above.
Z, K	Fundraising	Same as above.

Appendix 1b: Privacy Indicator Summary of PIAs 2010 Review

List of Privacy Impact Assessments Reviewed Since 2008 and a Description of Any Amendments Made

Name of Staff Member	Last Review	Description of Amendments Made
All PIAs (24) completed since 2008 have been reviewed	2010 & Winter 2011	As this is a collaborative process whereby POGO's Privacy Coordinators work directly with POGO's agents to ensure accurate and complete Privacy Impact Assessments, the details of amendments that may have been made during the course of this process are not available.

Total: 24

Appendix 1b: Privacy Indicator.Summary of PIAs.2010 Review

2008

Therefore Unable to Complete

Name of Staff Member	Data Holding, Information System, Technology or Program	Completed PIA Prior to 2008	Date Left POGO
T, L	Research	Yes (2007)	April, 2008

Appendix 1c: Privacy Indicator Audits Completed 2010 Review

Audits of Staff, Researchers, and Affiliates Since 2008 Granted Approval to Access or Use Personal Health Information

Staff, Researcher, or Affiliate	Date of Audit	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
A. T., as relates to *Costs Incurred by Families of Children Newly Diagnosed with Cancer*	May, 2008	Conduct privacy training with research team	May, 2007	Conducted privacy training with research team
		Move and secure family survey files	January, 2008	Family survey files were moved and secured
		Conduct data entry in POGO's secured data centre	July, 2007	Data (de-identified) entered in POGO's secured data centre
		Supply POGO with annual research ethics board approvals	April, 2008	Researcher agreed to supply POGO with annual research ethics board approvals
		Supply POGO with an up-to-date consent form	April, 2008	Researcher supplied POGO with an up-to-date consent form
		Modify all transcripts to be identified by study code only	April, 2008	Researcher modified all transcripts to be identified by study code only, thus, deleting patient name, home city, and physician
		Paper copy of the master list should be shredded, electronically encrypted and password-protected. A second back-up copy of this file should be encrypted encrypted and password-protected, and securely stored.	April, 2008	Paper copy of the master list were shredded and electronic copy was encrypted and password-protected. A second back-up copy of this file is encrypted and password-protected, and secured.
		Researcher should develop a policy to follow in the event of receiving requests from individuals regarding access to, and amendment of, their own personal health information	Summer 2008	Researcher developed a policy to follow in the event of receiving requests from individuals regarding access to, and amendment of, their own personal health information
S. L., as relates to *Childhood Cancer Survivor Study Expansion*	April, 2008	Return data disk to POGO for destruction	April, 2008	Data disk was returned to POGO and destroyed

Staff, Researcher, or Affiliate	Date of Audit	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
		Retain consents for 5 years after the end of the study	April, 2008	Consents will be retained for 5 years after study completion
		Set up automatic shutdown procedures for computer terminals when in use	April, 2008	Automatic shutdown procedures were put in place for computer terminals in use (timed lock-out)
		Eliminate confidential information from surgery reporting photocopies	April, 2008	All confidential information was blacked out on surgery reporting photocopies
		Determine whether Project Coordinator can have sole user access to the hospital computer she uses and/or whether encryption is possible	April, 2008	Given the database is on the hospital network, the researcher had sole user access
		Create a policy and procedure in the event of receiving requests from individuals regarding access to, and amendment of, their own personal health information	April, 2008	Coordinator created a policy and procedure in the event of receiving requests from individuals regarding access to, and amendment of, their own personal health information
		Notify POGO when a requestor has successfully demonstrated an inaccuracy	April, 2008	Coordinator agreed to notify POGO when a requestor has successfully demonstrated an inaccuracy
		Notify POGO when a complaint is received from a study participant regarding the use of their personal health information	April, 2008	Coordinator agreed to notify the POGO Co-Privacy Officers when a complaint is received from a study participant regarding the use of their personal health information
		Provide new privacy impact assessment, listing the administrative support staff member	April, 2008	Coordinator provided new privacy impact assessment, listed the administrative support staff member
		Provide updated research ethics board approval to extend the project for one year ending July, 2008	April, 2008	Coordinator provided updated research ethics board approval to extend the project for one year ending July, 2008
		Forward the signed agreement with SickKids to the POGO office	April, 2008	Coordinator forwarded the signed agreement with SickKids to the POGO office

Staff, Researcher, or Affiliate	Date of Audit	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
Total: 2				

Appendix 1c: Privacy Indicator Audits Completed 2010 Review
Other Privacy Audits Since 2008

Nature and Type of Audit Conducted	Audit Completion Date	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
Program Area Reviews:				
AfterCare	July, 2009	Review the Passport to Health: explore new customized format related to privacy and security	Ongoing	Reviewing Passport to Health and exploring new customized format related to privacy and security.
		Discuss possible electronic transfer of Passport to Health	Ongoing	Discussing possible electronic transfer
	January, 2010	Make a site visit to the Dana-Farber Cancer Institute	January, 2010	Site visit made to Dana-Farber Cancer Institute
Fundraising	Summer, 2010	Review credit card process for major fundraising events	August, 2010	Reviewed credit card process for major fundraising events and developed new credit card policy in order to maintain the confidentiality of donor identity
Interlink	April, 2008	Develop guidelines for Interlink	May, 2009	Guidelines for Interlink developed
		Hire new Interlink nurse	Spring, 2008	New Interlink nurse hired (D. D.)
		Sign Interlink agreement with Orillia Soldiers' Memorial Hospital	Under discussion	Under discussion
		Sign Interlink agreement with The Hospital for Sick Children (SickKids)	May, 2007	Agreement signed with SickKids
	Spring 2010	Put in place a policy for the transmission of personal health information via email	Summer, 2010	Policy put in place for the transmission of personal health information via email to protect against disclosure of PHI via email.
		Design a new fax form with added disclaimer	October, 2010	New fax form with added disclaimer designed and put into use to protect against disclosure of PHI
		Write a new patient care plan policy	June, 2010	New patient care plan policy written to protect against disclosure of PHI
POFAP	April, 2008	Changes to be made regarding the receiving of POFAP registration forms to the secured fax machine	May, 2008	All POFAP registration forms received at the secured fax machine to protect against disclosure of PHI

