



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

**Re-Submitted: September 29, 2017
Review Period: 2014-2017**

Table of Contents

BACKGROUND INFORMATION

Introduction	4
Background	6
Definitions	8

Part 1- PRIVACY DOCUMENTATION

1. Privacy Policy in Respect of POGO's Status as a Prescribed Entity	10
<i>Status under the Act</i>	10
<i>Privacy and Security Accountability Framework</i>	10
<i>Collection of Personal Health Information</i>	11
<i>Use of Personal Health Information</i>	11
<i>Disclosure of Personal Health Information</i>	12
<i>Secure Retention, Transfer, and Disposal of Records of Personal Health Information</i>	12
<i>Implementation of Administrative, Technical, and Physical Safeguards</i>	13
<i>Inquiries, Concerns, or Complaints Related to Information Practices</i>	13
<i>Transparency of Practices in Respect of Personal Health Information</i>	13
2. Policy and Procedures for Ongoing Review of Privacy Policies, Procedures, and Practices	14
3. Policy on the Transparency of Privacy Policies, Procedures, and Practices	15
4. Policy and Procedures for the Collection of Personal Health Information	16
<i>Review and Approval Process</i>	17
<i>Conditions or Restrictions on the Approval</i>	18
<i>Secure Retention</i>	18
<i>Secure Transfer</i>	18
<i>Secure Return or Disposal</i>	18
5. List of Data Holdings Containing Personal Health Information	19
6. Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information	19
7. Statements of Purpose for Data Holdings Containing Personal Health Information	20
8. Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information	20
<i>Review and Approval Process</i>	21
<i>Conditions or Restrictions on the Approval</i>	21
<i>Notification and Termination of Access and Use</i>	22
<i>Secure Retention</i>	22
<i>Secure Disposal</i>	23
<i>Tracking Approved Access to and Use of Personal Health Information</i>	23
<i>Compliance, Audit, and Enforcement</i>	23
9. Log of Agents Granted Approval to Access and Use Personal Health Information	23
10. Policy and Procedures for the Use of Personal Health Information for Research	24
<i>Where the use of Personal Health Information is Permitted for Research</i>	24

<i>Distinction between the Use of Personal Health Information for Research and Other Purposes</i>	24
<i>Review and Approval Process</i>	24
<i>Conditions or Restrictions on the Approval</i>	25
<i>Secure Retention</i>	26
<i>Secure Return or Disposal</i>	26
<i>Tracking Approved Uses of Personal Health Information for Research</i>	27
<i>Where the Use of Personal Health Information is not Permitted for Research</i>	27
11. Log of Approved Uses of Personal Health Information for Research	27
12. Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research	27
<i>Where the Disclosure of Personal Health Information is Permitted</i>	28
<i>Review and Approval Process</i>	28
<i>Conditions or Restrictions on the Approval</i>	29
<i>Secure Transfer</i>	29
<i>Secure Return or Disposal</i>	29
<i>Documentation Related to Approved Disclosures of Personal Health Information</i>	30
<i>Where the Disclosure of Personal Health Information is not Permitted</i>	30
13. Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements	30
<i>Where the Disclosure of Personal Health Information is Permitted for Research</i>	30
<i>Review and Approval Process</i>	30
<i>Conditions or Restrictions on the Approval</i>	31
<i>Secure Transfer</i>	32
<i>Secure Return or Disposal</i>	32
<i>Documentation Related to Approved Disclosures of Personal Health Information</i>	32
<i>Where the Disclosure of Personal Health Information is not Permitted for Research</i>	32
14. Template Research Agreement	32
<i>General Provisions</i>	32
<i>Purposes of Collection, Use and Disclosure</i>	33
<i>Compliance with the Statutory Requirements for the Disclosure for Research Purposes</i>	33
<i>Secure Transfer</i>	34
<i>Secure Retention</i>	34
<i>Secure Return or Disposal</i>	34
<i>Notification</i>	35
<i>Consequences of Breach and Monitoring Compliance</i>	36
15. Log of Research Agreements	36
16. Policy and Procedures for the Execution of Data Sharing Agreements	36
17. Template Data Sharing Agreement	37
<i>General Provisions</i>	37
<i>Purposes of Collection, Use and Disclosure</i>	38
<i>Secure Transfer</i>	38
<i>Secure Retention</i>	38
<i>Secure Return or Disposal</i>	39
<i>Notification</i>	39
<i>Consequences of Breach and Monitoring Compliance</i>	40
18. Log of Data Sharing Agreements	40
19. Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information	41

20. Template Agreement for All Third Party Service Providers	41
<i>General Provisions</i>	42
<i>Obligations with Respect to Access and Use</i>	42
<i>Obligations with Respect to Disclosure</i>	43
<i>Secure Transfer</i>	43
<i>Secure Retention</i>	44
<i>Secure Return or Disposal Following Termination of the Agreement</i>	44
<i>Secure Disposal as a Contracted Service</i>	45
<i>Implementation of Safeguards</i>	45
<i>Training of Agents of the Third Party Service Provider</i>	45
<i>Subcontracting of the Services</i>	46
<i>Notification</i>	46
<i>Consequences of Breach and Monitoring Compliance</i>	46
21. Log of Agreements with Third Privacy Service Providers	46
22. Policy and Procedures for the Linkage of Records of Personal Health Information	46
<i>Review and Approval Process</i>	47
<i>Conditions or Restrictions on the Approval</i>	47
<i>Process for the Linkage of Records of Personal Health Information</i>	48
<i>Retention</i>	48
<i>Secure Disposal</i>	48
<i>Compliance, Audit and Enforcement</i>	48
<i>Tracking Approved Linkages of Records of Personal Health Information</i>	49
23. Log of Approved Linkages of Records of Personal Health Information	49
24. Policy and Procedures with Respect to De-Identification and Aggregation	49
25. Privacy Impact Assessment Policy and Procedures	50
26. Log of Privacy Impact Assessments	52
27. Policy and Procedures in Respect of Privacy Audits	53
28. Log of Privacy Audits	54
29. Policy and Procedures for Privacy Breach Management	54
30. Log of Privacy Breaches	57
31. Policy and Procedures for Privacy Complaints	58
32. Log of Privacy Complaints	60
33. Policy and Procedures for Privacy Inquiries	60

Part 2- SECURITY DOCUMENTATION

1. Information Security Policy	65
2. Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices	67
3. Policy and Procedures for Ensuring Physical Security of Personal Health Information	68
<i>Policy, Procedures and Practices with Respect to Access by Agents</i>	68
<i>Theft, Loss and Misplacement of Identification Cards, Access Cards and Keys</i>	69
<i>Termination of the Employment, Contractual or Other Relationship</i>	70
<i>Notification When Access is No Longer Required</i>	70
<i>Audits of Agents with Access to the Premises</i>	70
<i>Tracking and Retention of Documentation Related to Access to the Premises</i>	71
<i>Policy, Procedures and Practices with Respect to Access by Visitors</i>	71
4. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity	71
5. Policy and Procedures for Secure Retention of Records of Personal Health Information	71
6. Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices	72
<i>Where Personal Health Information is Permitted to be Retained on a Mobile Device</i>	72
<i>Approval Process</i>	73
<i>Conditions or Restrictions on the Retention of Personal Health Information on a Mobile Device</i>	73
<i>Where Personal Health Information is not Permitted to be Retained on a Mobile Device</i>	74
7. Policy and Procedures for Secure Transfer of Records for Personal Health Information	74
8. Policy and Procedures for Secure Disposal of Records of Personal Health Information	76
9. Policy and Procedures Relating to Passwords	78
10. Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs	79
11. Policy and Procedures for Patch Management	81
12. Policy and Procedures Related to Change Management	82
13. Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information	83
14. Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information Policy and Procedures Relating to Passwords	84

15. Policy and Procedures In Respect of Security Audits	85
16. Log of Security Audits	86
17. Policy and Procedures for Information Security Breach Management	86
18. Log of Information Security Breaches	89

Part 3- HUMAN RESOURCES DOCUMENTATION

1. Policy and Procedures for Privacy Training and Awareness	90
2. Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training	92
3. Policy and Procedures for Security Training and Awareness	92
4. Log of Attendance at Initial Security Orientation and Ongoing Security Training	94
5. Policy and Procedures for the Execution of Confidentiality Agreements by Agents	94
6. Template Confidentiality Agreement with Agents	95
<i>General Provisions</i>	95
<i>Obligations with Respect to Collection, Use and Disclosure of Personal Health Information</i>	95
<i>Termination of the Contractual, Employment or Other Relationship</i>	96
<i>Notification</i>	96
<i>Consequences of Breach and Monitoring Compliance</i>	96
7. Log of Executed Confidentiality Agreements with Agents	96
8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program	96
9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program	97
10. Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship	98
11. Policy and Procedures for Discipline and Corrective Action	99

Part 4 – ORGANIZATIONAL AND OTHER DOCUMENTATION

1. Privacy Governance and Accountability Framework	105
2. Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program	106
3. Corporate Risk Management Framework	107
4. Corporate Risk Register	108
5. Policy and Procedures for Maintaining a Consolidated Log of Recommendations	107
6. Consolidated Log of Recommendations	109
7. Business Continuity and Disaster Recovery Plan	109

Background Information

Introduction

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

POGO's mandate is to:

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

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);
- Children's Hospital of Eastern Ontario (Ottawa); as well as

- a growing number of partners drawn from community hospitals, community services, other members of the health care sector, families of children who have or have had cancer, corporate and private benefactors, and volunteers.

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

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

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

Major components of current POGO activities include:

- 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) was designated as the oversight body responsible for ensuring compliance with the *Act*. The *Act* establishes rules for the collection, use, and disclosure of personal health information by health information custodians that protect the confidentiality and privacy of individuals with respect to that personal health information. In particular, the *Act* stipulates that health information custodians may only collect, use, and disclose personal health information with the consent of the individual to whom the personal health information relates, or as permitted or required by the *Act*.

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

Subsection 45(3) of the *Act* requires each prescribed entity to have in place practices and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Subsection 45(3) further requires each prescribed entity to ensure that these practices and procedures are approved by the IPC in order for health information custodians to be able to disclose personal health information to the prescribed entity without consent and for the prescribed entity to:

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

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

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

Definitions

ACTS Database

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

Agents

- 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.

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.

Information Technology (IT) Team

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

Interlink Community Nurses

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

POFAP - POGO's Financial Assistance Program

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

POGO AfterCare Adult Programs

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

POGO Satellite Community Hospitals

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

POGO Tertiary Pediatric Oncology Hospital Partners

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

POGONIS Database

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

Prescribed Entities

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

Privacy and Data Security Code

- The 10 tenets of POGO's Privacy Program.

Privacy and Data Security Procedures

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

Privacy and Security Policies and Procedures (the Manual)

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

Privacy Team

- Includes the POGO Privacy Officers and administrative support personnel.

The Privacy Program

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

Third Party Service Providers

- Individuals or organizations that provide a service to or on behalf of POGO in the role of contractors or consultants.

SAVTI – POGO's Successful Academic Vocational Transition Initiative

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

Part 1 – Privacy Documentation

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

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

Status under the Act

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

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

Privacy and Security Accountability Framework

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

The Privacy Program, which includes the security program, identifies the positions of the Privacy Officers as having the authority to manage the Privacy Program, and POGO’s System & Network Analyst, and Database Administrator, Analyst & Programmer as having the day-to-day authority to manage POGO’s Information Technology (IT) Security Program. The Privacy Program also defines the responsibilities of these two positions by identifying the unique roles of each individual, as related to the specific program functions and key activities. POGO’s Privacy Officers report to the Chief Executive Officer of POGO. POGO’s System & Network Analyst reports to the Privacy Officers.

Collection of Personal Health Information

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

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

POGO's Privacy and Data Security Code and Policy #9.1.5 (*Data Holding Containing Personal Health Information*) indicate that POGO maintains a list of its data holdings of personal health information. The Privacy Officers are identified 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 and Policy # 9.1.7 (*Use of Personal Health Information for Research*) and Policy # 9.1.1 (*Process for 44 and 45 Projects*) and Policy # 9.1.13 (*De-Identified and Aggregate Personal Health Information*) describe the purpose for which POGO uses personal health information and includes policies and procedures that distinguish between the use of personal health information and the use of de-identified and/or aggregate information under section 45 of the *Act* and the use of personal health information for research purposes. The Privacy Program further specifies that the use of personal health information must be consistent with the uses of personal health information permitted by the *Act* and its regulation.

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

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

Disclosure of Personal Health Information

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

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

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

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

The Privacy Program and Policy #9.2.6 (*Retention, Return and Destruction of Data*), Policy #9.2.9 (*Secure Transfer of Personal Health Information*) and Policy #9.2.7 (*Personal Health Information on Mobile Devices*) address the secure retention of records of personal health information in paper and electronic format, including the acceptable use of portable media and mobile devices for the collection, transfer, and storage of personal health information. The Privacy Program addresses the permitted retention periods and specifies methods for the secure transfer and destruction of personal health information depending on the media on which it is stored. Identifiable personal health information is secured and only retained for as long as necessary to meet the purposes of long-term analysis and reporting. Personal health information that is no longer required to fulfill the identified purposes is de-identified or securely destroyed. POGO has developed guidelines and implemented procedures to govern the de-identification of personal health information and has developed guidelines and implemented procedures to govern the secure destruction of personal health information.

Implementation of Administrative, Technical, and Physical Safeguards

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

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

Inquiries, Concerns, or Complaints Related to Information Practices

The Privacy Program identifies the Privacy Officers of POGO as the contacts 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 filing inquiries or complaints.

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

Transparency of Practices in Respect of Personal Health Information

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

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

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

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

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

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

The Privacy Program further states that the Privacy Officers are responsible for determining the procedure to be followed in communicating the amended or newly developed privacy policies, procedures, and practices. For agents, the Privacy Officers are guided by POGO Policy #9.3.1 (*Privacy and Security Training*) which stipulates that the Privacy Officers will be responsible for determining the method and nature when communicating the amended or newly developed privacy policies, procedures, and practices. The Privacy Program also identifies that the Privacy Officers are responsible for the procedure to be followed in reviewing and amending the communication materials available to the public and other stakeholders as a result of the amended or newly developed privacy policies, procedures and practices.

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

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, 2014) 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; and
6. The name, title, mailing address, and contact information of the persons(s) to whom inquiries, concerns, or complaints regarding compliance with the privacy policies, procedures, and practices implemented and regarding compliance with the *Act* and its regulation may be directed.

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

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

1. The status of POGO under the *Act*;
2. POGO's obligations under the *Act*;
3. The types of personal health information collected;
4. The POGO tertiary hospital partner organizations and prescribed registry from which personal health information is collected;
5. The purposes for which personal health information is collected;

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

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

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

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

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

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

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

Agents are required to comply with the policy and procedures in regard to the collection of personal health information. Compliance is enforced by the Privacy Officers who are also responsible for enforcing consequences or a breach. Compliance is also audited in accordance with POGO's

policies and procedures in respect of POGO's Privacy Audit Program, and Policy #9.1.15 (*Privacy Audits*) which state that privacy audits are carried out annually at minimum by the Privacy Officers.