Nature and Type of Audit Conducted	Audit Completion Date	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
POGONIS	2010	Build a new platform (POGONIS 2.0)	January, 2010	New platform built and put into place
		Institute new controls (security and information)	January, 2010	New security and information controls put in place based on new platform to enhance firewall, two levels of authentification and authorization and comprehensive automated audit log - all to protect the privacy of individuals.
		Compose a new data dictionary	March, 2010	New data dictionary put in place and distributed to appropriate individuals
		Institute new policies	March, 2010	New policies in place to reflecting the new platform and updated security controls.
Satellite Program	Fall, 2010	Allow Clinical Research Associates (CRAs) access to shuttle sheet	Fall, 2010	CRAs allowed access to shuttle sheets
		Send letters to the Privacy Officers at the POGO centres for their approval	March, 2010 and November, 2010	Letters sent to the Privacy Officers at the POGO centres for their approval
		CRAs to sign agreements with eCHN and hospitals	Hospital monitored	CRAs signed agreements
SAVTI	Spring, 2010	Conceptualize a new database for client registration	Spring 2010	A new database for client registration conceptualized
		Investigate SSL technology as a possible mode of secure transfer	Spring 2010	SSL technology investigated as a possible mode of secure transfer to ensure high level of protection and security of PHI
		Send a letter to the IPC seeking the addition of SAVTI as a data holding	November, 2010	Letter sent to the IPC seeking the addition of SAVTI as a data holding; verbal approval received November 29, 2010
External Privacy Compliance Reviews:				
Atlas Project	December, 2009	Data transfer and linkage at ICES as per the data sharing agreement	Ongoing	Conducting data transfer and linkage at ICES as per the data sharing agreement to ensure secure transmission of PHI
		Develop Atlas author confidentiality agreement	February, 2010 and ongoing	Atlas author confidentiality agreement developed to ensure confidentiality of PHI

Nature and Type of Audit Conducted	Audit Completion Date	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
		Collect signed Atlas author confidentiality agreements	Pending disclosure of personal health information	Atlas author confidentiality agreement signed prior to receiving personal health information to ensure confidentiality of PHI
		Review secure transfer of data with Research Coordinator as per privacy policies to stakeholders	Ongoing	Reviewing secure transfer of data with Research Coordinator as per privacy policies to stakeholders
		Review secure transfer and destruction of CCO data linkage for mortality data	February, 2009	Reviewed secure transfer and destruction of CCO data linkage for mortality data
Assessing the Fertility Status of Male Hodgkin's Lymphoma Survivors and Canadian Sperm Banking Practices **(Researcher: A. L. C.)**	June, 2009 and December, 2010	Conduct POGONIS and privacy training with the project team	January, 2010	POGONIS and privacy training conducted with the project team
		Sign confidentiality agreements with all team members	June to August, 2009	Confidentiality agreements signed by all team members
		Sign Researcher Agreement	August, 2009	Researcher Agreement signed
		Obtain research ethics board letter of renewal	Dated May, 2009	Research ethics board letter of renewal obtained
		Review use of secure IronKey for transmission of data between POGO and SickKids	January, 2010	Reviewed use of secure iron key for transmission of data between POGO and SickKids to ensure security of PHI
		Receive Project-Specific Privacy Impact Assessment Form from researcher	March, 2011	Privacy impact assessment will be completed by researcher prior to the delivery of personal health information

Nature and Type of Audit Conducted	Audit Completion Date	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
		Provide unidentified aggregate data	February, 2010	Unidentified aggregate data provided
Part One of Project: Survey	June, 2009	Complete part one of project and store surveys securely	April, 2010	Completed and surveys stored securely
Part Two of Project: Study of Participants	June, 2009 and December, 2010	Complete part two of project (recruiting participants)	Ongoing	Participants are being recruited
Pediatric Cancer Outcomes Initiative (PCOI) POGONIS Backfill Project	January, 2010 and December, 2010	Conduct POGONIS and privacy training with the project team	January to December, 2010 (as team expanded)	POGONIS and privacy training conducted with the project team
		Sign confidentiality agreements with the team	January to December, 2010 (as team expanded)	Confidentiality agreements signed with the team
		Ensure encryption of the project laptop by SickKids	June, 2010	Project laptop encrypted by SickKids to ensure security of PHI
		Execute the breach procedure with the SickKids Privacy Officer and the project team re: the SickKids breach to POGO	September, 2010	Breach procedure executed with the SickKids Privacy Officer and the project team re: the SickKids breach to POGO
		Retrain project staff on email and encryption policies following the incident and breach	August to October, 2010	Project staff retrained on email and encryption policies following the incident and breach
		Change the email address of the Project Coordinator in the wake of the incident and breach	September, 2010	The email address of the Project Coordinator was changed in the wake of the incident and breach
Topic Reviews:				
Atlas Author Agreements	February, 2010	Develop Atlas-specific confidentiality agreements for Atlas authors	February, 2010	Atlas-specific confidentiality agreement developed for Atlas authors

Nature and Type of Audit Conducted	Audit Completion Date	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
Confidentiality Agreement	December, 2010	Make additions to the confidentiality agreement as per IPC recommendations of 2008	December, 2010	Additions made to the agreement as per IPC recommendations of 2008
Data Destruction Documentation	June, 2010	Develop a Certificate of Destruction	June, 2010	Certificate of Destruction developed to ensure the proper destruction of PHI
Data Linkage Procedures	April, 2008	Review and update data linkage procedures	April, 2008	Data linkage procedures reviewed and updated in policy #10 (*Confidentiality and Security of Data Policy*)
		Complete a data linkage sharing agreement with ICES	August, 2007	Data linkage sharing agreement signed with ICES
		Complete data sharing agreement with Cancer Care Ontario	August, 2008	Data sharing agreement signed with Cancer Care Ontario
De-Identifying Personal Health Information	October, 2009	Revise policy to include procedures regarding 45 and 44 purposes	October, 2009	Policy revised to include procedures regarding 45 and 44 purposes
Ethics Review	October, 2009	Revise policy with current links to the Tri-Research Councils	October, 2009	Policy with current links to the Tri-Research Councils revised
Email	October, 2009	Revise policy to include IPC health order 004	October, 2009	Policy revised to include IPC health order 004
Encryption	January, 2010	Update the encryption policy based on the 2008 IPC recommendation and on IPC health order 007	September, 2010	The encryption policy was updated based on the 2008 IPC recommendation and on IPC Health Order 007 to ensure security of PHI
Faxing Personal Health Information	October, 2009	Revise policy to include new procedure regarding the new dedicated fax machine located in the secured data room	October, 2009	Policy revised to include new procedure regarding the new dedicated fax machine located in the secured data room to ensure security of PHI
Privacy and Security Policies in the POGO Privacy Binder	December, 2010	Update all policies in the POGO Privacy Binder based on the 2008 IPC recommendations, IPC health orders, IPC fact sheets, and the IPC Manual (2010)	December, 2010	Updated all policies in the POGO Privacy Binder based on the 2008 IPC recommendations, IPC health orders, IPC fact sheets, and the IPC Manual (2010)

Nature and Type of Audit Conducted	Audit Completion Date	Description of Recommendation	Date Addressed or Proposed Date	Manner Each Recommendation Addressed or Proposed Manner
Short Privacy Impact Assessment Form	April, 2008	Review the applicability of the use of the short form of the privacy impact assessment for aggregate data requests	April, 2008	The applicability of the use of the short form of the privacy impact assessment was reviewed and determined that it was no longer needed
***Small Cell Policy* and procedures**	January-June, 2010	Develop policies and procedures for the distribution of small cell data for the Atlas	June, 2010	Policies and procedures developed for the distribution of small cell data for the Atlas to ensure security of PHI

Total: 23

Appendix 1d: Privacy Indicator.Privacy Breaches.2010 Review
Notification of Privacy Breaches or Suspected Privacy Breaches Since 2008

Internal (X Hospital) Privacy Breach	
Date Notification Received	July 16, 2010 at X hospital
Extent of Breach	On July 15, 2010, an email with personal health information relating to a project was inadvertently sent by a Data Abstractor at X hospital to a pharmacist at X hospital, who shares the same first and last names as the project's Research Coordinator (who is an X hospital employee doing contract work for POGO on the POGONIS Backfill Project)
Internal or External	Internal (X hospital)
Nature and Extent of Personal Health Information at Issue	8 full patient names, IDs, and disease stage codes
Date Senior Management Notified	At X hospital: July 16, 2010 At POGO: July 20, 2010
Containment Measures Implemented	The project's Research Coordinator sent an email to the Pharmacist (incorrect recipient): indicating the error in receipt of the email and its contents; providing a brief background of the research ethics board approved project; requesting deletion of the email; requesting that the Project Coordinator be informed if any subsequent emails are received in error; and indicating that the POGO Co-Privacy Officers were notified and that a record of the breach was documented at POGO.
Date(s) Containment Implemented	July 21, 2010
Date(s) HICs or Other Organizations Notified	POGO was notified on July 20, 2010; X hospital was notified July 16, 2010
Date Investigation Commenced	July 20, 2010
Date Investigation Completed	July 21, 2010
Recommendation(s)	Upon identification of a breach, no matter how small or contained, it must be reported to one of POGO's Co-Privacy Officers immediately. The Project Coordinator will contact X hospital's IT Department to see if her email can be displayed with her full name. All data abstractors should be very careful when sending emails to the Project Coordinator, ensuring they have selected the correct email address. For emails within X hospital, no patient identifiers should be part of the body of the email, but rather should be contained in a password-protected attachment. For emails sent outside of X hospital, no patient identifiers should be part of the body of the email, but rather the information should be contained in a password-protected, encrypted attachment. Whenever in doubt, guidance should be sought from the POGO Co-Privacy Officers.
Date(s) Recommendation(s) Addressed	July 21, 2010

Manner Recommendation(s) Addressed or Proposed Manner	POGO changed the Research Coordinator's email address display name. The project's investigators were notified immediately. The Research Coordinator spoke with the Data Abstractors to review the gravity of the situation and the importance of POGO's privacy status and requirements to secure personal health information. Data abstractors were reminded to ensure they were using the correct email address and not to send personal health information outside of X hospital unless it is encrypted and password-protected in an attachment.

External Incident	
Date Notification Received	July 27, 2011
Extent of Breach	On July 26, 2011, X physican, sent via email to POGO's Medical Director, a file containing relapse data for Y hospital patients. The file contained personal health information, and was not encrypted or password protected. POGO's Medcial Director was the sole recipient of this data.
Internal or External	External (originating at Y hospital)
Nature and Extent of Personal Health Information at Issue	Personal health information for relapsed patients at Y hospital
Date Senior Management Notified	July 27, 2011
Containment Measures Implemented	Upon opening the e-mail attachment (July 27, 2011), POGO's Medical Director immediately notified one of POGO's Privacy Officers that a breach had occurred. X physican was immediately contacted by POGO's Privacy Officer to ensure the data was securely deleted from their email system. X physician was asked to delete the email and its attachment from the 'Sent' box and then to delete these same items from their 'Deleted' box. X physician then confirmed via email that steps had been taken to secure the data. Likewise, POGO's Medical Director immediately deleted from his 'Inbox' the email and its attachment received from X physican, and then deleted these same items from their 'Deleted' Box. The POGO IT Team permanently deleted the msesage from the POGO email server.
Date(s) Containment Implemented	July 27, 2011
Date(s) HICs or Other Organizations Notified	
Date Investigation Commenced	July 27, 2011
Date Investigation Completed	July 27, 2011
Recommendation(s)	When sending sensitive data via email, data must either contain only POGO ID's and no personal health information, or it must be encrypted and sent under password protection, with a separate email containing the password.

Date(s) Recommendation(s) Addressed	July 27, 2011
Manner Recommendation(s) Addressed or Proposed Manner	X physican was asked to contact POGO’s IT Department in the future for information/assistance on how to send sensitive information securely.

Total: 2

POGO
PEDIATRIC ONCOLOGY GROUP OF ONTARIO

COLLABORATING FOR KIDS WITH CANCER SINCE 1983

September 20, 2011

Judith Goldstein
Legal Counsel
Information and Privacy Commissioner, Ontario
2 Bloor Street East, 14th Floor
Toronto, Ontario, M4W 1A8

Dear Judith,

Enclosed please find a signed affidavit to accompany the Pediatric Oncology Group of Ontario's recent submission of its report in compliance with the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities, issued by your office on April 19, 2010.

Thank you for your continued support in this regard.

Best regards,

Bruna DiMonte, RN, BScN
Senior Database Administrator
& Co-Privacy Officer

Madeline Riehl, MHSc
Senior Associate Research and
Planning & Co-Privacy Officer

480 University Avenue
Suite 1014
Toronto, Ontario
Canada M5G 1V2
tel. 416-592-1232
toll-free. 1-855-FOR POGO
(1-855-367-7646)
fax 416-592-1285
www.pogo.ca

POGO
PEDIATRIC ONCOLOGY GROUP OF ONTARIO

Appendix 2: Affidavit of Executive Director

I, Dr. Corin Greenberg, of Toronto, in the Province of Ontario, MAKE OATH AND SAY:

1. I am the Executive Director of the Pediatric Oncology Group of Ontario (POGO).

2. The Pediatric Oncology Group of Ontario's Executive Director has formally delegated the supervision and management of day-to-day operations of the privacy portfolio to Bruna DiMonte (RN, BScN): Senior Database Administrator & Co-Privacy Officer, and to Madeline Riehl (MHSc): Senior Associate Research and Planning & Co-Privacy Officer, and has also formally delegated the supervision and management of day-to-day operations of the IT security portfolio to Husein Patel (BSc): IS Manager.

3. The Pediatric Oncology Group of Ontario has in place privacy and security policies, procedures, protocols, practices, standards, tools, guidelines and other instruments ("Privacy and Security Policies") to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of that information.

4. The Pediatric Oncology Group of Ontario has submitted a written report (the "Report") to the Information and Privacy Commissioner of Ontario in compliance with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, as issued by the Information and Privacy Commissioner of Ontario on April 19, 2010.