POGO Policy #9.1.16 (*Privacy Breach and Incident Management*) requires 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 allowed POGO to retrospectively add personal health information data elements (treatment and outcome information) to the POGONIS database on the cases diagnosed between 1985 and 1994. This same information was already collected for the 1995 and forward case population. These additional personal health information data elements were reviewed and approved by POGO's Senior Database Administrator, POGO's Senior Adviser, Policy and Clinical Affairs, Medical Director, and other external content experts if applicable, who are responsible for reviewing and determining whether to approve a collection of personal health information and determining the process and requirements to be followed and were subsequently endorsed by the Program Directors from each of the POGO tertiary pediatric oncology hospitals. The additional retrospective data collection was completed in April 2013.

In addition, POGO maintains four 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);
- Satellite service utilization;
- Interlink Community Nurses; and
- AfterCare Treatment Summaries (ACTS)

POGO's policies and procedures outlines the criteria that must be considered by POGO's Senior Database Administrator, Senior Adviser, Policy and Clinical Affairs, Medical Director, and external content experts if applicable when determining whether to approve the collection of personal health information. The collection of this personal health information is governed by the data sharing agreements POGO has in place with its tertiary pediatric oncology hospital partners, AfterCare Adult 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 policies and procedures set out the criteria that must be considered by POGO's Senior Database Administrator, POGO's Senior Adviser, Policy and Clinical Affairs, and Medical

Director, and external content experts (if applicable) who are responsible for determining whether to approve the collection of personal health information to ensure that the collection is permitted under the *Act* and its regulation and that any and all conditions or restrictions set out in the *Act* and its regulation have been satisfied. The criteria also require POGO's Senior Database Administrator, POGO's Senior Adviser, Policy and Clinical Affairs, Medical Director, and external content experts if applicable when determining whether to approve the collection of personal health to ensure that other information, such as de-identified and/or aggregate information will serve the identified purpose such that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

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

Conditions or Restrictions on the Approval.

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

Secure Retention

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

Secure Transfer

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

Secure Return or Disposal

POGO's privacy policies and procedures identify POGO's Privacy 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 #9.2.9 (*Secure Transfer of Records of Personal Health Information*), and Policy #9.2.6 (*Retention, Return, Destruction of Data*).

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

5. List of Data Holdings Containing Personal Health Information

POGO maintains an up-to date list 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 the Privacy Officers are responsible for ensuring the process that must be followed in completing the statements of purpose for the data holdings containing personal health information, including the agent(s) or other organizations that must be consulted in completing the statements of purpose and the agent(s) responsible for approving the statements of purpose. The POGO Privacy Officer's role is to manage the Privacy Program and the process to be followed in respect of preparing, reviewing, and approving the statements of purpose for data holdings containing personal health information. The Privacy Program outlines that POGO's Senior Adviser, Policy and Clinical Affairs, and Medical Director together with the data holding Manager, in consultation with external agents where applicable, are consulted in reviewing and amending the statements of purpose and are responsible for approving the amended statements of purpose. Once finalized, the statement of purpose is reviewed and approved by POGO's Chief Executive Officer.

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

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

The Privacy 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, and prescribed registry from whom the personal health information in the data holding is collected.

Compliance with POGO's *Privacy and Security Policies and Procedures Manual* is mandatory for all agents of POGO and is monitored by POGO's Privacy 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 Policy #9.1.15 (*Privacy Audits*) that states that policies and procedures will be audited annually or sooner if required, and that the POGO Privacy Officers 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 #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

For each data holding containing personal health information, the 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 POGO access and use both the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual, or other responsibilities.

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

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

In this regard, POGO's policies and procedures explicitly prohibit access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose and prohibit access to or use of more personal health information than is reasonably necessary to meet the identified purpose.

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

Review and Approval Process

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

In outlining the process to be followed, the policy and procedures also set out the requirements to be satisfied in requesting, reviewing and determining whether to approve or deny a request by a 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, POGO's Senior Adviser, Policy and Clinical Affairs, and Medical Director for determining whether to approve or deny a request for access to and use of personal health information and, if the request is approved, the criteria that must be considered in determining the appropriate level of access. At a minimum, the Senior Database Administrator, the Senior Adviser, Policy and Clinical Affairs, and the Medical Director are responsible for determining whether to approve or deny the request and must be satisfied that:

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

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

Conditions or Restrictions on the Approval

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

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

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

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

Notification and Termination of Access and Use

Policy #9.1.6 (*Levels of Access*) states that an agent granted approval to access and use personal health information, as well as his or her supervisor, notify the POGO Privacy 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; 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 identify 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 #9.3.4 (*Termination or Cessation of the Employment or Contractual Relationship*).

Secure Retention

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

Secure Disposal

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

Tracking Approved Access to and Use of Personal Health Information

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

Compliance, Audit, and Enforcement

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

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

The purpose of the audit is to ensure that agents granted such approval continue to be employed or retained by POGO and continue to require access to the same amount and type of personal health information. In this regard, the policy and procedure identifies the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

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

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

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

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

POGO requires agents to comply with its policies and procedures and address how 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 #9.1.15 (*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 #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of the policy or its procedures.

Where the Use of Personal Health Information is Permitted for Research

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

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

POGO's *Privacy and Data Security Procedures and Policy #9.1.1 (Process for 44 and 45 Projects)* distinguishes between the use of personal health information for research purposes (section 44) and the use of personal health information for purposes of section 45 of the Act. The criteria that must be considered is outlined in *Policy #9.1.1 (Process for 44 and 45 Projects)* 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 #9.1.1 (*Process for 44 and 45 Projects*) identifies the Privacy Officers, the Senior Adviser, Policy and Clinical Affairs, and Medical Director as the agents responsible for receiving, reviewing, and determining whether to approve or deny a request for the use of personal health information for research purposes and the process that must be followed in this regard. This policy includes a discussion of the documentation that must be completed, provided and/or executed; the agents responsible for completing, providing and/or executing the documentation; the Privacy 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, the Senior Adviser, Policy and Clinical Affairs, 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, the Senior Adviser, Policy and Clinical Affairs, and Medical Director are responsible for determining whether to approve or deny the request to review the written research plan to ensure it complies with the requirements in the Act and its regulation, to ensure that the written research plan has been approved by a 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, Senior Adviser, Policy and Clinical Affairs, and Medical Director are responsible for determining whether to approve or deny the request and ensuring that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the Research Ethics Board. The Privacy Officers, Senior Adviser, Policy and Clinical Affairs, and Medical Director are also responsible for ensuring that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.

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

Conditions or Restrictions on the Approval

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

In addition, the Privacy 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* and Policy #9.2.6 (*Retention, Return and Destruction of Data*) 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, and in compliance with the policy and procedure for secure retention, return and destruction.

Secure Return or Disposal

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

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

If the records of personal health information are required to be disposed of in a secure manner, Policy #9.2.6 (*Retention, Return and Destruction of Data*) requires the records to be disposed of in accordance with this policy. The policy further stipulates the time frame following the retention period in the written research plan within which the records must be securely disposed of, 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 that the records of personal health information are securely disposed of including the date, time, location, and method of secure

disposal employed, and is required to bear the name and signature of the agent who performed the secure disposal.

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

Further, this policy identifies the Privacy 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 #9.1.1 (*Process for 44 and 45 Projects*) requires that a log is maintained of the approved uses of personal health information for research purposes and 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

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

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

Review and Approval Process

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

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

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

Conditions or Restrictions on the Approval

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

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

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

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

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

- The name of the research study;
- The name of the agent(s) to whom the approval was granted;
- The date of the decision of the 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 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;

- Whether the records of personal health information will be securely returned, securely disposed of or de-identified and retained following the retention period; and
- The date the records of personal health information were securely returned; the date, time, location and method of destruction (as per a certificate of destruction); or the date by which they must be returned or disposed of, if applicable; or the date, time and location that de-identification was completed (as per written confirmation).

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

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

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

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

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

Where the Disclosure of Personal Health Information is Permitted

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

Review and Approval Process

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

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

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

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

POGO's *Privacy and Data Security Code* and POGO's *Privacy and Data Security Procedures* require the Privacy Officers, Chief Adviser, Policy and Clinical Affairs, Medical Director and Chief Executive Officer who are responsible for determining whether to approve or deny the request are required to ensure that other information, namely de-identified and/or aggregate information will not serve the identified purpose of the disclosure and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

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

Conditions or Restrictions on the Approval

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

POGO's *Privacy and Security Policies and Procedures*, Policy #9.1.10 (*Execution of Data Sharing Agreements*) identify the Privacy 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*, and Policy #9.2.9 (*Secure Transfer of Records of PHI*) require records of personal health information to be transferred in a secure manner.

Secure Return or Disposal

Policy #9.2.6 (*Retention, Return, and Destruction of Data*) identifies the Privacy 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 #9.1.1 (*Process for 44 and 45 Projects*) address 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

Review and Approval Process

POGO permits de-identified and/or aggregate data to be disclosed for purposes other than research. POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*), and Policy #9.1.8 (*Disclosure of Personal Health Information for Purposes Other Than Research*) identify the Privacy Officers, the Senior Adviser, Policy and Clinical Affairs, and Medical Director as those responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure de-identified or aggregate information for purposes other than research and the process that must be followed in this regard. This includes a discussion of the documentation that must be completed, provided and/or executed; the agents or other 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.

The policy and procedures also address the requirements that must be satisfied and the criteria that must be considered by the Privacy Officers, Senior Adviser, Policy and Clinical Affairs, and

Medical Director responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for purposes other than research. At a minimum, POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) and Policy #9.1.8 (Disclosure of Personal Health Information for Purposes Other Than Research) require the de-identified and/or aggregate information to be reviewed prior to the disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The Privacy Officers, Senior Adviser, Policy and Clinical Affairs, and Medical Director are responsible for undertaking this review.

POGO's *Privacy and Data Security Procedures*, specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) and Policy #9.1.8 (Disclosure of Personal Health Information for Purposes Other Than Research) 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 Procedure*, specifically Principle 5 (*Limiting Use, Disclosure and Retention of Personal Health Information*) and Policy #9.1.8 (Disclosure of Personal Health Information for Purposes Other Than Research) identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for purposes other than research, including any documentation and/or agreements that must be completed, provided or executed, and the Privacy Officers or researcher responsible for completing, providing or executing the documentation and/or agreements.

At a minimum, POGO's Privacy Officers require the person or organization to which the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

POGO's *Privacy and Data Security Code*, and POGO's *Privacy and Data Security Procedures* and Policy #9.1.8 (Disclosure of Personal Health Information for Purposes Other Than Research) identify the Privacy Officers as responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of de-identified and/or aggregate information have been satisfied, including the execution of a written acknowledgment. Further, the policy and procedures require the Privacy Officers to track receipt of the executed written acknowledgements and set out the procedures that must be followed and the documentation that must be maintained in this regard.

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

POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45*

Projects), and Policy #9.1.9 (Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements) identify when, and under what circumstances, personal health information is permitted to be disclosed for research purposes (44 purposes).

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

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

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

Where the Disclosure of Personal Health Information is Permitted for Research

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

Review and Approval Process

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

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

At a minimum, the Privacy Officers, Senior Adviser, Policy and Clinical Affairs, and Medical Director who are responsible for determining whether to approve or deny the request for the disclosure of personal health information for research purposes must be in receipt of a written application, a written research plan, and a copy of the decision of the 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, the Senior Adviser, Policy and Clinical Affairs, and Medical Director who are responsible for determining whether to approve or deny the request are required to ensure that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board. The Privacy Officers, the Senior Adviser, Policy and Clinical Affairs, and Medical Director ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.

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

Conditions or Restrictions on the Approval

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

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

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

Secure Return or Disposal

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

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

Documentation Related to Approved Disclosures of Personal Health Information for Research

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

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

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

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

Review and Approval Process

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

For example, POGO's *Privacy and Data Security Procedures* and Policy #9.1.1 (*Process for 44 and 45 Projects*) address whether the prescribed person or prescribed entity requires the preparation of a written research plan in accordance with the Act and its regulation and/or required

research ethics board approval of the written research plan prior to the disclosure of de-identified and/or aggregate information for research purposes.

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

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

Conditions or Restrictions on the Approval

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

At a minimum, POGO's Privacy Officers require the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that they will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

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

14. Template Research Agreement

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

General Provisions

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

Purposes of Collection, Use and Disclosure

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

In particular, the Researcher Agreement clearly sets out that the researcher may only use the personal health information for the purposes set out in the written research plan approved by the 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 #9.2.9 (*Secure Transfer of Records of Personal Health Information*) implemented by POGO.

Secure Retention

The retention period for the records of personal health information subject to the Researcher Agreement and Privacy Impact Assessment also identify, 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 #9.2.9 (*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 POGO Privacy Officers.

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

If the records of personal health information are required to be disposed of in a secure manner, the Researcher Agreement provides a definition of secure disposal that is consistent with the *Act* and its regulation and identifies the precise manner in which the records of personal health information subject to the Researcher Agreement must be securely disposed of. The Researcher Agreement also stipulates the time frame following the retention period set out in the Researcher Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.

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

Further, the Researcher Agreement identifies the Privacy 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 #9.1.13 (*De-Identifying Personal Health Information*) implemented by POGO. The Researcher Agreement also requires that the researcher submit written confirmation that the records were de-identified, and the time frame following the retention period set out in the Researcher Agreement within which the written confirmation must be provided and the POGO Privacy Officers 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 #9.1.10 (*Execution of Data Sharing Agreements*) identifies the circumstances requiring the execution of a Data Sharing Agreement, the process that must be followed, and the requirements that must be satisfied prior to the execution of a Data Sharing Agreement.

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

The policy and procedure further identifies the Privacy 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 who are 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 are also responsible for ensuring that a Data Sharing Agreement is executed and must also be satisfied that the collection was approved in accordance with Principle 4 (*Limiting Collection*)

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

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

All agents of POGO must understand that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*) on an annual basis or as required, and that the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

17. Template Data Sharing Agreement

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

General Provisions

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

Purposes of Collection, Use and Disclosure

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

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

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

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

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

Secure Transfer

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

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

Secure Retention

The retention period for the records of personal health information subject to the Data Sharing Agreement is also specified in the Data Sharing Agreement. In identifying the relevant retention period, the Privacy 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 #9.2.6 (*Retention, Return, and Destruction*) implemented by POGO.

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

Secure Return or Disposal

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

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

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

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

Further, the Data Sharing Agreement sets out that the certificate of destruction must be provided to the Privacy 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 #9.1.11 (*Template for Agreement with Third Party Service Providers*) requires written agreements to be entered into with third party service providers prior to permitting third party service providers to access and use POGO personal health information. The policy requires the written agreements to contain the relevant language from the policy.

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

POGO requires third party service providers to comply with specific policies and procedures as outlined in each Third Party Service Agreement and set out how the Privacy Officers enforce compliance and the consequences of breach. Compliance will be audited in accordance with

principles within Policy #9.1.15 (*Privacy Audits*) specific to Third Parties and will be audited by the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*) if a third party service provider breaches or believes there may have been a breach of specific procedures and/or terms as set out in the agreement.

20. Template Agreement for All Third Party Service Providers

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

General Provisions

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

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

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 #9.2.9 (*Secure Transfer of Records of Personal Health Information*) implemented by POGO.

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

Secure Retention

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

The agreement further outlines the responsibilities of the third party service provider in securely retaining the records of personal health information. In identifying the secure manner in which the records of personal health information will be retained, and the methods by which the records of personal health information will be securely retained, the agreement shall have regard to Policy #9.2.6 (*Retention, Return, and Destruction of Data*) implemented by POGO.

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 #9.2.9 (*Secure Transfer of Records of Personal Health Information*) implemented by POGO.

If the records of personal health information are required to be disposed of in a secure manner, the agreement provides a definition of secure disposal that is consistent with the *Act* and its regulation and identifies the precise manner in which the records of personal health information are to be securely disposed 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 Policy #9.2.6 (*Retention, Return, and Destruction of Data*) implemented by POGO.

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

Secure Disposal as a Contracted Service

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

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

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

Implementation of Safeguards

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

Training of Agents of the Third Party Service Provider

The agreement requires the third party service provider to provide training to its agents on the importance of protecting the privacy of individuals whose personal health information is accessed

and used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations.

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

Subcontracting of the Services

Notification

At a minimum, the agreement requires the third party service provider to notify the POGO Privacy Officers at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if personal health information handled by the third party service provider on behalf of (POGO's Privacy Officers 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; and
- 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 #9.2.18 (*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 have regard to the sources of the records of personal health information that are requested to be linked, and the identity of the person or organization that will ultimately make use of the linked records of personal health information, including:

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

Review and Approval Process

The policy and procedures identify the Senior Database Administrator, and the Senior Adviser, Policy and Clinical Affairs, 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 agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the Senior Database Administrator to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also address the requirements that must be satisfied and the criteria that must be considered by the Senior Database Administrator, the Senior Adviser, Policy and Clinical Affairs, 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 person or organization, e.g. 45 entities or researcher), the policy and procedures require that the disclosure be approved pursuant to Policy #9.1.1 (*Process for 44 and 45 Projects*), and Policy #9.1.10 (*Execution of Data Sharing Agreements*).

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

Process for the Linkage of Records of Personal Health Information

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

Retention

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

Secure Disposal

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

Compliance, Audit and Enforcement

POGO requires agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

Tracking Approved Linkages of Records of Personal Health Information

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

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

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

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

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

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

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

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

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

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

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

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

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

POGO requires agents to comply with the policy and its procedures and sets out how the Privacy Officers will enforce compliance and the consequences of breach. The policy and procedures stipulate that compliance will be audited in accordance with Policy #9.1.15 (*Privacy Audits*) annually, and the audit will be conducted by the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*), if an agent breaches or believes there may have been a breach of this policy or its procedures.

25. Privacy Impact Assessment Policy and Procedures

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

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

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

The policy and procedures also set out the timing of privacy impact assessments. . With respect to proposed data holdings involving personal health information and new or changes to existing information systems, technologies or programs involving personal health information, the policy and procedures set out that privacy impact assessments be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage. With respect to existing data holdings involving personal health information, the policy and procedures set out a timetable to ensure privacy impact assessments are conducted, and the policy and procedures identify the Privacy 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 day-to-day authority to manage 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 #9.1.15 (*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 require agents to notify POGO at the first reasonable opportunity, in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

26. Log of Privacy Impact Assessments

POGO maintains a log of privacy impact assessments that have been completed and of privacy impact assessments that have been undertaken but that have not been completed. The log describes the data holding, information system, technology, or program involving personal health information that is at issue; the date that the privacy impact assessment was completed or is expected to be completed; the Privacy Team who are the agents responsible for completing or ensuring the completion of the privacy impact assessment; the recommendations arising from the privacy impact assessment; the Privacy 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 #9.1.15 (*Privacy Audits*) set out the types of privacy audits that are required to be conducted. At a minimum, the audits required to be conducted include audits to assess compliance with the privacy policies, procedures and practices implemented by POGO, and audits of the agent(s) permitted to access and use personal health information pursuant to POGO's *Privacy and Data Security Procedures*, Principle 5 (*Limiting Use, Disclosure, and Retention*).

With respect to each privacy audit that is required to be conducted, the policy and procedures set out the purposes of the privacy audit; the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections); the Privacy 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 to whom this documentation must be provided; and the required content of the documentation.

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

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

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

The policy and procedures further address the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of addressing the recommendations, are communicated. This includes a discussion of the Privacy 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 Chief Executive Officer.

The policy and procedures further require that a log be maintained of privacy audits and identifies the Privacy Team as the agents responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified time frame. They also set out that the documentation related to privacy audits is retained in POGO's secured central filing system, and that the Privacy 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 Chief Executive Officer and POGO's Medical Director at the first reasonable opportunity of a privacy breach or suspected privacy breach in accordance with the Policy #9.1.16 (*Privacy Breach and Incident Management*) and of an information security breach or suspected information security breach in accordance with the same policy.

28. Log of Privacy Audits

POGO maintains a log of privacy audits that have been completed. The log sets out the nature and type of the privacy audit conducted; the date that the privacy audit was completed; the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*) sets out the policy and procedures that address the identification, reporting, containment, notification, investigation, and remediation of privacy breaches.

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

- The collection, use, and disclosure of personal health information that is not in compliance with the *Act* or its regulation;
- A contravention of the privacy policies, procedures, or practices implemented by POGO;
- A contravention of Data Sharing Agreements, Research Agreements, Confidentiality Agreements, and Agreements with Third Party Service Providers retained by POGO; and

- Circumstances where personal health information is stolen, lost, or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification or disposal.

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

In this regard, the policy and procedures identify the Privacy 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 stipulate the time frame within which notification must be provided, that the notification must be provided verbally and in writing, and the nature of the information that must be provided upon notification. The policy and procedures also address the documentation that must be completed, provided and/or executed with respect to notification; the agent(s) responsible for completing, providing and/or executing the documentation; the Privacy 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 Chief Executive Officer. 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 directly notify the individual to whom the personal health information relates of a privacy breach. The required notification shall be provided by the health information custodian.

The policy and procedures also set out whether any other persons or organizations must be notified of the privacy breach and sets out the Privacy 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 day-to-day authority to manage the Privacy and Security Breach Programs.

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; and the agents to whom the documentation must be provided.

The policy and procedures also address the manner and format in which the findings of the investigation of the privacy breach, including the recommendations arising from the investigation

and the status of implementation of the recommendations, are communicated. This includes a discussion of the Privacy 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 Chief Executive Officer.

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

Further, the policy and procedures require that a log be maintained of privacy breaches and identify the Privacy Team as the agents responsible for maintaining the log and the Privacy 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 #9.1.15 (*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

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

- The date of the privacy breach;
- The date that the privacy breach was identified or suspected;
- Whether the privacy breach was internal or external
- The nature of the personal health information that was the subject matter of the privacy breach and the nature and extent of the privacy breach
- The date that the privacy breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to POGO was notified;
- The date that the investigation of the privacy breach was completed;
- The Privacy 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 require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken; advising the individual that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that POGO has contravened or is about to contravene the *Act* or its regulation; and providing contact information for the Information and Privacy Commissioner of Ontario.

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

The policy and procedures identify the Chief Executive Officer and Privacy 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, the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The Privacy Officers have been delegated day-to-day authority to manage the privacy program and the security program and are identified in the policy and procedures.

The process for addressing the recommendations arising from the investigation of privacy complaints and the Privacy Officers as the 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, the Privacy Officers to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures also address the manner and format in which the findings of the investigation of the privacy complaint, including recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This process includes a discussion of the Privacy 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 Chief Executive Officer.

The policy and procedures further require the individual making the privacy complaint to be notified, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint. The individual making the privacy complaint will be advised that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the *Act* or its regulation has been or is about to be contravened. The contact information for the Information and Privacy Commissioner of Ontario is also provided. The Privacy 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 Team as the agents responsible for maintaining the log and for tracking whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines. The process further addresses that the documentation related to the receipt, investigation, notification, and remediation of privacy complaints will be retained on POGO's secured central files by the Privacy 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 #9.1.15 (*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 #9.1.16 (*Privacy Breach and Incident Management*) is also addressed.

32. Log of Privacy Complaints

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

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

33. Policy and Procedures for Privacy Inquiries

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

The information that must be communicated to the public relating to the manner in which, to whom, and where individuals may direct privacy inquiries is also identified. At a minimum, the information communicated to the public includes the name and/or title, mailing address, and contact information of the Privacy 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 day-to-day authority to manage the privacy program and the security program and is also identified.

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

Part 2 – Security Documentation

1. Information Security Policy

POGO's Privacy Program, which includes the Security Program, is articulated in the following overarching information security documents: POGO's *Privacy and Data Security Code*, and POGO's *Privacy and Data Security Procedures (the Manual)* POGO's *Business Continuity and Disaster Recovery Plan*, POGO's *Corporate Risk Management Framework*, POGO's *Security Standards*, and POGO's *Privacy and Security Governance and Accountability Framework*. These documents have been implemented in relation to personal health information received by POGO under the Act. The Privacy Program as well as POGO Policy #9.2.3 (*Security Standards and Procedures*) 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 Policy #9.2.4 (*Threat and Risk Assessment*) require POGO to undertake comprehensive and organization-wide threat and risk assessments of all information security assets including personal health information, as well as appropriate project specific threat and risk assessments. Policy #9.2.4 (*Threat and Risk Assessment*) establishes and documents the methodology for identifying, assessing, and remediating threats and risks and for prioritizing all threats and risks identified for remedial action.

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

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

- A security program for the implementation of the information security program, including security training and awareness (i.e., Policy #9.2.3: *Security Standards and Procedures* and Policy #9.3.1: *Privacy and Security Training*);
- Policies and procedures for the ongoing review of the security policies, procedures, and practices implemented (i.e., Policy #9.1.2: *Review of Privacy and Security Policies and Procedures* and Policy #9.2.2: *Ongoing Review of Security Policies, Procedures and Practices*);
- Policies and procedures for ensuring the physical security of the premises (i.e., Policy #9.2.5: *Physical-Office Security*);
- Policies and procedures for the secure retention, transfer, and disposal of records of personal health information, including policies and procedures related to mobile devices, remote access and security of data at rest (i.e., Policy #9.2.6: *Retention, Return, and Destruction of Data*);
- Policies and procedures to establish access controls and authorization including business

requirements, user access management, user responsibilities, network access control, operating system access control, and application and information access control (i.e., Policy #9.2.3 *Security Standards and Procedures*, and Section 3.3 of the POGO Privacy Binder: *POGONIS Security Controls and Performance*);

- Policies and procedures for information systems acquisition, development, and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development, and support procedures and technical vulnerability management (i.e., Policy #9.2.3: *Security Standards and Procedures*);
- Policies and procedures for monitoring, including policies and procedures for maintaining and reviewing system control and audit logs and security audits (i.e., Policy #9.2.3: *Security Standards and Procedures*);
- Policies and procedures for network security management, including change and patch management (i.e., Policy #9.2.13: *Change Management*);
- Policies and procedures related to the acceptable use of information technology (i.e., Policy #9.2.15: *Acceptable Usage*);
- Policies and procedures for back-up and recovery (i.e., Policy #9.2.14: *Back-up and Recovery of Records of Personal Health Information* and Policy #9.2.3 *Security Standards and Procedures*);
- Policies and procedures for information security breach management (i.e., Policy 9.1.16 *Privacy Breach and Incident Management* and Policy #9.2.17: *Information Security Incident Management Process*); and
- Policies and procedures to establish protection against malicious and mobile code (i.e., Policy #9.2.3: *Security Standards and Procedures* and Policy #9.2.24: *Anti-Virus Spam*).

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

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

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

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

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

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

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

Policy #9.1.2 (*Review of Privacy and Security Policies and Procedures*) and Policy #9.2.2 (*Ongoing Review of Security Policies, Procedures and Practices*) indicate that the Privacy Officers and the IT Team will undertake the annual review and will complete it in no more than 6 months. These policies 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 #9.1.2 (*Review of Privacy and Security Policies and Procedures*) and Policy #9.2.2 (*Ongoing Review of Security Policies, Procedures and Practices*) indicate that the Privacy 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 applicable policy changes or additions that are able to be shared with its agents, and determining the method and nature of the communication.. The Privacy Officers ensure that any communication materials made available to the public and other stakeholders are reviewed and amended accordingly, the procedure for which is set out in the policy.

POGO requires agents to comply with the policy and its procedures which are enforced by POGO's Chief Executive Officer through the Privacy 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 and Security 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 Privacy Program and Policy #9.2.5 (*Physical-Office Security*) addresses the physical safeguards implemented by POGO to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

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

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

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

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

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

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

Policy, Procedures and Practices with Respect to Access by Agents

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

Policy #9.1.6 (*Levels of Access*) identifies the Privacy 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 #9.1.6 (*Levels of Access*). The Access Control Card Tracking Log is completed by the Privacy Team who are the agents to whom the documentation must be provided and includes the required content of the documentation.

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

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

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

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

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

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

Termination of the Employment, Contractual or Other Relationship

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

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

Notification When Access is No Longer Required

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

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

Audits of Agents with Access to the Premises

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

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

Policy, Procedures and Practices with Respect to Access by Visitors

POGO is a small organization and has determined it does not require a formal visitor tracking procedure. POGO's current procedure for authorizing and supervising visitors to the POGO premises is the responsibility of the POGO Receptionist/Administrative Assistant. This agent receives the visitor, notifies the staff member they are meeting, and either escorts the visitor to the staff members' 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 Privacy Program and Policy #9.2.6 (*Retention, Return, and Destruction of Data*), was developed and implemented with respect to the secure retention of records of personal health information in paper and electronic format.

This policy identifies the retention period for records of personal health information in both paper and electronic format, including various categories thereof. For records of personal health information used for research purposes, POGO 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 steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal. These steps that must be taken by agents are also outlined in the policy and procedures.

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

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

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

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

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

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

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

Officers as the agents responsible for conducting an annual audit and for ensuring compliance with the policy and its procedures.

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

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

Policy #9.2.7 (Personal Health Information on Mobile Devices), and Policy # 9.1.6 (*Levels of Access*) also 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:

Personal health information is stored on a mobile device 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 agents conducting analysis and reporting for POGO.

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

Approval Process

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

If approval is required, the policy and procedures identify the process that must be followed and the Privacy 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 require the Privacy Officers responsible for determining whether to approve or deny the request to ensure that the use of the personal health information has been approved pursuant to Policy #9.1.6 (*Levels of Access*), and Policy #9.2.7 (*Personal Health Information on Mobile Devices*).

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

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

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

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

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

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

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

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

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

Conditions or Restrictions on the Remote Access to Personal Health Information

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

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

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

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

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

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

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

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

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

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

POGO requires agents to comply with Policy # 9.2.9 (*Secure Transfer of Records of PHI*) and addresses how and by whom compliance will be enforced and the consequences of breach. This policy stipulates that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

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

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

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

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

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

- Identifying the records of personal health information to be securely disposed of;
- Confirming the secure disposal of the records of personal health information;
- Setting out the date, time and method of secure disposal employed; and
- Bearing the name and signature of the agent(s) who performed the secure disposal.

Policy #9.2.6 (*Retention, Return, and Destruction of Data*) sets out the time frame within which, and the Privacy 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 #9.2.19 (*Document Shredding*) and POGO's *Third Party Service Agreement* details the procedure to be followed by POGO in securely transferring the records of personal health information to the third party service provider for secure disposal. The policy and procedures identify the secure manner in which the records of personal health information will be transferred to the third party service provider, the conditions pursuant to which the records will be transferred and the agent(s) responsible for ensuring the secure transfer of the records. In this regard, the policy and procedures comply with Policy #9.2.19 (*Document Shredding*).