5. I have made due inquiries of Bruna DiMonte (RN, BScN): Senior Database Administrator & Co-Privacy Officer; of Madeline Riehl (MHSc): Senior Associate Research and Planning & Co-Privacy Officer; and of Husein Patel (BSc): IS Manager regarding the contents of the Privacy and Security Policies implemented by the Pediatric Oncology Group of Ontario, as relates to the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* and the Report.

6. Based on my knowledge, having exercised reasonable diligence, the Report describes the Privacy and Security Policies implemented by the Pediatric Oncology Group of Ontario, in an accurate and complete manner as of the date on which the Report is submitted.

7. Based on my knowledge, having exercised reasonable diligence, the Pediatric Oncology Group of Ontario has taken the steps set out in the Report that are reasonable in the circumstances to: (i) ensure the Privacy and Security Policies implemented comply with the Manual as set out in the Report; (ii) ensure compliance with the Privacy and Security Policies implemented; and (iii) protect personal health information against theft, loss, unauthorized use, disclosure, unauthorized copying, modification, or disposal.

theft, loss, unauthorized use, disclosure, unauthorized copying, modification, or disposal.

SWORN (OR AFFIRMED) BEFORE ME)

at the City/Town/Etc. of Toronto, in the)

County/Regional Municipality/Etc. of)

York, in the Province of Ontario,)

on September 15, 2011.)

Signature of Dr. Corin Greenberg

Appendix 3: POGO Data Holdings

1) POGO Networked Information System (POGONIS)

The purpose and value of the POGO Networked Information System (POGONIS) is in its ability to estimate the incidence of childhood cancer in the province in terms of determining population projections, service surveillance, outcome measures, survival information, program evaluation potential, and in assembling cohorts for investigation in multiple research projects.

2) POFAP (Pediatric Oncology Financial Assistance Program) Data

This database contains registration information on families who are funded within the Pediatric Oncology Financial Assistance Program.

The purpose of the database is to track the number of Ontario families incurring out-of-pocket expenses (e.g. food, accommodation, and child care) and report to stakeholders, the MOHLTC, and donors.

3) Interlink Community Cancer Nurses Database

The patient database contains information on patients and their families who have accessed Interlink Community Cancer Nursing services. Information collected includes patient identifiers, service delivery, frequency of visits, and discharge and re-admission information. This information is available per patient by Interlink nurse and by region.

The purpose of this database is for reporting the nursing workload per activity and the number of patients assisted by the Interlink nurses to the MOHLTC.

4) Successful Academic and Vocational Transition Initiative (SAVTI) Database

The Successful Academic and Vocational Transition Initiative (SAVTI) database contains demographic information on survivors who need assistance in transitioning to post-secondary education or to the workforce. The survivor's name, date of birth, diagnosis, date of diagnosis, general treatment, educational attainment, and vocational goals are maintained in the database.

The purpose of this database is for reporting academic or vocational outcomes to the Ministry of Education. The data collection will be used for evaluation purposes: retrospective study and longitudinal study in the future.

Appendix 4: Compliance Timeline

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Policy must make the following information available:		
Documentation related to the review by the IPC of the policies, procedures and practices implemented by POGO to protect the privacy and confidentiality of PHI received	Y	complete
Identify agent(s) responsible for implementing the process to be followed where records are not securely returned or a certificate of destruction is not received and stipulate time frame when this process must be implemented	Y	complete
Address the process to be followed by the responsible agent(s) where records of PHI are not securely returned, a certificate of destruction is not received or written confirmation of de-identification is not received within the time set out in the Research Agreement	Y	complete
A Research Agreement must be executed with the researchers to whom PHI will be disclosed. The Research Agreement must:		
Secure Return or Disposal:		
Set out the manner and process for de-identification if the records of PHI are required to be de-indentified and retained by the researcher:		
Require the researcher to submit written confirmation that the records were de-identified	Y	complete
Stipulate the time frame following the retention period within which the written confirmation must be provided and the agent of POGO to whom the written confirmation must be provided	Y	complete
Require log of Data Sharing Agreements to be maintained and identify the agent(s) responsible for maintaining log	Y	complete
Maintain a log of executed Data Sharing Agreements. The log must include:		

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The name of the person or organization from whom the PHI was collected or to whom the PHI was disclosed	Y	complete
The date that the collection or disclosure of PHI was approved	Y	complete
The date that the Data Sharing Agreement was executed	Y	complete
The date the PHI was collected or disclosed	Y	complete
The nature of the PHI subject to the Data Sharing Agreement	Y	complete
The retention period for the records of PHI	Y	complete
Whether the records of PHI will be securely returned or disposed of following retention period	Y	complete
The date the records of PHI were securely returned or a certificate of destruction, or the date by which they must be returned or disposed of	Y	complete
A policy and procedure must be developed and implemented requiring written agreements to be entered into with third party service providers prior to permitting third party service providers to access and use the PHI of POGO. Policy and procedures must:		
Require the written agreements to contain the relevant language from the *Template Agreement for All Third Party Service Providers*	Y	30-Sep-2011
Identify agent(s) responsible for ensuring that an agreement is executed, and a process is followed and requirements are satisfied	Y	30-Sep-2011
State that POGO shall not provide PHI to a third party service provider if de-identified and/or aggregate information will serve the purpose, will not provide more PHI than is reasonably necessary to meet purpose, and identify agent(s) responsible for making determination	Y	30-Sep-2011
Identify the agent(s) responsible for ensuring that records of PHI provided to a third party are securely returned or disposed of	Y	30-Sep-2011

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Address process to be followed where records of PHI are not securely returned or a certificate of destruction is not received, identify agent(s) responsible for implementing process, as well as the timeframe	Y	30-Sep-2011
Require a log be maintained of all agreements executed with third parties and identify agent(s) responsible for maintenance of log	Y	30-Sep-2011
Address where documentation related to the execution of agreements with third party service providers will be retained and the agent(s) responsible for retention (Recommendation only)	Y	30-Sep-2011
Require agents to comply with the policy and its procedures	Y	30-Sep-2011
Address how and by whom compliance will be enforced and the consequences of breach	Y	30-Sep-2011
Stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits,* set out frequency of audits and identify the agent(s) responsible for conducting the audits and ensuring compliance	Y	30-Sep-2011
Require agents to notify POGO at first reasonable opportunity if an agent believes there may have been a breach of this policy or its procedures, in accordance with the Policy and Procedures for Privacy Breach Management	Y	30-Sep-2011
A written agreement must be entered into with third party service providers that will be permitted to access and use PHI of POGO. The agreement must:		
General Provisions:		
Describe the status of POGO under the Act, as well as its duties and responsibilities under the Act	Y	21-Sep-2011