The policy and procedures also designates the Privacy 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 are created. 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 #9.1.11 (*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 #9.2.6 (*Retention, Return, and Destruction of Data*) and Policy #9.2.19 (*Document Shredding*) also outline the procedure to be followed in tracking the dates that records of personal health information are transferred for secure disposal and the dates that certificates of destruction are received, whether from the third party service provider or from the researcher that is not a third party service provider, and the Privacy Team who are the agents responsible for conducting such tracking. Further, the policy and procedures outline the process to be followed where a certificate of destruction is not received within the time set out in the policy and its procedures or within the time set out in the agreement with the third party service provider and the agents responsible for implementing this process.

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

POGO requires agents to comply with the policy and its procedures and 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 and Security 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 #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent or third party service provider breaches or believes there may have been a breach of these policies or their procedures.

9. Policy and Procedures Relating to Passwords

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

The policy and procedures identify the required minimum and maximum length of the password, the standard mandated for password composition and any other restrictions imposed on passwords, such as re-use of prior passwords and the use of passwords that resemble prior passwords. Further,

the policy stipulates that passwords must be comprised of a combination of upper and lower case letters as well as numbers and non-alphanumeric characters.

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

Policy #9.2.10 (*Password*) further identifies the administrative, technical and physical safeguards that must be implemented by agents in respect of passwords in order to ensure that the personal health information is protected against theft, loss and unauthorized use or disclosure and that the records of personal health information are protected against unauthorized copying, modification or disposal. Agents are required to keep their passwords private and secure and to change their passwords immediately if they suspect that their password has become known to any other individual, including another agent. Agents are also prohibited from writing down, displaying, 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 and Security 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 #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

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

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

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

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

The Privacy Officers and 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.

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

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

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

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

Further, POGO's Policy# 9.2.3 (*Security Standards and Procedures*) addresses the findings arising from the review of system control and audit logs, including the Privacy 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.

POGO's Policy# 9.2.3 (*Security Standards and Procedures*) also sets out the nature of the documentation, if any, that must be completed, provided and/or executed following the review of system control and audit logs; the IT Team who are responsible for completing, providing and/or

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

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program, sets out the frequency with which the policy and procedures will be audited and identifies the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

11. Policy and Procedures for Patch Management

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

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

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

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

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

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

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

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

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

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

12. Policy and Procedures Related to Change Management

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

This policy and its procedures identify the IT Team as responsible for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment and the process that must be followed and the requirements that must be satisfied in this regard. This includes a discussion of the documentation that must be completed, provided and/or executed; the IT Team that is responsible for completing, providing and/or executing the documentation; the Privacy 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 #9.2.13 (*Change Management*) also sets out the manner in which the decision approving or denying the request for a change to the operational environment and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Policy# 9.2.3 (*Security Standards and Procedures*) and POGO's Policy #9.2.14 (*Back-up and Recovery of Records of Personal Health Information*) requires agents to notify POGO at the first reasonable opportunity, in accordance with Policy #9.1.16 (*Privacy Breach and Incident*

Management) and Policy #9.2.17 (*Information Security Incident Management Process*), if an agent breaches or believes there may have been a breach of these policies or their procedures.

14. Policy and Procedures on the Acceptable Use of Technology

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

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

For those uses that are permitted only with prior approval, Policy #9.2.15 (*Acceptable Usage*) identifies the IT Team in consultation with the Privacy 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 IT Team and Privacy Officers for determining whether to approve or deny the request are also identified.

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

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

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

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

15. Policy and Procedures In Respect of Security Audits

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

With respect to each security audit POGO's Privacy and Security Audit Program sets out the purposes of the security audit; the nature and scope of the security audit; the IT Team that is responsible for conducting the security audit; and the frequency with which and the circumstances in which each security audit is required to be conducted. In this regard, POGO's Privacy and Security Audit Program requires a security audit schedule which identifies the IT Team and Privacy 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 the day-to-day authority to manage the Privacy and Security Audit Program, is identified. The IT Team has been delegated the day-to-day responsibility for completing, providing and/or executing the security audits.

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

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

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

POGO's Privacy and Security Audit Program also requires the IT Team who are responsible for conducting the security audit to notify POGO's Privacy Officers at the first reasonable opportunity, of an information security breach or suspected information security breach in accordance with

Policy #9.1.16 (*Privacy Breach and Incident Management*) or Policy #9.2.17 (*Information Security Incident Management Process*).

16. Log of Security Audits

POGO maintains a log of security audits that have been completed. The log sets out the nature and type of the security audit conducted; the date that the security audit was completed; the IT Team that is responsible for completing the security audit; the recommendations arising from the security audit; the IT Team in collaboration with the Privacy 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 Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) address the identification, reporting, containment, notification, investigation and remediation of information security breaches, and provides a definition of the term “information security breach”. At a minimum, an information security breach is defined as a contravention of the security policies, procedures or practices implemented by POGO.

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

In this regard, the policy identifies the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) require a determination to be made of whether an information security breach has in fact occurred, and if so, what if any personal health information has been breached. A determination is further made of the extent of the information security breach and whether the breach is an information security breach or privacy breach or both. The Privacy 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 Chief Executive Officer 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 breaches 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. POGO Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) also address any documentation that must be completed, provided and/or executed by the Privacy 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, POGO Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) 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

POGO Policy #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.2.17 (*Information Security Incident Management Process*) further identify 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 day-to-day authority to manage the Privacy 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.

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

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

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

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

The Privacy 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 agents responsible for providing notification to the Privacy Officers, the time frame within which notification must be provided, and the format of the notification.

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

- A description of the status of POGO under the *Act* and the duties and responsibilities that arise as a result of this status;
- A description of the nature of the personal health information collected and from whom this information is typically collected;
- An explanation of the purposes for which personal health information is collected and used and how this collection and use is permitted by the *Act* and its regulation;
- Limitations placed on access to and use of personal health information by agents;
- A description of the procedure that must be followed in the event that an agent is requested to disclose personal health information;
- An overview of the privacy policies, procedures, and practices that have been implemented by POGO, and the obligations arising from these policies, procedures, and practices;
- The consequences of breach of the privacy policies, procedures, and practices implemented;
- An explanation of the privacy program, including the key activities of the program and an explanation that the Privacy 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 the Privacy Team in implementing the administrative, technical, and physical safeguards put in place by POGO;
- A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute and the key provisions of the Confidentiality Agreement; and
- An explanation of Policy #9.1.16 (*Privacy Breach and Incident Management*) and the duties and responsibilities imposed on agents in identifying, reporting, containing, and participating in the investigation and remediation of privacy breaches.

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

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

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

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

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

POGO requires agents to comply with the policy and its procedures and sets out that compliance will be enforced by the Privacy Officers, and also sets out the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program as well as Policy #9.1.15 (*Privacy Audits*) and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy 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 #9.1.16 (Privacy Breach and Incident Management) if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

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

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

3. Policy and Procedures for Security Training and Awareness

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

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

The Privacy 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 the Privacy Team together with the IT Team in implementing the administrative, technical, and physical safeguards put in place by POGO; and

- An explanation of Policy #9.1.16 (*Privacy Breach and Incident Management*) and the duties and responsibilities imposed on agents in identifying, reporting, containing, and participating in the investigation and remediation of information security breaches.

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

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

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

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

The policy and procedures also discuss the other mechanisms implemented by POGO to raise awareness of the security program and the security policies, procedures, and practices implemented. The policy and procedures also discuss the frequency with which POGO communicates with its agents in relation to information security, the method and nature of the communication, and the Privacy 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 POGO's Privacy and Security Audit Program as well as Policy #9.2.16 (*Security Audits*), and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy Officers together with the IT Team as the agents responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

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

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

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

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

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

In particular, the policy and procedures outline the process that must be followed in notifying the Privacy 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 scanned and stored electronically in POGO's secured central files and in 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 breaches. The policy and procedures also stipulate that compliance with the policy and its procedures and with the Confidentiality Agreement will be audited in accordance with POGO's Privacy and Audit Program which sets out

the frequency with which the policy and its procedures will be audited and identifies the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

6. Template Confidentiality Agreement with Agents

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

General Provisions

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

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

Agents are also required to acknowledge that they have read, understood, and agree to comply with the privacy and security policies, procedures, and practices implemented by POGO and to comply with any privacy and security policies, procedures, and practices as may be implemented or amended from time to time following the execution of the Confidentiality and Non-Disclosure Agreement.

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

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

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

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

Further, the Confidentiality and Non-Disclosure Agreement prohibits agents from collecting, using, or disclosing personal health information if other information will serve the purpose and

from collecting, using, or disclosing more personal health information than is reasonably necessary to meet the purpose.

Termination of the Contractual, Employment or Other Relationship

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

Notification

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

Consequences of Breach and Monitoring Compliance

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

7. Log of Executed Confidentiality Agreements with Agents

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

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

Policy #9.3.3 (*Delegation of Roles and Responsibilities*) provides a job description for the position of Privacy 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 Chief Executive Officer. 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 (the Manual)*- Principle #10 (*Challenging Compliance*), and POGO Privacy Program, Section 7 (*Privacy Inquires, Challenges, and Complaints*);
- Receiving and responding to privacy inquiries pursuant to the Section 7 (*Privacy Inquires, Challenges, and Complaints*);
- Receiving, documenting, tracking, investigating, and remediating privacy breaches or suspected privacy breaches pursuant to Policy #9.1.16 (*Privacy Breach and Incident Management*); and
- Conducting privacy audits pursuant to Policy #9.2.16 (*Security Audits*).

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

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

The job description sets out the reporting relationship of the Privacy Officers who have been delegated day-to-day authority to manage the security program by the Chief Executive Officer. The job description identifies the responsibilities and obligations of the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*); and

- Conducting security audits pursuant to POGO's Privacy and Security Audit Program together with the IT Team.

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

Policy #9.3.4 (*Termination or Cessation of employment of Contract*) requires agents, as well as their supervisors, to notify POGO of the termination of any employment, contractual, or other relationship. The policy and procedures identify the Privacy Team to whom notification must be provided, the nature and format of the notification, the time frame within which notification must be provided, and the process that must be followed in providing notification.

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

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

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

POGO requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulate that compliance will be audited in accordance with POGO's Privacy and Security Audit Program and sets out the frequency with which the policy and procedures will be audited and identifies the Privacy 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 #9.1.16 (*Privacy Breach and Incident Management*) and Policy #9.3.6 (*Disciplinary Action – Privacy Breach*) if an agent breaches or believes there may have been a breach of this policy or its procedures.

11. Policy and Procedures for Discipline and Corrective Action

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

POGO Policy #9.3.6 (*Disciplinary Action – Privacy Breach*) addresses the investigation of disciplinary matters, including the Privacy 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 Privacy Officers, the agent's Manager, and POGO's Chief Executive Officer to whom the results of the investigation must be reported.

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

Part 4 – Organizational and Other Documentation

1. Privacy and Security Governance and Accountability Framework

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

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

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

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

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

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

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

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

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

3. Corporate Risk Management Framework

POGO has in place a comprehensive and integrated Corporate Risk Management Framework to identify, assess, mitigate, and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received, and to maintain the confidentiality of that information.

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

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

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

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

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

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

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

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

4. Corporate Risk Register

POGO has developed and maintains a corporate risk register that identifies each risk that may negatively affect the ability of POGO to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. For each risk identified, the corporate risk register includes an assessment of the risk, a ranking of the risk, the mitigation strategy to reduce the likelihood of the risk occurring and/or to reduce the impact of the risk if it does occur, the date that the mitigation strategy was implemented or is required to be implemented, and the agent(s) responsible for implementation of the mitigation strategy.

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

POGO has developed and implemented Policy 9.4.6 (*Consolidated Log of Recommendations*) and associated procedures requiring a consolidated and centralized log to be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits, and the investigation of privacy breaches, privacy complaints, and security breaches. The consolidated and

centralized log includes recommendations made by the Information and Privacy Commissioner of Ontario to be addressed by POGO prior to the next review of its practices and procedures.

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

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

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

6. Consolidated Log of Recommendations

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

In particular, the log sets out the name and date of the document, investigation, audit and/or review from which the recommendation arose. For each recommendation, the log sets out the recommendation made, the manner in which the recommendation was addressed or is proposed to be addressed, the date that the recommendation was addressed or by which it is required to be addressed, and the agent(s) responsible for addressing the recommendation.

7. Business Continuity and Disaster Recovery Plan

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

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

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

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

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

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

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

The Business Continuity and Disaster Recovery Plan also identifies the agent(s) responsible for resumption and recovery, the procedure that must be utilized in resumption and recovery for each critical application and business function, the prioritization of resumption and recovery activities, the criteria pursuant to which the prioritization of resumption and recovery activities is determined,

and the recovery time objectives for critical applications. This includes a discussion of the agents and other persons or organizations that are required to be consulted with respect to resumption and recovery activities; the documentation that must be completed, provided and/or executed; the required content of the documentation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of these activities must be communicated.

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

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

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

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

Appendix 1: Privacy, Security, and Other Indicators

Part 1 – Privacy Indicators

Categories	Privacy Indicators	POGO-IPC Review (2016)	
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.	Date	Policies Reviewed
		October 2013	9.3.2; 9.3.3; 9.3.4; 9.3.6; 9.4.1; 9.4.3; 9.4.4; 9.4.5; 9.4.6; 9.4.7; 9.4.20; 9.4.12; 9.
		February 2014	9.3.1.
		March 2014	9.1.23; 9.3.18.
		July 2014	9.1.13; 9.1.19; 9.1.22.
		September 2014	9.1.1; 9.1.2; 9.1.3; 9.1.4; 9.1.5; 9.1.6; 9.1.7; 9.1.8; 9.1.9; 9.1.10; 9.1.11; 9.1.12; 9.1.15; 9.1.17; 9.1.18.
		October 2014	9.1.14; 9.1.16; 9.1.21; 9.1.20.
		January 2015	9.1.1, 9.1.3; 9.1.4; 9.1.5; 9.1.6; 9.1.7; 9.1.8;9.1.9, 9.1.10, 9.1.11; 9.1.12; 9.1.13; 9.1.14; 9.1.15; 9.1.16; 9.1.17; 9.1.18; 9.1.19, 9.1.20, 9.1.21; 9.1.22, 9.1.23, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.6, 9.3.18, 9.4.1, 9.4.3, 9.4.4, 9.4.5, 9.4.6, 9.4.7, 9.4.10; 9.4.12
		July 2015	9.1.2; 9.1.3; 9.1.15; 9.1.21.
		October 2015	9.3.18, 9.4.7; 9.4.12.
		January 2016	9.1.1, 9.1.2; 9.1.3; 9.1.4; 9.1.5; 9.1.6; 9.1.7; 9.1.8; 9.1.9; 9.1.10; 9.1.11; 9.1.12; 9.1.13; 9.1.14; 9.1.15; 9.1.16; 9.1.17; 9.1.18; 9.1.19; 9.1.20; 9.1.21; 9.1.22; 9.1.23, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.6, 9.3.18, 9.4.1, 9.4.3, 9.4.4, 9.4.5, 9.4.6, 9.4.7, 9.4.10.
		February 2016	9.1.16; 9.1.21, 9.3.6.
		April 2016	9.1.1,9.1.2; 9.1.23, 9.3.1, 9.3.2, 9.3.3,9.3.18, 9.4.1, 9.4.3, 9.4.4, 9.4.5, 9.4.6, 9.4.7, 9.4.10

Appendix 1: Privacy, Security, and Other Indicators

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.	<table><tr><th>Policy #</th><th>Policy Subject</th><th>If yes, reason for and nature of amendments made</th></tr><tr><td>9.1.16</td><td>Breaches</td><td>Updated definitions – External and Internal breaches</td></tr></table>		Policy #	Policy Subject	If yes, reason for and nature of amendments made	9.1.16	Breaches	Updated definitions – External and Internal breaches				
	Policy #	Policy Subject	If yes, reason for and nature of amendments made									
	9.1.16	Breaches	Updated definitions – External and Internal breaches									
	No other amendments were made to existing privacy policies and procedures as a result of the review.											
- 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. - A Business Continuity and Disaster Recovery Plan and its associated policies: #9.4.7 Business Continuity and Disaster Recovery Plan October 2015 and #9.4.12 BCDR Plan Essential Services October 2015 were further developed and implemented as a result of the 2013 review. This policy includes: - The purpose of the BCDR Plan - The nature and scope of the BCDR Plan - The individuals responsible for: updating and testing the Plan; notifying POGO agents and external stakeholders of interruption; maintaining contact lists; assessing level of severity, completing necessary document, and disseminating appropriately; conducting impact assessments; conducting damage assessment; resumption and recovery procedures and implementation; and for taking inventory of all business functions and office equipment, and IT specifications - The frequency with which testing and maintenance are to be completed.												
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.	<table><tr><th>Date</th><th>Nature of Communication</th></tr><tr><td>24 January 2014</td><td>Communication of amendments to Privacy and Security policies and the need for BCDR at Board of Directors meeting. Amendments communicated for the following privacy policies: 9.1.1, 9.1.2; 9.1.3; 9.1.4; 9.1.5; 9.1.6; 9.1.7; 9.1.8; 9.1.9; 9.1.10; 9.1.11; 9.1.12; 9.1.13; 9.1.14; 9.1.15; 9.1.16; 9.1.17; 9.1.18; 9.1.19; 9.1.20; 9.1.21.</td></tr><tr><td>21 February 2014</td><td>E-mail communication to staff regarding newly created Code of Conduct, Policy 9.3.8. All POGO staff asked to review and sign.</td></tr><tr><td>14 March 2014</td><td>Presentation to Interlink Nurses and Social Workers highlighting new privacy policies and procedures. Amendments communicated for the following privacy policies: 9.1.4, 9.1.5, 9.1.16, 9.1.2, 9.1.22, 9.2.23.</td></tr><tr><td>6 June 2014</td><td>POGO Privacy Newsletter distributed to POGO staff and agents which included highlighting of new policies and procedures.</td></tr></table>		Date	Nature of Communication	24 January 2014	Communication of amendments to Privacy and Security policies and the need for BCDR at Board of Directors meeting. Amendments communicated for the following privacy policies: 9.1.1, 9.1.2; 9.1.3; 9.1.4; 9.1.5; 9.1.6; 9.1.7; 9.1.8; 9.1.9; 9.1.10; 9.1.11; 9.1.12; 9.1.13; 9.1.14; 9.1.15; 9.1.16; 9.1.17; 9.1.18; 9.1.19; 9.1.20; 9.1.21.	21 February 2014	E-mail communication to staff regarding newly created Code of Conduct, Policy 9.3.8. All POGO staff asked to review and sign.	14 March 2014	Presentation to Interlink Nurses and Social Workers highlighting new privacy policies and procedures. Amendments communicated for the following privacy policies: 9.1.4, 9.1.5, 9.1.16, 9.1.2, 9.1.22, 9.2.23.	6 June 2014	POGO Privacy Newsletter distributed to POGO staff and agents which included highlighting of new policies and procedures.
	Date	Nature of Communication										
	24 January 2014	Communication of amendments to Privacy and Security policies and the need for BCDR at Board of Directors meeting. Amendments communicated for the following privacy policies: 9.1.1, 9.1.2; 9.1.3; 9.1.4; 9.1.5; 9.1.6; 9.1.7; 9.1.8; 9.1.9; 9.1.10; 9.1.11; 9.1.12; 9.1.13; 9.1.14; 9.1.15; 9.1.16; 9.1.17; 9.1.18; 9.1.19; 9.1.20; 9.1.21.										
	21 February 2014	E-mail communication to staff regarding newly created Code of Conduct, Policy 9.3.8. All POGO staff asked to review and sign.										
	14 March 2014	Presentation to Interlink Nurses and Social Workers highlighting new privacy policies and procedures. Amendments communicated for the following privacy policies: 9.1.4, 9.1.5, 9.1.16, 9.1.2, 9.1.22, 9.2.23.										
6 June 2014	POGO Privacy Newsletter distributed to POGO staff and agents which included highlighting of new policies and procedures.											

Appendix 1: Privacy, Security, and Other Indicators

		20 January 2015	Amendments to policies made throughout 2014 communicated to staff at a regularly scheduled staff meeting. Amendments communicated for the following privacy policies: 9.1.22, 9.1.23.
		30 January 2015	Directors updated on amendments made to Privacy policies and procedures at a regularly scheduled Board of Directors meeting. Amendments communicated for the following privacy policies: 9.1.22, 9.1.23
		4 February 2015	E-mail communication sent to Interlink Nurses regarding updates to privacy policies and procedures. Amendments communicated for the following privacy policies: 9.2.7.
		8 April 2015	Interlink Nurses privacy training to update on amendments made specific to Interlink practices. Amendments communicated for the following privacy policies: 9.1.21, 9.1.22,
		16 June 2015	Amendments to policies communicated to staff at a regularly scheduled staff meeting Amendments communicated for the following privacy policies: 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.11, 9.1.12, 9.1.13, 9.1.14, 9.1.15, 9.1.16, 9.1.17, 9.1.18, 9.1.21, 9.1.22
		30 September 2015	Directors asked to sign Confidentiality agreements as per policy 9.3.2 and conducted a Board Risk Assessment Exercise at Board of Directors Annual General Meeting as per policies 9.4.4 and 9.4.5
		17 November 2015	The roll out of the BCDR Plan, its use, and testing measures with BCDR Planning, Executive Control and Business Resumption teams as per policies 9.4.4, 9.4.5, 9.4.6, 9.4.7, 9.4.12.
		29 January 2016 and 21 March 2016	BCDR training for Tier 1 staff and Board of Directors as per policies 9.4.7 and 9.4.12; Discussed POGO Risk Assessment-Survey results, Annual Privacy Report and BCDR shared at Board of Directors meetings;
		9 February 2016	BCDR training for Tier 2 staff as per policies 9.4.7 and 9.4.12.
		16 February 2016 and 21 March 2016	BCDR training for Tier 3 staff as per policies 9.4.7 and 9.4.12.
		6 April 2016	Presentation regarding amendments to policies and procedures for SAVTI counsellors. Amendments communicated for the following privacy policies: 9.1.4, 9.1.7, 9.1.8, 9.1.10, 9.1.14, 9.1.16, 9.1.23
	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.	- POGO Privacy and Data Security Code updated and made available on POGO website in January 2014, following IPC review. - POGO Privacy and Data Security Code updated in September 2016 to include the BCDR Plan in Principle 7.3 Safeguards.	

Appendix 1: Privacy, Security, and Other Indicators

Collection	The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.	5 data holdings: - POGONIS (Pediatric Oncology Group of Ontario Networked Information System); - POFAP (Pediatric Oncology Financial Assistance Program) Database; - Interlink Community Cancer Nurses Database; - SAVTI (Successful Academic Vocational Transition Initiative (SAVTI) database; and - ACTS (After Care Treatment Summary) Database. The ACTS database (new) was created in 2014, and a new statement of purpose was created. The AfterCare Treatment Summary (ACTS) database was added in 2014. This database was added as a recommendation from the Institute of Medicine and supported by the pediatric community addressing the need to provide survivors of childhood cancer and their primary care physicians with specific, individual, detailed survivor care plans containing recommendations for their care in light of the many late effects of treatment that survivors may develop. Patient specific diagnosis and treatment data from POGONIS is exported to ACTS application. This data is used to develop the individual survivor care plans that are disclosed by physicians to the patient at POGO’s AfterCare programs.
	The number of statements of purpose developed for data holdings containing personal health information.	Each of the 5 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.	5 statements of purpose for the data holdings have been reviewed annually since the last IPC review (2013). - POGONIS (Pediatric Oncology Group of Ontario Networked Information System); - POFAP (Pediatric Oncology Financial Assistance Program) Database; - Interlink Community Cancer Nurses Database; - SAVTI (Successful Academic Vocational Transition Initiative (SAVTI) database; and - ACTS (After Care Treatment Summary) Database.
	Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the	No statements of purpose have been amended as a result of the review.

Appendix 1: Privacy, Security, and Other Indicators

	review, and a list of the amended statements of purpose and, for each statement of purpose amended, brief description of the amendments made.	
Use	▪ The number of agents granted approval to access and use personal health information for purposes other than research.	▪ POGO staff: 10 in 2014, 9 in 2015, 10 in 2016 ▪ 7 Data Managers for each year and 1 data clerk (starting in 2015) ▪ 2 Artificial Intelligence in Medicine, Inc. (AIM) staff for each year ▪ 20 Atlas authors/collaborators in 2014. Project completed and published January 2015. (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) ▪ 2 for Atlas projects (1 from ICES for the Atlas project, 1 from CCO) in 2014. ▪ 1 from CCO for enhanced death clearance in 2015. ▪ 10 (1 analyst and 1 physician lead per 5 pediatric tertiary sites) for the <i>Impact of Post-Transplant Care on Referring Centres</i> initiative. Data analyzed in 2014, presented in 2015. ▪ 32 users of ACTS data granted in 2015.
	▪ The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy Commissioner of Ontario.	Total: 33 ▪ 15 requests have been received. ▪ 14 ICES requests. ▪ 4 CYP-C.
	▪ 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.	Total: 33 ▪ 15 requests have been received. ▪ 14 ICES requests. ▪ 4 CYP-C. ▪ No requests have been denied.

Appendix 1: Privacy, Security, and Other Indicators

Disclosure	The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario.	Total: 56 20 Atlas authors/collaborators in 2014. Project completed and published January 2015. (Atlas authors/collaborators are agents of POGO, thus this is a use of PHI and a disclosure of aggregate data 2 for Atlas projects (1 from ICES for the Atlas project, 1 from CCO) in 2014. 1 request in 2014. <i>Impact of Post-Transplant Care on Referring Centres</i>. 32 individual users of ACTS data (beginning in 2015) for clinical use. POGO logs access to ACTS server by users but unable to log disclosure made at the institution level. 1 from CCO for enhanced death clearance in 2015.
	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.	56 were granted. None were denied.
	The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario.	15 requests have been received. None were denied.
	The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the Information	10 Research Agreements have been executed for the 15 requests (4 Research Agreements were executed prior to the prior review. 1 project contains two disclosure requests for the same project with only one Research Agreement executed for the project). - For ICES and CYP-C research projects no research agreements are executed by POGO as per blanket data sharing agreements. POGO executes project permissions with the centres with accompanying approval and documentation.

Appendix 1: Privacy, Security, and Other Indicators

	Privacy Commissioner of Ontario.	
	▪ 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.	▪ 75 requests received for other 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 for other purposes, as agreements are not required for aggregate data requests. ▪ There were 355 agents who used aggregate data and who sign a confidentiality agreement annually for 45 purposes. ▪ There were 30 agents (POGO staff and Atlas authors) who used de-identified data and signed a confidentiality agreement annually for 45 purposes. ▪ POGO is currently undertaking a Provincial Pediatric Oncology Planning exercise where de-identified data will be disclosed to working group members if required. Members will sign confidentiality agreements. At this point, we have yet to release any de-identified data to working group members but we will log as per our policies and procedures and provide to IPC if requested. Planning exercise is projected to be completed in March 2017.
Data Sharing Agreements	▪ The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	▪ No Data Sharing Agreements have been executed for the purposes of collection <i>since</i> the last review by the IPC. There have been 7 amendments to Data Sharing Agreements executed for the collection of personal health information since the prior review: - o 5 tertiary centres ▪ The Hospital for Sick Children, Toronto. Amendment executed 2 April 2014 ▪ Children’s Hospital, London Health Sciences Centre. Amendments executed 16 December 2013 and 6 March 2014. ▪ McMaster Children’s Hospital, Hamilton Health Sciences. Amendment executed 18 December 2013 ▪ Kingston General Hospital. Amendment executed 24 January 2014. ▪ Children’s Hospital of Eastern Ontario, Ottawa. Amendment executed 16 December 2013.1 - o After Care Clinic (Princess Margaret Cancer Centre), Amendment executed 30 April 2014 - o Cancer Care Ontario. Amendments executed 9 April 2014 and 28 January 2015.

Appendix 1: Privacy, Security, and Other Indicators

	▪ The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario	▪ There are 2 Data Sharing Agreements that have been executed for the disclosure of personal health information since the last review by the IPC: - o Institute for Clinical Evaluative Science (ICES). Amendments executed 12 December 2013 and 28 April 2015. - o Cancer in Young People in Canada (CYP-C)-Public Health Agency of Canada. Data Sharing Agreement executed 2 January 2014. ▪ 7 amendments to Data Sharing Agreements have been executed for the purposes of disclosure <i>since</i> the last review by the IPC: - o 5 tertiary centres ▪ The Hospital for Sick Children, Toronto. Amendment executed 2 April 2014 ▪ Children’s Hospital, London Health Sciences Centre. Amendments executed 16 December 2013 and 6 March 2014. ▪ McMaster Children’s Hospital, Hamilton Health Sciences. Amendment executed 18 December 2013 ▪ Kingston General Hospital. Amendment executed 24 January 2014. ▪ Children’s Hospital of Eastern Ontario, Ottawa. Amendment executed 16 December 2013.1 - o After Care Clinic (Princess Margaret Cancer Centre), Amendment executed 30 April 2014 - o Cancer Care Ontario. Amendments executed 9 April 2014 and 28 January 2015.
Agreements with Third Party Service Providers	▪ The number of agreements executed with third party service providers with access to personal health information since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 1: - o 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.	▪ 33 (Based on numbers below): - o (2) ICES- Institute for Clinical Evaluative Science (yearly); - o (30) CCO-Cancer Care Ontario; CCO-PET monthly linkage since May 2014; - o (1) CCO Exchange Data (Death Clearance and Second Cancers) December 2015.