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
State whether or not the third party service provider is an agent of the POGO (All third party service providers that are permitted to access and use PHI shall be considered agents of POGO with the possible exception of electronic service providers.)	Y	21-Sep-2011
Explicitly state whether a third party electronic service provider is an agent of POGO in providing services pursuant to the agreement, when applicable	Y	30-Sep-2011
Require the third party service providers that are Agents of POGO to comply with the provisions of the Act and its regulation and privacy and security policies implemented by POGO	Y	21-Sep-2011
Provide a definition of PHI that is consistent with the Act and its regulation (Recommendation only)	Y	21-Sep-2011
Specify the precise nature of the PHI that third party service provider will be permitted to use	Y	30-Sep-2011
Require services provided by the third party to be performed in a professional manner, in accordance with industry standards and practices, and by properly trained agents	Y	21-Sep-2011
Notification :		
Identify the purposes for which the third party is permitted to access and use PHI, including any limitations, conditions or restrictions	Y	21-Sep-2011
Ensure that each use identified in the agreement is consistent with the uses of PHI permitted by the Act and its regulation	Y	21-Sep-2011
Prohibit the third party service provider from using PHI except as permitted by agreement	Y	21-Sep-2011

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Explicitly prohibit an electronic service provider that is not an agent from using PHI except as necessary in the course of providing services pursuant to the agreement	Y	30-Sep-2011
Prohibit the third party from using PHI if other information will serve the purpose and from using more PHI than is reasonably necessary to meet the purpose	Y	21-Sep-2011
Obligations with Respect to Disclosure:		
Identify the purposes for which the third party is permitted to disclose the PHI of POGO, including any limitations, conditions or restrictions	N/A	N/A
Ensure that each disclosure identified in the agreement is consistent with the disclosures of PHI permitted by the Act and its regulation.	N/A	N/A
Prohibit the third party from disclosing PHI (except as permitted in the agreement or required by law) if other information will serve the purpose, or from disclosing more PHI than is reasonably necessary for the purpose	N/A	N/A
Prohibit an electronic service provider that is not an agent of POGO from disclosing PHI to which it has access, except as required by law	N/A	N/A
Secure Transfer:		
Require the third party to securely transfer the records of PHI	N/A	N/A
Set out the secure manner in which records of PHI will be transferred (including what conditions and to whom the records will be transferred, and the procedure that will be followed)	N/A	N/A
Have regard to the Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by POGO when identifying the secure manner of transfer	N/A	N/A

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Require the third party to provide documentation setting out the date, time and mode of transfer of the records of PHI (in cases where the retention or disposal of records of PHI outside the premises of POGO is the primary service provided to POGO)	N/A	N/A
Require the third party to maintain a detailed inventory of the records of PHI transferred	N/A	N/A
Secure Retention:		
Require the third party to ensure that the records of PHI are retained in a secure manner, and identify precise manner in which records of PHI in paper and electronic format will be retained, as well as on other media	Y	30-Sep-2011
Outline responsibilities of third party in securely retaining records of PHI	Y	21-Sep-2011
Have regard to *Policy and Procedures for Secure Retention of Records of Personal Health Information* in identifying the secure manner in which records of PHI will be retained	Y	21-Sep-2011
Obligate the third party to maintain a detailed inventory of the records of PHI being retained on behalf of POGO and a method to track the records (in cases where the retention of records of PHI is the primary service provided to POGO by the third party)	N/A	N/A
Secure Return or Disposal Following Termination of the Agreement:		
Address whether records of PHI will be securely returned or disposed of to POGO in a secure manner	Y	21-Sep-2011
Stipulate the various security measures the third party must take if the records of PHI are required to be returned in a secure manner:		
Time frame following the retention period within which the records must be securely returned	Y	30-Sep-2011
The secure manner in which the records must be returned	Y	30-Sep-2011

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The agent of POGO to whom the records must be securely returned	Y	30-Sep-2011
Have regard to Policy and Procedures for Secure Transfer of Records of Personal Health Information implemented by POGO	Y	21-Sep-2011
Stipulate the various requirements if records of PHI are required to be disposed of in a secure manner:		
Provide a definition of secure disposal consistent with the Act and its regulation	Y	30-Sep-2011
Identify the precise manner in which the records of PHI are to be securely disposed of	Y	30-Sep-2011
Ensure that the method of secure disposal identified is consistent with the Act and its regulation; orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario. Regard may be had to Policy and Procedures for Secure Disposal of Records of Personal Health Information implemented by POGO	Y	21-Sep-2011
Identify the agent of POGO to whom the certificate of destruction must be provided and the time frame following secure disposal within which the certificate of destruction must be provided	Y	30-Sep-2011
Indicate the required content of the certificate of destruction:		
Identification of the disposed records of PHI	On data destruction form	
The date, time, location and method of secure disposal employed		
The name and signature of the person who performed the secure disposal		
Secure Disposal as a Contracted Service:		

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Set out the responsibilities of the third party where the disposal of records of PHI is the primary service provided to POGO:		
The time frame within which the records are required to be securely disposed of	N/A	N/A
The precise method by which records must be securely disposed of	N/A	N/A
The conditions pursuant to which the records will be securely disposed of	N/A	N/A
The person(s) responsible for ensuring the secure disposal of the records	N/A	N/A
Enable POGO to witness the secure disposal of the records of PHI, subject to reasonable terms and conditions as may be required	N/A	N/A
Implementation of Safeguards:		
Require the third party service provider to take steps to ensure that PHI accessed and used is protected against theft, loss and unauthorized use or disclosure, unauthorized copying, modification or disposal	Y	21-Sep-2011
Detail the reasonable steps that the third party must implement to protect PHI	Y	30-Sep-2011
Training of Agents of the Third Party Service Provider:		
Require the third party to provide training to its agents on the importance of protecting PHI and on the consequence of a breach	Y	21-Sep-2011
Require the third party to ensure that its agents who will have access to the records of PHI agree to comply with the terms and conditions of the agreement prior to being given access PHI, and set out the method by which this will be ensured	Y	21-Sep-2011
Subcontracting of Services:		

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Require third party to provide POGO with advance notice of its intention to subcontract services, if the agreement permits subcontracting	N/A	N/A
Require third party to enter into written agreement with subcontractor on terms consistent with its obligations to the POGO and provide a copy of the written agreement to the POGO	N/A	N/A
Notification:		
Require the third party to notify POGO at first reasonable opportunity if there has been a breach or suspected breach of the PHI or if PHI has been stolen, lost or accessed by unauthorized persons	Y	21-Sep-2011
Identify whether notification must be verbal, written or both and to whom the notification must be provided	Y	21-Sep-2011
Require third party to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons	Y	21-Sep-2011
Consequences of Breach and Monitoring Compliance:		
Outline the consequences of breach of the agreement	Y	30-Sep-2011
Indicate whether POGO will be auditing compliance with the agreement, and if so, the manner in which compliance will be audited, and the notice that will be provided of the audit	Y	21-Sep-2011
POGO must maintain a log of executed agreements with third party service providers. The log must include:	Y	10-Feb-2011
The name of the third party service provider	Y	10-Feb-2011
The nature of the services provided that require access and use of PHI	Y	10-Feb-2011
The date that the agreement was executed	Y	10-Feb-2011
The date that the records of PHI or access was provided	Y	10-Feb-2011
The nature of the PHI provided	Y	10-Feb-2011
The date of termination of the agreement	Y	10-Feb-2011
Whether the records of PHI will be securely returned or disposed of following termination of the agreement	Y	10-Feb-2011