Appendix 1: Privacy, Security, and Other Indicators

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.	70 privacy impact assessments have been completed since the previous review. For details of PIAs please see appendix 1: PIA					
			Agent (Data Holding)	Date Completed PIA	Description of Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed
			[REDACTED] (POGONIS, Research)	14-Nov-13	No recommendations for 2013		
				3-Dec-14	No recommendations for 2014		
				4-Mar-15	Complete Acceptable Usage Form to access Level xx IT resources	25-Mar-15	As per Policy #9.2.15 completed Acceptable Usage Form.
				16-Sep-16	No recommendations		
			[REDACTED] (Atlas Project)	14-Nov-13	No recommendations for 2013		
				3-Dec-14	No recommendations for 2014		
				17-Mar-15	Complete Acceptable Usage Form De-identified record level data is currently transferred outside of the POGONIS room via encrypted iron key	31-Mar-15	As per Policy #9.2.15 completed Acceptable Usage Form. As per Policy #9.2.9 De-identified record level data transferred outside of the POGONIS room will be transferred via Iron Key.
			[REDACTED] (Clinical Programs; Satellite, AfterCare, ACTS)	14-Nov-13	No recommendations for 2013		
				3-Dec-14	No recommendations for 2014		
				17-Mar-15	Complete Acceptable Usage Form. Include FTP as secure method of transferring PHI with Satellite centres	24-Mar-15	As per Policy #9.2.15 completed Acceptable Usage Form. FTP user account set- up by System and Network Analyst and implemented as per Policy #9.2.9 procedures.
				1-Oct-16	No recommendations		

Appendix 1: Privacy, Security, and Other Indicators

		██████ (Research, Clinical Programs: Satellite, AfterCare, POGONIS, Atlas)	7-Nov-13	No recommendations for 2013			
			3-Dec-14	No recommendations for 2014			
			8-Jun-15	Complete Acceptable Usage Form. De-identified record level data is currently transferred outside of the POGONIS room via encrypted Ironkey. Include FTP as secure method of transferring PHI with Tertiary and Satellite centres and other agents	8-Jun-15	As per Policy #9.2.15 completed Acceptable Usage Form. De-identified record level data transferred outside of the POGONIS room will be transferred via IronKey. FTP user account set- up by System and Network Analyst and implemented as per Policy #9.2.9 procedures.	
			1-Oct-16	No recommendations			
		██████ (Administration : Senior Adviser, Policy & Clinical Affairs, Corporate)	14-Nov-13	No recommendations for 2013			
			3-Dec-14	No recommendations for 2014			
			29-Jun-15	Complete Acceptable Usage Form. Include FTP as secure method of transferring PHI with Tertiary centres and MOH EAP of the Ontario Public Drug Program	24-Mar-15	As per Policy #9.2.15 completed Acceptable Usage Form. FTP user account set- up by System and Network Analyst and implemented as per Policy #9.2.9 procedures.	
			18-Oct-16	No recommendations			
		██████ (POGONIS)	21-Nov-13	No recommendations for 2013			
			24-Nov-14	No recommendations for 2014			
			29-Sep-15	Complete Acceptable Usage Form	29-Sep-15	As per Policy #9.2.15 completed Acceptable Usage Form.	

Appendix 1: Privacy, Security, and Other Indicators

			30-Sep-16	No recommendations			
		(IT, POGONIS, POFAP, SAVTI, Interlink, ACTS)	3-Dec-13	No recommendation for 2013			
			24-Nov-14	No recommendation for 2014			
			27-Mar-15	Complete Acceptable Usage Form to include all Level 0 IT resources.	30-Mar-15	As per Policy #9.2.15 completed Acceptable Usage Form.	
			12-Sep-16	No recommendations			
		(Clinical Programs: Satellite, AfterCare, POGONIS, Atlas)	21-Dec-13	No recommendation for 2013			
			4-Mar-14	No recommendation for 2014			
			24-Jul-15	Complete Acceptable Usage Form to include all Level 0 IT resources.	24-Jul-15	As per Policy #9.2.15 completed Acceptable Usage Form.	
			1-Sep-16	No recommendations			
		Medical Director/Research	18-Dec-13	No recommendation for 2013			
			6-Nov-14	No recommendation for 2014			
			24-Sep-15	Complete Acceptable Usage Form to include all Level 0 IT resources.	24-Sep-15	As per Policy #9.2.15 completed Acceptable Usage Form.	
			18-Oct-16	No recommendations for 2016			
		(IT, POGONIS, POFAP, SAVTI, Interlink, ACTS)	21-Dec-13	No recommendations for 2013			
			4-Mar-14	No recommendations for 2014			
			2-Jun-15	Complete Acceptable Usage Form to	2-Jun-15	As per Policy #9.2.15 completed Acceptable Usage Form.	

Appendix 1: Privacy, Security, and Other Indicators

				include access to Level 0 IT Resources.			
			1-Sep-16	No recommendations			
		(IT, POGONIS, POFAP, SAVTI, Interlink, ACTS)	15-Jan-13	No recommendations for 2013			
			29-Jan-14	No recommendations for 2014			
			23-Mar-15	Complete Acceptable Usage Form to include access to all Level 0 IT Resources.	25-Mar-15	As per Policy #9.2.15 completed Acceptable Usage Form.	
			1-Sep-16	No recommendations			
		(POGONIS, Research)	19-Dec-13	No recommendations for 2013			
			27-Nov-14	No recommendations for 2014			
			13-Apr-15	Complete Acceptable Usage Form to include access to Level 1 IT Resources.	13-Apr-15	As per Policy #9.2.15 completed Acceptable Usage Form.	
			1-Sep-16	No recommendations			
		(POFAP)	20-Nov-13	No recommendations for 2013			
			27-Nov-14	No recommendations for 2014			
			17 -Mar-15 (POFAP), and 15-Mar-15 (SAVTI)	Complete Acceptable Usage Form to include access to Level 2 IT Resources.	24-Mar-15	As per Policy #9.2.15 completed Acceptable Usage Form.	
			Retired - Oct 16 Sep 16	No recommendations			
		(POGONIS)	21-Nov-13	No recommendations for 2013			
			24-Nov-14	No recommendations for 2014			

Appendix 1: Privacy, Security, and Other Indicators

			4-Jun-15	Complete Acceptable Usage Form to include access for all Level 1 IT resources.	4-Jun-15	As per Policy #9.2.15 completed Acceptable Usage Form.	
			21-Oct-16	No recommendations			
		██████████ (SAVTI)	21-Nov-13	No recommendations for 2013			
			24-Nov-14	No recommendations for 2014			
			7-Jul-15	On maternity leave			
			16-Oct-16	Complete Acceptable Usage Form to include access for all Level 2 IT resources	20-Oct-16	As per Policy #9.2.15 completed Acceptable Usage Form	
		██████████ (POFAP & Education Administrator)	10-Dec-13	No recommendations for 2013			
			24-Nov-14	No recommendations for 2014			
			4-Jun-15	Complete Acceptable Usage Form (B,E and I,J)	4-Jun-15	As per Policy #9.2.15 completed Acceptable Usage Form.	
			16-Oct-16	No recommendations			
		██████████ (SAVTI -new employee ██████████)	4-Mar-15	Complete Acceptable Usage Form to access Level 2 IT resources.	25-Mar-15	As per Policy #9.2.15 completed Acceptable Usage Form	
			27-Sep-16	No recommendations			
		██████████ (Research, Clinical Programs: Satellite, AfterCare, POGONIS, Atlas -new	28-Sep-16	Complete Acceptable Usage Form.	27-Oct-16	As per Policy #9.2.15 completed Acceptable Usage Form.	
				De-identified record level data is currently transferred outside of the POGONIS room via encrypted iron key.	27-Oct-16	De-identified record level data transferred outside of the POGONIS room will be transferred via IronKey.	

Appendix 1: Privacy, Security, and Other Indicators

		employee August 2016)		Include FTP as secure method of transferring PHI with Tertiary and Satellite centres and other agents	27-Oct-16	FTP user account set- up by System and Network Analyst and implemented as per Policy #9.2.9 procedures.		
				Programs/Initiatives				
				Data Holding	Date PIA Complete	Description of Recommendation	Date Addressed or Proposed	Manner Each Recommendation Addressed
				SAVTI Database	14-Nov-13	POGO moved from paper-based client files to an internally developed database. With the development of the database and associated procedures, recommendations were made: 1) only authorized users (counsellors) would be given details re how to access the system remotely; 2) confidentiality agreements would be executed; 3) patient consents would be obtained; 4) user name and password protection would be in place via Remote Desktop Service (RDS) with SSL encryption; 5) implementation of a policy to enforce strong passwords and set automatic logging of failed attempts that will be reviewed by POGO IT staff; 6) set policies to activate screen saver after 15 minutes and session termination after 30 minutes; 7) set policies to limit and restrict data transfer from SAVTI-designated POGO laptops and prevent installation of software by user; 8) block access to SAVTI application from non-POGO computers/laptops; and 9) include line item in POGO Confidentiality	9-Mar-15	POGO's IT, SAVTI Provincial Coordinator worked collaboratively to develop the database and to ensure the recommendations were met. POGO IT then worked with the SAVTI Counsellors to instruct them on the new database and associated privacy and security procedures.

Appendix 1: Privacy, Security, and Other Indicators

				agreements to specify user conduct when logged on to system.		
		ACTS Database	15-Jan-14	The following recommendations were made: 1) ensure agreements are signed by both parties - Dana Farber and Parallax software; 2) DSA's are in place with the tertiary hospitals and PIA's are completed; 3) user name and password protection to be set for Remote Desktop Service (RDS) with SSL encryption 4) undertake audits regularly 5) ensure a threat and risk assessment is in place 6) Educational materials should be in place.	14-May-14	POGO worked collaboratively with all parties to ensure recommendations were in place.
		1. POFAP Registration Database (New) and 2. Processing payment for family by POGO (new)	25-Jun-15	After internal meetings, it was recommended that POGO develop a new POFAP Database with defined formatting/options to ensure greater accuracy and consistency of data coming from the tertiary centres, reduce IT support time for both POGO and the tertiary centres, flag death information, and provide better data validation. The new database would: 1) include a financial component whereby POGO (as opposed to the centres) could reimburse families directly for a portion of their out-of-pocket costs; 2) eliminate the transfer of data thereby reducing the risk of potential data breaches. It was recommended that the financial should first be piloted with a hospital.	1-Sep-16	POGO's IT, Database Developer and POFAP Manager worked collaboratively with the pilot tertiary centre to ensure appropriate policies and procedures were implemented. Access to e-files have been limited so that only staff involved in processing payments have access (POFAP Coordinator, Assistant, IT and CFO) access all; General Accounting Clerk accesses only the files she needs to generate payments; Raiser's Edge supervisor only to access the files for emailing notification that payment has been made and families are in RE with restriction to this usage only. Cheque numbers are taken from copies of VOID cheques to ensure accuracy. Letters were sent to families previously paid by CHEO informing them of the change of payer and consents were signed for transfer/use of financial information for POFAP payments. New families also sign consent forms.
		Monthly web-based rounds for health care	29-May-14	POGO Privacy Officers reviewed and recommended: 1) consent be obtained from patients/survivors prior to presenting their case at rounds;	10-Jan-15	POGO drafted patient consent from which was reviewed by Janice Campbell, Privacy Officer for SickKids. Consents for neuro-oncology and stem cell transplant rounds

Appendix 1: Privacy, Security, and Other Indicators

		professionals and parent advisory panels for the purpose of inter-centre communication and clinical consultation initiative		2) participants can only connect in the secure OTN room at the centres; 3) a separate POGO secure FTP account is created for each type of rounds (neuro-oncology, stem cell transplant); 4) FTP user accounts created for each user as per POGO Policy #9.2.9 (<i>Secure Transfer of Records of PHI</i>); and 5) POGO documents the schedule of the rounds and stores all minuted rounds securely in the POGONIS secured data centre		are managed by physician heads at SickKids, and the patient consented list is sent to centres prior to OTN session via POGO secure FTP. Dissemination of patient list to participating oncology staff at each institution is restricted to internal email distribution only. Minutes of the rounds are circulated via POGO secure FTP and attendees secure the minutes as per hospital privacy and security policies and procedures.
		POGONIS	4-Apr-16	Confidentiality Agreements should be signed by pre-authorized agents who view PRDV and are renewed annually. And implement mitigation strategies recommended: 1)All authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) Server and Network level security rules are in place. 3) All connections are logged by POGO System and Network Administrator; 4) P/P are in place to secure and protect the data by where the data is viewed, by whom, and when; 5) Patient names, address and HC# are blocked from viewing. If this application is viewed for by any member of a Research Team for POGO Approved Research Projects e.g. IMPACT study , a member of the IT/Data team must be present at all times; and 7) Print outs are not available from the PRDV application.	4-Apr-16	All recommendations were addressed and implemented. as per below: 1)All authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) Server and Network level security rules are in place. 3) All connections are logged by POGO System and Network Administrator; 4) P/P are in place to secure and protect the data by where the data is viewed, by whom, and when; 5) Patient names, address and HC# are blocked from viewing. If this application is viewed for by any member of a Research Team for POGO Approved Research Projects e.g. IMPACT study , a member of the IT/Data 7) Print outs are not available from the PRDV application

Appendix 1: Privacy, Security, and Other Indicators

	▪ The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion.	▪ There have been 2 privacy impact assessments undertaken but not completed since the prior review. ▪ The proposed date of review is November 2016
	▪ The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion.	▪ None

Appendix 1: Privacy, Security, and Other Indicators

	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.	There are 33 determinations where a privacy impact assessment is not required to be completed (11 programs per year over 3 years). <table><tr><th>Data Holding, Information System, Technology or Program</th><th>Reasons for Determination</th></tr><tr><td>Fundraising</td><td>Data holdings, information systems, technologies or programs do not involve the collecting, use or disclosure of personal health information.</td></tr><tr><td>Finance</td><td>Same as above.</td></tr><tr><td>Human Resources</td><td>Same as above.</td></tr><tr><td>Research</td><td>Same as above.</td></tr><tr><td>Special Events & Community Outreach</td><td>Same as above.</td></tr><tr><td>Student Program</td><td>Same as above.</td></tr><tr><td>Communications</td><td>Same as above.</td></tr><tr><td>Guidelines Methodologist</td><td>Same as above.</td></tr><tr><td>Volunteer Program</td><td>Same as above.</td></tr><tr><td>Conference & Educational Events</td><td>Same as above.</td></tr><tr><td>Administration and Reception</td><td>Same as above.</td></tr></table>	Data Holding, Information System, Technology or Program	Reasons for Determination	Fundraising	Data holdings, information systems, technologies or programs do not involve the collecting, use or disclosure of personal health information.	Finance	Same as above.	Human Resources	Same as above.	Research	Same as above.	Special Events & Community Outreach	Same as above.	Student Program	Same as above.	Communications	Same as above.	Guidelines Methodologist	Same as above.	Volunteer Program	Same as above.	Conference & Educational Events	Same as above.	Administration and Reception	Same as above.
Data Holding, Information System, Technology or Program	Reasons for Determination																									
Fundraising	Data holdings, information systems, technologies or programs do not involve the collecting, use or disclosure of personal health information.																									
Finance	Same as above.																									
Human Resources	Same as above.																									
Research	Same as above.																									
Special Events & Community Outreach	Same as above.																									
Student Program	Same as above.																									
Communications	Same as above.																									
Guidelines Methodologist	Same as above.																									
Volunteer Program	Same as above.																									
Conference & Educational Events	Same as above.																									
Administration and Reception	Same as 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.	There are 25 privacy impact assessments that have been reviewed and amended since the previous review. <table><tr><th>Agent (Data Holding)</th><th>Description of Recommendation</th><th>Amendments Made</th></tr><tr><td>████ (POGONIS, Research)</td><td>Complete Acceptable Usage Form to access Level 1 IT resources</td><td>As per Policy #9.2.15 completed Acceptable Usage Form.</td></tr><tr><td>████ (Atlas Project)</td><td>Complete Acceptable Usage Form. De-identified record level data is currently transferred outside of the POGONIS room via encrypted Iron Key</td><td>As per Policy #9.2.15 completed Acceptable Usage Form. As per Policy #9.2.9 De-identified record level data transferred outside of the POGONIS room will be transferred via Iron Key.</td></tr></table>	Agent (Data Holding)	Description of Recommendation	Amendments Made	████ (POGONIS, Research)	Complete Acceptable Usage Form to access Level 1 IT resources	As per Policy #9.2.15 completed Acceptable Usage Form.	████ (Atlas Project)	Complete Acceptable Usage Form. De-identified record level data is currently transferred outside of the POGONIS room via encrypted Iron Key	As per Policy #9.2.15 completed Acceptable Usage Form. As per Policy #9.2.9 De-identified record level data transferred outside of the POGONIS room will be transferred via Iron Key.															
Agent (Data Holding)	Description of Recommendation	Amendments Made																								
████ (POGONIS, Research)	Complete Acceptable Usage Form to access Level 1 IT resources	As per Policy #9.2.15 completed Acceptable Usage Form.																								
████ (Atlas Project)	Complete Acceptable Usage Form. De-identified record level data is currently transferred outside of the POGONIS room via encrypted Iron Key	As per Policy #9.2.15 completed Acceptable Usage Form. As per Policy #9.2.9 De-identified record level data transferred outside of the POGONIS room will be transferred via Iron Key.																								