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The date the records of PHI were securely returned or a certificate of destruction was provided, or the date by which the records of PHI must be returned or disposed of or access terminated	Y	10-Feb-2011
Tracking Approved Linkages of Records of Personal Health Information:		
Require that a log be maintained of the linkages of records of PHI approved by POGO and identify the agent(s) responsible for maintaining such a log.	Y	30-Sep-2011
Address where documentation related to the receipt, review, approval or denial of request will be retained and agent(s) responsible for retaining this documentation (Recommendation only)	Y	30-Sep-2011
POGO must maintain a log of linkages of records of PHI approved by the POGO. The log must include:	Y	10-Feb-2011
Name of the agent, person or organization who requested the linkage.	Y	10-Feb-2011
Date that the linkage of records of PHI was approved.	Y	10-Feb-2011
Nature of the records of PHI linked	Y	10-Feb-2011
A policy and procedures must be developed and implemented to identify the circumstances in which privacy impact assessments are required to be conducted. The policy and procedures must:		
Stipulate the required content of a PIA:		
Require that a log be maintained of privacy impact assessments that have been completed, that have been undertaken but that have not been completed, that have not been undertaken, and the agent(s) responsible for maintaining such a log	Y	complete
POGO must maintain a log of PIAs that have been completed and of PIAs that have been undertaken but that have not been completed. The log shall describe:		
The data holding, information system, technology or program involving PHI	Y	30-Sep-11
The date that the PIA was completed or is expected to be completed	Y	30-Sep-11

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The agent(s) responsible for completing or ensuring the completion of the PIA	Y	30-Sep-11
The recommendations arising from the PIA	Y	30-Sep-11
The agent(s) responsible for addressing each recommendation, and the date that each recommendation was or is expected to be addressed	Y	30-Sep-11
The manner in which each recommendation was or is expected to be addressed.	Y	30-Sep-11
A policy and procedures must be developed and implemented to address privacy breaches. The policy and procedures must:		
Address the manner and format in which the findings recommendations of the investigation are communicated and must include discussion of:		
Require that a log be maintained of privacy breaches and for tracking the recommendations from the investigation of privacy breaches, and identify the agent(s) responsible for maintenance of log	Y	complete
POGO shall maintain a log of privacy breaches setting out:		
The date of the privacy breach	Y	complete
The date that the privacy breach was identified or suspected	Y	complete
Whether the privacy breach was internal or external	Y	complete
The nature of the PHI that was the subject matter of the privacy breach	Y	complete
The date that the privacy breach was contained and nature of the containment	Y	complete
The date that the HIC or other organization that disclosed the PHI to POGO was notified	Y	complete
The date that the investigation of the privacy breach was completed	Y	complete
The agent(s) responsible for conducting the investigation	Y	30-Sep-11
The recommendations arising from the investigation	Y	complete
The agent(s) responsible for addressing each recommendation	Y	30-Sep-11
The date each recommendation was or is expected to be addressed	Y	complete

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The manner in which each recommendation was or is expected to be addressed	Y	complete

A policy and procedures must be developed and implemented to address the process to be followed when responding to privacy complaints. (It may be a stand-alone document or combined with the *Policy and Procedures for Privacy Inquiries.*) The policy and procedures must:

Require that a letter must be provided to the individual making the privacy complaint when an investigation will be undertaken, including:	Y	22-Sep-2011
Acknowledgement of receipt of the privacy complaint	Y	22-Sep-2011
Notice that an investigation of the privacy complaint will be undertaken	Y	22-Sep-2011
An explanation of the privacy complaint investigation procedure	Y	22-Sep-2011
An indication of whether the individual will be contacted for further information concerning the privacy complaint	Y	22-Sep-2011
The projected time frame for completion of the investigation	Y	22-Sep-2011
The nature of the documentation that will be provided to the individual following the investigation	Y	22-Sep-2011
Identify the agent(s) responsible for sending the above noted letters to the individuals making privacy complaints	Y	22-Sep-2011
POGO shall maintain a log of privacy complaints received setting out:		
The date that the privacy complaint was received and the nature of the complaint	Y	30-Sep-2011
The determination as to whether or not the privacy complaint will be investigated and the date of the determination	Y	30-Sep-2011

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The date that the individual making the complaint was advised that the complaint will not be investigated an was provided a response	Y	30-Sep-2011
The date that the individual making the complaint was advised that the complaint will be investigated	Y	30-Sep-2011
The agent(s) responsible for the investigation	Y	30-Sep-2011
The dates that the investigation was commenced and completed	Y	30-Sep-2011
The recommendations arising from the investigation	Y	30-Sep-2011
The agent(s) responsible for addressing each recommendation	Y	30-Sep-2011
The date each recommendation was or is expected to be addressed	Y	30-Sep-2011
The manner in which the recommendation was or is expected to be addressed	Y	30-Sep-2011
The date that the individual making the complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint	Y	30-Sep-2011
Maintain a log of agents granted approval to access the premises of POGO		
The log must include:		
The date of the next audit of access	Y	complete
Develop and implement a policy and procedures that sets out the types of security audits that are required to be conducted	N	1-Jan-12
The audits required to be conducted shall include assessment of:		
Compliance with the security policies, procedures and practices implemented by POGO	N	1-Jan-12
Threat and risk	N	1-Jan-12
Security reviews	N	1-Jan-12
Vulnerability	N	1-Jan-12
Penetration testing	N	1-Jan-12
Ethical hacks and reviews of system control and audit logs	N	1-Jan-12
For each security audit that is required to be conducted, set out:		
The purposes of the security audit	N	1-Jan-12

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The nature and scope of the security audit	N	1-Jan-12
The agent(s) responsible for conducting the security audit	N	1-Jan-12
A requirement for a security audit schedule to be developed and identification of the agent(s) responsible for developing the schedule	N	1-Jan-12
The frequency with which and the circumstances in which each security audit is required to be conducted	N	1-Jan-12
The criteria that must be considered in selecting the subject matter of the audit	N	1-Jan-12
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	N	1-Jan-12
The documentation that must be completed in undertaking each security audit	N	1-Jan-12
The agent(s) responsible for documentation	N	1-Jan-12
The agent(s) to whom this documentation must be provided	N	1-Jan-12
The required content of the documentation	N	1-Jan-12
The process to be followed in conducting the audit	N	1-Jan-12
The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program	N	1-Jan-12
The process that must be followed in addressing the recommendations arising from security audits, including	N	1-Jan-12
The agent(s) responsible for assigning other agent(s) to address the recommendations	N	1-Jan-12
The agents responsible for establishing timelines to address recommendations	N	1-Jan-12
The agents responsible for addressing the recommendations and for monitoring and ensuring the implementation of recommendations	N	1-Jan-12