Appendix 1: Privacy, Security, and Other Indicators

		██████████ (Clinical Programs; Satellite, AfterCare, ACTS)	Complete Acceptable Usage Form. Include FTP as secure method of transferring PHI with Satellite centres	As per Policy #9.2.15 completed Acceptable Usage Form. FTP user account set- up by System and Network Analyst and implemented as per Policy #9.2.9 procedures.
		██████████ (Research, Clinical Programs: Satellite, AfterCare, POGONIS, Atlas)	Complete Acceptable Usage Form. De-identified record level data is currently transferred outside of the POGONIS room via encrypted Iron Key. Include FTP as secure method of transferring PHI with tertiary and satellite centres and other agents.	As per Policy #9.2.15 completed Acceptable Usage Form. De-identified record level data transferred outside of the POGONIS room will be transferred via Iron Key. FTP user account set- up by System and Network Analyst and implemented as per Policy #9.2.9 procedures.
		██████████ (Administration: Medical Director, Corporate	Complete Acceptable Usage Form. Include FTP as secure method of transferring PHI with tertiary centres and MOH EAP of the Ontario Public Drug Program	As per Policy #9.2.15 completed Acceptable Usage Form. FTP user account set- up by System and Network Analyst and implemented as per Policy #9.2.9 procedures.
		██████████ (POGONIS)	Complete Acceptable Usage Form.	As per Policy #9.2.15 completed Acceptable Usage Form.
		██████████ (IT, POGONIS, POFAP, SAVTI, Interlink, ACTS)	Complete Acceptable Usage Form to include all Level 0 IT resources.	As per Policy #9.2.15 completed Acceptable Usage Form.
		██████████ (Clinical Programs: Satellite, AfterCare, POGONIS, Atlas)	Complete Acceptable Usage Form to include all Level 1 IT resources.	As per Policy #9.2.15 completed Acceptable Usage Form.
		██████████ (IT, POGONIS, POFAP, SAVTI, Interlink, ACTS)	Complete Acceptable Usage Form to include access to Level 0 IT Resources.	As per Policy #9.2.15 completed Acceptable Usage Form.
		██████████ (IT, POGONIS, POFAP, SAVTI, Interlink, ACTS)	Complete Acceptable Usage Form to include access to all Level 0 IT Resources.	As per Policy #9.2.15 completed Acceptable Usage Form.

Appendix 1: Privacy, Security, and Other Indicators

		 (POGONIS, Research)	Complete Acceptable Usage Form to include access to Level 1 IT Resources.	As per Policy #9.2.15 completed Acceptable Usage Form.
		 (POFAP)	Complete Acceptable Usage Form to include access to Level 2 IT Resources.	As per Policy #9.2.15 completed Acceptable Usage Form.
		 (POGONIS)	Complete Acceptable Usage Form to include access for all Level 1 IT resources.	As per Policy #9.2.15 completed Acceptable Usage Form.
		 (SAVTI)	Complete Acceptable Usage Form to include access for all Level 2 IT resources.	As per Policy #9.2.15 completed Acceptable Usage Form.
		 (POFAP & Education Administrator)	Complete Acceptable Usage Form (B,E and I,J).	As per Policy #9.2.15 completed Acceptable Usage Form.
		 (SAVTI -new employee)	Complete Acceptable Usage Form to access Level 2 IT resources.	As per Policy #9.2.15 completed Acceptable Usage Form.
		 (Research, Clinical Programs: Satellite, AfterCare, POGONIS, Atlas - new employee August 2016)	Complete Acceptable Usage Form.	As per Policy #9.2.15 completed Acceptable Usage Form.
			De-identified record level data is currently transferred outside of the POGONIS room via encrypted Iron Key.	De-identified record level data transferred outside of the POGONIS room will be transferred via Iron Key.
			Include FTP as secure method of transferring PHI with tertiary and satellite centres and other agents.	FTP user account set- up by System and Network Analyst and implemented as per Policy #9.2.9 procedures.
		Programs/Initiatives		

Appendix 1: Privacy, Security, and Other Indicators

		SAVTI Database	POGO moved from paper-based client files to an internally developed database. With the development of the database and associated procedures, recommendations were made: 1) only authorized users (counsellors) would be given details re how to access the system remotely; 2) confidentiality agreements would be executed; 3) patient consents would be obtained; 4) user name and password protection would be in place via Remote Desktop Service (RDS) with SSL encryption; 5) implementation of a policy to enforce strong passwords and set automatic logging of failed attempts that will be reviewed by POGO IT staff; 6) set policies to activate screen saver after 15 minutes and session termination after 30 minutes; 7) set policies to limit and restrict data transfer from SAVTI-designated POGO laptops and prevent installation of software by user; 8) block access to SAVTI application from non-POGO computers/laptops; and 9) include line item in POGO Confidentiality agreements to specify user conduct when logged on to system.	POGO's IT, SAVTI Provincial Coordinator worked collaboratively to develop the database and to ensure the recommendations were met. POGO IT then worked with the SAVTI Counsellors to instruct them on the new database and associated privacy and security procedures.
		ACTS Database	The following recommendations were made: 1) ensure agreements are signed by both parties - Dana Farber and Parallax software; 2) DSA's are in place with the tertiary hospitals and PIA's are completed; 3) user name and password protection to be set for Remote Desktop Service (RDS) with SSL encryption 4) undertake audits regularly 5) ensure a threat and risk assessment is in place 6) Educational materials should be in place.	POGO worked collaboratively with all Parties to ensure recommendations were in place.

Appendix 1: Privacy, Security, and Other Indicators

		1. POFAP Registration Database (New) and 2. Processing payment for family by POGO (new)	After internal meetings, it was recommended that POGO develop a new POFAP Database with defined formatting/options to ensure greater accuracy and consistency of data coming from the tertiary centres, reduce IT support time for both POGO and the tertiary centres, flag death information, and provide better data validation. The new database would: 1) include a financial component whereby POGO (as opposed to the centres) could reimburse families directly for a portion of their out-of-pocket costs; 2) eliminate the transfer of data thereby reducing the risk of potential data breaches. It was recommended that the financial should first be piloted with a hospital.	POGO's IT, Database Developer and POFAP Manager worked collaboratively with the pilot tertiary centre to ensure appropriate policies and procedures were implemented. Access to e-files have been limited so that only staff involved in processing payments have access (POFAP Coordinator, Administrative Assistant, IT and CFO) access all; General Accounting Clerk accesses only the files she needs To generate payments; Raiser's Edge (RE)supervisor only to access the files for emailing notification that payment has been made and families are in RE with restriction to this usage only. Cheque numbers are taken from copies of VOID cheques to ensure accuracy. Letters were sent to families previously paid by CHEO informing them of the change of payer and consents were signed for transfer/use of financial information for POFAP payments. New families also sign consent forms.
		Monthly web-based rounds for health care professionals and parent advisory panels for the purpose of inter-centre communication and clinical consultation initiative	POGO Privacy Officers reviewed and recommended: 1) consent be obtained from patients/survivors prior to presenting their case at rounds; 2) participants can only connect in the secure OTN room at the centres; 3) a separate POGO secure FTP account is created for each type of rounds (neuro-oncology, stem cell transplant); 4) FTP user accounts created for each user as per POGO Policy #9.2.9 (<i>Secure Transfer of Records of PHI</i>); and 5) POGO documents the schedule of the rounds and stores all minuted rounds securely in the POGONIS secured data centre	POGO drafted patient consent from which was reviewed by Janice Campbell, Privacy Officer for SickKids. Consents for neuro-oncology and stem cell transplant rounds are managed by physician heads at SickKids, and the patient consented list is sent to centres prior to OTN session via POGO secure FTP. Dissemination of patient list to participating oncology staff at each institution is restricted to internal email distribution only. Minutes of the rounds are circulated via POGO secure FTP and attendees secure the minutes as per hospital privacy and security policies and procedures.
		POGONIS	Confidentiality Agreements should be signed by pre-authorized agents who view PRDV and are renewed annually. And implement mitigation strategies recommended: 1)All authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) Server and Network level security rules are in	All recommendations were addressed and Implemented as follows: 1) Confidentiality Agreements are signed by all agents granted Access to view PRDV and are renewed annually. 2) All authorized agents connect to PRCV application using Remote Desktop Connection to application server 3) POGO System and Network Analyst configured security settings to prevent unauthorized attempts and granted access to

Appendix 1: Privacy, Security, and Other Indicators

		place. 3) All connections are logged by POGO System and Network Administrator; 4) P/P are in place to secure and protect the data by where the data is viewed, by whom, and when; 5) Patient names, address and HC# are blocked from viewing. If this application is viewed for by any member of a Research Team for POGO Approved Research Projects e.g. IMPACT study , a member of the IT/Data team must be present at all times; and 7) Print outs are not available from the PRDV application.	only authorized agent. In addition, all connections are logged. Each authorized agent is given username and strong password. 4) P/P developed and implemented by Privacy Officers and IT Team to secure and protect the data by where the data is viewed, by whom and when (date). 5) The application was developed to block highly sensitive Identifiers i.e. patient names, address and HC# from being viewed. In addition, P/P are in place to ensure that a member of the IT/Data team must be present at all times when application is viewed by a Research team members. 6) The application does not allow for any print outs of data.			
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.	2014				
		Programs	Review Date	Recommendations	Date Completed	Manner Each Recommendation Addressed Or Proposed Manner
		Internal Program Area Reviews				
		POGONIS: PET (7 sites)	5-Jan-14	1) Ensure PIA completed by CCO; 2) DSA executed between CCO and POGO; 3) Secure Data Transfer procedure through Tumbleweed tested and user access implemented; 4) Training of pediatric tertiary centres prior to Launch date of May 1, 2014; and 5) POGO to test and implement importing of PET e-tool data into POGONIS patient records.	1-Jun-14	1) PIA completed by CCO in November 2013. reviewed by POGO April 2014; 2) DSA signed April 2014; 3) Data transfer process successfully implemented by CCO and successfully tested POGO IT team; 4) Training module developed by CCO/POGO and training completed at 5 pediatric tertiary centres between March and April 2014); and 5) POGO IT test the successful importing of PET e-tool data into POGONIS case records by using PHI to match cases. Successful testing of import completed.
		AfterCare: ACTS/ ACTS users (32 agents)	2-May-14	1) PIA and TRA to be completed prior to implementation. 2) Software License Agreement to be executed between POGO and DFCI. 3) Amendments to Tertiary Centre DSAs to be executed.	29-May-14	1) PIA and TRA completed by POGO May 2014. 2) License Agreement with DFCI signed June 2013. 3) Amendment DSA signed with tertiary centres (Jan to May 2014). 4) Server security completed 29 May 2014. 5) User authentication completed prior to given

Appendix 1: Privacy, Security, and Other Indicators

				4) Server security put in place (restrict web access to external hospitals IP addresses as per TRA). 5) Two level of user authentication - on Reverse Proxy using HTTPS and secondly on ACTS application. 6) Confidentiality agreements signed with all users. 7) Testing of external access and authentication. 8) Logging of failed Logon attempts and review by system administrators.		access in 2015. 6) Confidentiality agreements were signed for all users prior to end of Dec 2014. 7) Testing completed 29 May 2014. 8) Log created by System Administrators.	
		Interlink: Transfer of Data procedures, Laptops and IronKeys (11 agents)	19-Feb-14	Reviewed and audited: 1) Use of secure fax for transfer of data; 2) Emailing requests (first name, last initial); 3) Providing document passwords by phone; 4) Whether death information was inadvertently sent via email; 5) procedure re hotel accommodation requests; 6) procedure re. not sending thread from 3rd parties with names in emails; 7) procedure re. use POFAP # in emails and no diagnostic information to be include in email; 8) procedure re. transfer of POFAP client to another Interlink Nurse; 9) any breach incident that occurred. Distribute encrypted IronKeys to select Interlink Nurses and provide policy and procedure on use; acceptable use forms to be signed	19-Feb-14	In person meeting with all Interlink Nurses at POGO Office. Distributing encrypted keys and signing of Acceptable Use Form.	

Appendix 1: Privacy, Security, and Other Indicators

		POFAP: Privacy Training, Review/ Audit of Transfer of Data (7 agents)	12-Mar-14	Reviewed and audited: 1) use of secure fax for transfer of data; 2) emailing requests (first name, last initial); 3) providing document passwords by phone; 4) whether death information was inadvertently sent via email; 5) procedure regarding hotel accommodation requests; 6) procedure re. not sending thread from 3rd parties with names in emails; 7) procedure re. use POFAP # in emails and no diagnostic information to be include in email; 8) procedure re. transfer of POFAP client to another Interlink Nurse; 9) any breach incident that occurred.	12-Mar-14	In person meeting with all POFAP Data Managers at POGO Office.
		Atlas: Atlas Authors Data Destruction Forms (9 agents)	2-Dec-14	POGO Privacy Team audited the Data Destruction Forms with the Atlas Research Coordinator to confirm that all datasets provided to the Atlas Chapter Authors were duly destroyed as pre POGO policies and procedures for data destruction.	2-Dec-14	All outstanding data destruction forms were completed by Atlas Authors and Atlas Research Coordinator confirmed destruction.
		<u>2015</u>				
		Programs	Review Date	Recommendations	Date Completed	Manner Each Recommendation Addressed Or Proposed Manner
Internal Program Area Reviews						

Appendix 1: Privacy, Security, and Other Indicators

		Satellites: Auditing patient identifiers in Satellite database with Satellite nurse coordinators (7 agents)	6-Aug-15 to 19-May-16	To ensure the accuracy of Patient identifiers in the Satellite database, Satellite centre specific patient lists were shared and audited by the Senior Clinical Program Manager and Satellite Nurse Coordinators. Secure file transfer protocol (FTP) used to shared the patient lists. When PHI was required to further confirm case, telephone communication occurred between POGO and Satellite site.	6-Aug-15 to 19-May-16	1) Nurse Coordinators were given detailed instructions on how to use FTP to download patient lists (by NB). Data destruction procedures were provided; 2) Final audited patient lists were stored securely on POGO filing system; and 3) Edits were made in the Satellite database accordingly.
		AfterCare: ACTS Implementation of Pilot Project (32 agents)	Between Jan 15 & Nov 15	Pilot project site visits for training, auditing and testing at site, and ensuring appropriate access by health care professionals.	Between Jan 15 & Nov 15	Worked with each site to ensure they had access to POGO's secure server, ensured restriction to limited uses was in place, ensured secure printing and user authentication forms completed between January 2015 to November 2015.
		SAVTI Provincial Coordinator and Counsellors (5 agents)	4-Mar-15	Following the implementation of the electronic SAVTI Database, the Privacy Officers audited the new SAVTI process: 1) only authorized users (counsellors) would be given details re how to access the system remotely; 2) confidentiality agreements would be executed; 3) patient consents would be obtained; 4) user name and password protection would be in place via Remote Desktop Service (RDS) with SSL encryption; 5) implementation of a policy to enforce strong passwords and set automatic logging of failed attempts that will be reviewed by POGO IT staff; 6) set policies to activate screen saver after 15 minutes and session termination after 30 minutes; 7) set policies to limit and restrict data transfer from SAVTI-designated POGO	9-Mar-15	POGO's Privacy Officers and POGO IT met with each SAVTI Provincial Coordinator and Counsellor to ensure the recommendations were met and to instruct them on the new database and associated privacy and security procedures.