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The nature of the documentation that must be gathered at the conclusion of the security audit, including:	N	1-Jan-12
The agent(s) responsible for completing the documentation	N	1-Jan-12
The required content of the documentation	N	1-Jan-12
The agent(s) to whom the documentation must provided	N	1-Jan-12
The manner and format in which the findings and status of security audits are communicated, including:	N	1-Jan-12
A discussion of the agent(s) responsible for communicating the findings of the security audit	N	1-Jan-12
The mechanism and format for communicating the findings	N	1-Jan-12
The time frame within which the findings must be communicated	N	1-Jan-12
To whom the findings of the security audit will be communicated, including a requirement that the CEO or Executive Director be contacted	N	1-Jan-12
A requirement for a log to be maintained of security audits	N	1-Jan-12
The agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the security audits are addressed within the identified time frame	N	1-Jan-12
Where documentation related to security audits will be retained and the agent(s) responsible for retaining this documentation	N	1-Jan-12
Require agents to notify POGO at the first reasonable opportunity, in accordance with the Policy and Procedures for Information Security Breach Management if an agent breaches or believes there may have been a breach of this policy or its procedures	N	1-Jan-12
Maintain a log of security audits that have been completed. The log shall set out:		
The nature and type of the security audit conducted	N	1-Jan-12

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The date that the security audit was completed	N	1-Jan-12
The agent(s) responsible for completing the security audit	N	1-Jan-12
The recommendations arising from the security audit	N	1-Jan-12
The agent(s) responsible for addressing each recommendation	N	1-Jan-12
The date that each recommendation was or is expected to be addressed	N	1-Jan-12
The manner in which each recommendation was or is expected to be addressed.	N	1-Jan-12
Develop and implement a comprehensive and integrated corporate risk management framework	N	1-Dec-12
Address the agent(s) responsible and the process that must be followed in identifying risks to the ability of the POGO to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of the information	N	1-Dec-12
Discuss the agents or other organizations that must be consulted in identifying these risks	N	1-Dec-12
Describe the documentation that must be completed, provided and/or executed	N	1-Dec-12
Identify the agent(s) responsible for completing, providing and/or executing the documentation	N	1-Dec-12
Identify the agent(s) to whom this documentation must be provided	N	1-Dec-12
Set out the required content of the documentation	N	1-Dec-12
In discussing the assessment of the likelihood of the risks occurring and the potential impact if they occur, address:		
The agent(s) responsible	N	1-Dec-12
The process that must be followed and the criteria that must be considered in ranking the risks	N	1-Dec-12
Discussion of the agents or other organizations that must be consulted in assessing and ranking the risks	N	1-Dec-12

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The documentation that must be completed in assessing the risk	N	1-Dec-12
The documentation that must be completed in setting out the rationale for the assessment and ranking of the risks	N	1-Dec-12
The agent(s) responsible for completing the documentation	N	1-Dec-12
The agent(s) to whom this documentation must be provided	N	1-Dec-12
The require content of this documentation	N	1-Dec-12
Policies related to identifying strategies to mitigate the actual or potential risks to privacy that were identified must address:		
The agent(s) responsible	N	1-Dec-12
The process that must be followed and criteria that must be considered in identifying these strategies	N	1-Dec-12
Process for implementing the mitigation strategies	N	1-Dec-12
The agents or other organizations that must be consulted in identifying and implementing the mitigation strategies	N	1-Dec-12
The agent(s) responsible for assigning other agent(s) to implement the mitigation strategies, establishing timelines to implement the mitigation strategies and for monitoring and ensuring that the mitigation strategies have been implemented	N	1-Dec-12
The documentation that must be completed in identifying, implementing, monitoring and ensuring the implementation of the mitigation strategies	N	1-Dec-12
The agent(s) responsible for completing this documentation	N	1-Dec-12
The agent(s) to whom this documentation must be provided	N	1-Dec-12
The required content of the documentation	N	1-Dec-12
In addressing the manner and format in which the result of the corporate risk management process, including the identification and assessment of risk, the strategies to mitigate actual or potential risks to privacy and the status of implementation of the mitigation strategies, the policy must describe:		

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The agent(s) responsible for communicating and reporting the results of the corporate risk management process	N	1-Dec-12
The nature and format of the communication	N	1-Dec-12
To whom the results will be communicated and reported, including the CEO or the Executive Director	N	1-Dec-12
The approval and endorsement of the results of the risk management process	N	1-Dec-12
Require corporate risk register to be maintained and reviewed on an ongoing basis and that confidentiality of that information continues to be identified, assessed and mitigated	N	1-Dec-12
Address the frequency of review of this risk register, the agent(s) responsible and the process that must be followed in reviewing and amending the risk register	N	1-Dec-12
Address the manner in which the corporate risk management framework will be integrated into the policies, procedures and practices of the POGO and into projects undertaken by POGO	N	1-Dec-12
Develop and maintain a corporate risk register identifying risks that may negatively affect the ability of POGO to protect PHI	N	1-Dec-12
For each risk identified, include:		
An assessment of the risk	N	1-Dec-12
A ranking of the risk	N	1-Dec-12
The mitigation strategy to reduce the likelihood of the risk occurring	N	1-Dec-12
The date that the mitigation strategy was implemented	N	1-Dec-12
The agent(s) responsible for implementation of the mitigation strategy	N	1-Dec-12
Develop and implement a policy requiring a consolidated and centralized log to be maintained of all recommendations arising from PIAs, privacy audits, security audits and the investigation of privacy complaints and privacy and security breaches and reviews by the IPC	Y	complete

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
The policy and procedures must address:		
The frequency with which and the circumstances in which the consolidated and centralized log must be reviewed	Y	complete
The agent(s) responsible for reviewing and amending the log	Y	complete
That a log be updated each time a recommendation has been addressed (Recommendation only)	Y	complete
That a log be reviewed on an ongoing basis (Recommendation only)	Y	complete
The process that must be followed in this regard	Y	complete
Require agents to comply with the policy and its procedure and address how and by whom compliance will be enforced and the consequences of breach	Y	complete
Stipulate that compliance will be audited in accordance with the *Policy and Procedures for Privacy Breach Management* and/or the *Policy and Procedures for Information Security Breach Management,* if an agent breaches or believes there may have been a breach of this policy or its procedures	Y	complete
Develop and maintain a consolidated and centralized log of all recommendations arising from PIAs, privacy audits, security audits and the investigation of privacy complaints and privacy and security breaches and reviews by the IPC	Y	complete
Set out the name and date of the document, investigation, audit and/or review from which the recommendation arose	Y	complete
For each recommendation, require the log to set out:		
The recommendation made	Y	complete
The manner in which the recommendation was addressed	Y	complete
The date that the recommendation was addressed	Y	complete
The agent(s) responsible for addressing the recommendation	Y	complete

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Develop and implement a policy to protect and ensure the continued availability of the information technology environment of POGO in the event of business interruptions, including natural disasters	N	1-Sep-12
This policy must address:		
Notification of the interruption or threat	N	1-Sep-12
Documentation of the interruption or threat	N	1-Sep-12
Assessment of the severity of the interruption or threat	N	1-Sep-12
Activation of the business continuity plan	N	1-Sep-12
The disaster recovery plan	N	1-Sep-12
Recovery of PHI	N	1-Sep-12
The agent(s) or other persons or organizations that must be notified of business interruptions	N	1-Sep-12
The time frame within which notification must be provided	N	1-Sep-12
The manner and format of notification	N	1-Sep-12
The nature of the information that must be provided upon notification	N	1-Sep-12
Documentation that must be completed	N	1-Sep-12
Development of a contact list of all agents that must be notified of business interruptions	N	1-Sep-12
The identity of the agent(s) responsible for assessing the severity level	N	1-Sep-12
The criteria pursuant to which this assessment is to be made	N	1-Sep-12
The agent(s) or other persons or organizations that must be consulted in assessing the severity level of the interruption or threat	N	1-Sep-12
The documentation that must be completed arising from this assessment	N	1-Sep-12
The required content of the documentation	N	1-Sep-12
The agent(s) to whom the documentation must be provided	N	1-Sep-12
To whom the results of this assessment must be reported	N	1-Sep-12

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Set out agent(s) responsible and process to be followed in conducting an initial impact assessment of the interruption, including its impact on the technical and physical infrastructure and business processes of the POGO, including:		
The agents and other persons or organizations that are required to be consulted in undertaking the assessment	N	1-Sep-12
The documentation that must be completed	N	1-Sep-12
The agent(s) responsible for completing the documentation	N	1-Sep-12
The agent(s) to whom the documentation must be provided	N	1-Sep-12
To whom the results of the initial impact assessment must be communicated	N	1-Sep-12
In addressing the damage assessment and determination of the expected effort required to resume and restore infrastructure elements, the policy should:		
Set out agent(s) responsible for conducting a damage assessment	N	1-Sep-12
The manner in which the assessment will be conducted	N	1-Sep-12
Persons required to be consulted during the assessment	N	1-Sep-12
Requirements that must be met and the criteria to be considered when undertaking the assessment	N	1-Sep-12
The documentation that must be completed	N	1-Sep-12
Agent(s) to whom the documentation must be provided	N	1-Sep-12
Agent(s) to whom the results must be communicated.	N	1-Sep-12
In addressing the resumption and recovery, the policy should address:		
The agent(s) responsible for resumption and recovery	N	1-Sep-12
The procedure that must be utilized in resumption and recovery	N	1-Sep-12
The prioritization of resumption and recovery activities	N	1-Sep-12
The criteria pursuant to which prioritization of resumption and recovery activities is determined	N	1-Sep-12
The recovery time objectives for critical applications	N	1-Sep-12

IPC Manual Requirements	Requirement Met	Date to be Completed/ date completed
Persons required to be consulted with respect to the resumption and recovery activities	N	1-Sep-12
The documentation that must be completed	N	1-Sep-12
The required content of the documentation	N	1-Sep-12
Agent responsible for completing the documentation	N	1-Sep-12
Agent(s) to whom the documentation must be provided	N	1-Sep-12
Agent(s) to whom the results must be communicated	N	1-Sep-12
Outline the procedure by which decisions made and actions taken during business interruptions and threats to the operating capabilities of the prescribed person or prescribed entity will be documented and communicated, including identification of by and to whom it will be communicated	N	1-Sep-12
In addressing the testing, maintenance and assessment of the business continuity and disaster recovery plan, the policy must:		
Identify the frequency of testing	N	1-Sep-12
Identify the agent(s) responsible for ensuring that the business continuity and delivery plan is tested and maintained	N	1-Sep-12
Identify the agent(s) responsible for amending the business continuity and discovery plan as a result of the testing	N	1-Sep-12
Outline the procedure to be followed in testing, maintaining and assessing and amending the plan and any amendments	N	1-Sep-12
Address the agent(s) responsible and the procedure to be followed in communicating the plan and any amendments to agents, including the method and nature of the communication	N	1-Sep-12
Identify the agent(s) responsible for managing communications in relation to the threat or interruption, including the method and nature of the communication	N	1-Sep-12

Appendix 5: IPC Recommendations from the 2008 Review

Section	Date Completed
Privacy Breach Policy (pages 4-5)	2-Oct-09
Disciplinary Action-Privacy Infractions Policy (page 5)	2-Oct-09
De-Identifying Personal Health Information Policy (pages 5-6)	2-Oct-09
Email Policy (page 6)	2-Oct-09
Secured Faxes Policy (page 6)	2-Oct-09
Information Available Related to Privacy and Security Policies and Procedures (page 7)	27-Oct-10
Ethics Review Process Policy (pages 9-10)	Oct-09
Retention and Destruction of Data Policy (page 11)	16-Oct-09
Staff Education and Training Policy (pages 11-12)	Dec-10
Data Sharing Agreements (pages 13-14)	5 Pediatric AfterCare data sharing agreements are complete; Adult AfterCare data sharing agreement with Princess Margaret Hospital signed Oct. 2009; Adult AfterCare data sharing agreement with Ottawa General Hospital is addressed in the CHEO agreement; Satellite data sharing agreements are in discussion (Fall 2010) and are to be complete 2011/12
Data Sharing Agreements (pages 13-14)	ICES agreement amendments: June 2009; CCO data sharing agreement: March 2010
Project-Specific Privacy Impact Assessment (page 14)	Oct-10
Research Agreement (page 15-16)	Oct-10
Privacy Audit Program (page 17)	Dec-10
Security Audit Program (page 17)	Dec-10
Encryption Policy (page 18)	Dec-10
Threat and Risk Assessment (page 18)	▪ Since the threat and risk assessment completion in June 2008, POGO has implemented the following security control recommendations: 1. Disable the VPN access afterhours; (completed March 2011) 2. Implement the configuration standards of the network devices that have been developed by the IT Team; (completed March 2011)

3. Complete the implementation of all documented firewall controls developed by the IT Team; (To be completed by November 2011).

4. Complete the implementation of the documented VPN rules. See item 3.