Appendix 1: Privacy, Security, and Other Indicators

				laptops and prevent installation of software by user; 8) block access to SAVTI application from non-POGO computers/laptops; and 9) include line item in POGO Confidentiality agreements to specify user conduct when logged on to system.		
		External Privacy Compliance Reviews (10% of PRU Projects)				
		PRU # 144: [REDACTED]	4-Nov-15	1) Require copy of amendments to REB; 2) Due to large dataset collected from SickKids, not permitted to collect information from POGO tertiary sites; 3) Further discussion with PIs is required whether POGO should receive a listing of all additional cases within POGONIS database who have confirmed ICH or any other confirmed Organ Complication based on SickKids Health Records extraction and research team member's chart review; 4) Destruction date TBD; key file that can decode de-identified ID will be destroyed upon researcher's discretion, POGO will be notified upon its destruction; and 5) Remote chance that individuals will be able to identify themselves within a publication (not a consented study); agents will use the same hospital process as consented studies there is a request for access	6-Nov-15	1) Amendment received November 6, 2015. 2) Small cell protocol followed when transferring of data. 3) Method of destruction: Document shredding and electronic dataset destruction for February 2023.
		PRU #129 [REDACTED]	19-Nov-15	1) Extended retention period to 2023; requires researcher's sign off 2) Data destruction date, updated to 2023 reflect above change 3) Destruction will take place at POGO office 4) POGO to be provided with updates regarding published work.	19-Nov-2015	1) PIA retention period updated. Researcher signed off. 2) Destruction date updated to 30 June 2023. Researcher signed off. 3)PIA updated to reflect change; destruction will take place at POGO Office. Researcher signed off. 4) Per POGO Researcher Agreement, POGO is

Appendix 1: Privacy, Security, and Other Indicators

						provided with regular updates regarding published work.
		PRU #130:	20-Nov-15	1) Updates to Privacy Impact Assessment requested 2) Extended retention period to 2023; requires researcher's sign off 3) Data destruction date, updated to reflect above change 4) Confirmation of coding of subjects by using unique ID and removal of PHI 5) Researcher to confirm with team member that chart abstraction copies are destroyed 6) REB re-approval letter requested 7) Confirmation of destruction of paper copies of chart abstractions 8) POGO to be provided with updates regarding published work.	20-Nov-2015	1) New project team members amended on PIA. Researcher signed off. 2) Update PIA to reflect new retention period and destruction date. Researcher signed off. 3) Researcher confirmed creation of Unique ID for each subject and removed PHI from main file. Linkage file (PHI to Unique ID) kept in separate and protected file, not in main project file. 4) Research coordinator confirmed Paper copies were destroyed as per policy post entry into main project file. 5) REB re-approval letter obtained by POGO 6) Per POGO Researcher Agreement, POGO is provided with regular updates regarding published work.
		PRU # 128:	4-Nov-15	1) Resend London REB approval; 2) Researcher will review Case Report Forms for patient data, upon her approval for use a Study ID will be issued with the following identifiers: date of birth, diagnosis, and date of diagnosis; source documents to be printed with patient identifiers being blocked as per policy; 3) Require list of active research team members, ensure confidentiality agreements in place for each; 4) Once results are available, PI's may	15-Nov-15	1) London REB provided by researcher Nov 4, 2015; and 2) List of active team members sent, and confidentiality agreements signed by all.

Appendix 1: Privacy, Security, and Other Indicators

		wish to send to POGO to incorporate into POGONIS database; 5) POGO to be provided with updates regarding published work; and 6) Currently no procedure in place to receive complaint regarding use of participant's PHI.																	
		<u>2016</u> <table border="1"> <thead> <tr> <th>Programs</th><th>Review Date</th><th>Recommendations</th><th>Date Completed</th><th>Manner Each Recommendation Addressed Or Proposed Manner</th></tr> </thead> <tbody> <tr> <td colspan="5">Internal Program Area Reviews</td></tr> <tr> <td> POGONIS: Patient Record Data View (5 agents) </td><td>5-Apr-16</td><td> POGO audited 5 agents to ensure their confidentiality agreements were signed prior to having access to PRDV and that all connections to the application met below security rules, policies and procedures developed by POGO Privacy Officers and IT Team. Confidentiality Agreements should be signed by pre-authorized agents who view PRDV and are renewed annually. And implement mitigation strategies recommended: 1) POGO Privacy Officers and IT Team ensures all authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) The IT Team ensures all Server and Network level security rules are in place. 3) The Privacy Officer reviewed with the POGO System and Network Administrator to ensure a mechanism </td><td>21-Apr-16</td><td> POGO Privacy Officers ensure Confidentiality Agreements have been signed by all authorized agents of PRDV. POGO Privacy Officers, Senior Database Administrator met with POGO IT to ensure each recommended strategy was successfully implemented as per below: 1)All authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) Server and Network level security rules are in place. 3) All connections are logged and audited by POGO System and Network Administrator; 4) P/P are in place to secure and protect the data by where the data is viewed, by whom, and when; 5) Patient names, address and HC# are blocked from viewing. If this application is viewed for by any member of a Research Team for POGO Approved Research Projects e.g. IMPACT study , a member of the IT/Data team must be present at all times; and 7) Print outs are not available from the PRDV application. </td></tr> </tbody> </table>			Programs	Review Date	Recommendations	Date Completed	Manner Each Recommendation Addressed Or Proposed Manner	Internal Program Area Reviews					POGONIS: Patient Record Data View (5 agents)	5-Apr-16	POGO audited 5 agents to ensure their confidentiality agreements were signed prior to having access to PRDV and that all connections to the application met below security rules, policies and procedures developed by POGO Privacy Officers and IT Team. Confidentiality Agreements should be signed by pre-authorized agents who view PRDV and are renewed annually. And implement mitigation strategies recommended: 1) POGO Privacy Officers and IT Team ensures all authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) The IT Team ensures all Server and Network level security rules are in place. 3) The Privacy Officer reviewed with the POGO System and Network Administrator to ensure a mechanism	21-Apr-16	POGO Privacy Officers ensure Confidentiality Agreements have been signed by all authorized agents of PRDV. POGO Privacy Officers, Senior Database Administrator met with POGO IT to ensure each recommended strategy was successfully implemented as per below: 1)All authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) Server and Network level security rules are in place. 3) All connections are logged and audited by POGO System and Network Administrator; 4) P/P are in place to secure and protect the data by where the data is viewed, by whom, and when; 5) Patient names, address and HC# are blocked from viewing. If this application is viewed for by any member of a Research Team for POGO Approved Research Projects e.g. IMPACT study , a member of the IT/Data team must be present at all times; and 7) Print outs are not available from the PRDV application.
Programs	Review Date	Recommendations	Date Completed	Manner Each Recommendation Addressed Or Proposed Manner															
Internal Program Area Reviews																			
POGONIS: Patient Record Data View (5 agents)	5-Apr-16	POGO audited 5 agents to ensure their confidentiality agreements were signed prior to having access to PRDV and that all connections to the application met below security rules, policies and procedures developed by POGO Privacy Officers and IT Team. Confidentiality Agreements should be signed by pre-authorized agents who view PRDV and are renewed annually. And implement mitigation strategies recommended: 1) POGO Privacy Officers and IT Team ensures all authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) The IT Team ensures all Server and Network level security rules are in place. 3) The Privacy Officer reviewed with the POGO System and Network Administrator to ensure a mechanism	21-Apr-16	POGO Privacy Officers ensure Confidentiality Agreements have been signed by all authorized agents of PRDV. POGO Privacy Officers, Senior Database Administrator met with POGO IT to ensure each recommended strategy was successfully implemented as per below: 1)All authorized agents connect to PRDV application via Remote Desktop Connection to application server; 2) Server and Network level security rules are in place. 3) All connections are logged and audited by POGO System and Network Administrator; 4) P/P are in place to secure and protect the data by where the data is viewed, by whom, and when; 5) Patient names, address and HC# are blocked from viewing. If this application is viewed for by any member of a Research Team for POGO Approved Research Projects e.g. IMPACT study , a member of the IT/Data team must be present at all times; and 7) Print outs are not available from the PRDV application.															

Appendix 1: Privacy, Security, and Other Indicators

				is in place for logging all connections. ; 4) Privacy Officers ensure P/P are in place to secure and protect the data by where the data is viewed, by whom, and when; 5) Privacy Officers and the IT Team ensure all Patient names, address and HC# are blocked from viewing. If this application is viewed for by any member of a Research Team for POGO Approved Research Projects e.g. IMPACT study , a member of the IT/Data team must be present at all times; and 7) Privacy Officers ensure that IT Team disables the Print out feature for the PRDV application.		
		MRD Proposal: Audit of PIA, data transfer and destruction (1 agent)	27-Apr-16	Audit of 45 Analysis Project - Minimal Residual Disease in collaboration with HQO and THETA: 1) Ensure Small Cell Committee approval documented; 2) Given data to be disclosed was small cell transfer of data via secure FTP was required; and 3) Small cell procedures and Authorization and Data Destruction documents to be completed.	4-May-16	POGO Analyst updated PIA as small cell data was not disclosed only aggregate data was shared with HQO and THETA. Data analysis occurred at POGO.
		POFAP: Manager and Data Managers (7 agents)	1-Sep-16	Following the implementation of the new POFAP Database, the Privacy Officers audited the new POFAP process to ensure the formatting/options maintained the privacy, security and accuracy of data coming from the tertiary centres, death information would no longer be received via email, and ensured data validation/logging in place with a view	7-Sep-16	POGO Privacy Officers and POGO's IT, Database Developer met with POFAP Manager and Data Managers to ensure: 1) Appropriate policies and procedures were implemented; 2) Access to e-files were limited so that only staff involved in processing registration and payment have access (POFAP Coordinator, Assistant, IT and CFO); and 3) New families sign consent forms.

Appendix 1: Privacy, Security, and Other Indicators

				to reducing the risk of potential data breaches.																	
		External Privacy Compliance Reviews (10% of PRU Projects)																			
		PRU #154: [REDACTED]	29-Jun-16 (Preliminary Audit)	Ironkey (encrypted USB key) given to Co-Principle Investigator Dr. L,A on 29-Jun-16. Agreement to be signed by PI and Co-PI and POGO Co-Privacy Officers to indicate contents and process in returning IronKey to POGO in October 2016. IronKey contents reviewed and audited by POGO Scientist to ensure no PHI contained. Permission received by SickKids REB for transfer of de-identified record level data via IronKey for analysis purposes to Spain. Acceptable use form to be signed by Co-PI.	30-Jun-16	1) POGO IT prepared IronKey for Co-PI; 2) Agreement prepared by Privacy Officers indicating all privacy and security procedures to be followed by Co-PI. Agreement signed by PI, Co-PI, POGO Scientist and Co-Privacy Officers; 3) Permissions received in writing from SickKids REB; and 4) POGO Scientist audited IronKey to ensure no PHI present.															
	- 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	12 other privacy audits completed since the prior review 2014: Other Privacy Audits <table><tr><th>Description</th><th>Review date</th><th>Recommendations</th><th>Date Each Recommendation was Addressed</th><th>Manner Each Recommendation Addressed or Proposed Manner</th></tr><tr><td colspan="5">Topic Reviews</td></tr><tr><td>Small cell size guidelines: POGO wished to investigate the possibility of using “OneMail”email service to securely transfer small cell data</td><td>8-Jan-14</td><td>1. invite OneMail representatives to present an overview of the features and possible solutions for POGO. 2. If OneMail was not possible, investigate other possible solutions to securely transfer PHI</td><td>20-Feb-14</td><td>1.After meeting with the OneMail representatives, it became clear that POGO would not be able to implement this process given not all POGO tertiary centers are part of OneMail. 2. POGO IT Team investigated other possible ways to transfer PHI and determined that Secure File Transfer via a FTP server could be used and was subsequently implemented.</td></tr></table>					Description	Review date	Recommendations	Date Each Recommendation was Addressed	Manner Each Recommendation Addressed or Proposed Manner	Topic Reviews					Small cell size guidelines: POGO wished to investigate the possibility of using “OneMail”email service to securely transfer small cell data	8-Jan-14	1. invite OneMail representatives to present an overview of the features and possible solutions for POGO. 2. If OneMail was not possible, investigate other possible solutions to securely transfer PHI	20-Feb-14	1.After meeting with the OneMail representatives, it became clear that POGO would not be able to implement this process given not all POGO tertiary centers are part of OneMail. 2. POGO IT Team investigated other possible ways to transfer PHI and determined that Secure File Transfer via a FTP server could be used and was subsequently implemented.
Description	Review date	Recommendations	Date Each Recommendation was Addressed	Manner Each Recommendation Addressed or Proposed Manner																	
Topic Reviews																					
Small cell size guidelines: POGO wished to investigate the possibility of using “OneMail”email service to securely transfer small cell data	8-Jan-14	1. invite OneMail representatives to present an overview of the features and possible solutions for POGO. 2. If OneMail was not possible, investigate other possible solutions to securely transfer PHI	20-Feb-14	1.After meeting with the OneMail representatives, it became clear that POGO would not be able to implement this process given not all POGO tertiary centers are part of OneMail. 2. POGO IT Team investigated other possible ways to transfer PHI and determined that Secure File Transfer via a FTP server could be used and was subsequently implemented.																	

Appendix 1: Privacy, Security, and Other Indicators

	was addressed or is proposed to be addressed.	between tertiary centers				
		Internal Privacy and Security Policies and Procedure Review				
		The Privacy Officers reviewed all Policies and Procedures in Section 9 of the POGO Privacy Binder: 9.1 Privacy 9.3 Human Resources 9.4 Organizational Policies	Jan to Dec 14	Review and edit (where applicable) all policies and procedures. Note where updates were needed in the revision section at the bottom of each policy	Jan to Dec 14	The Privacy Officers reviewed each policy over a year. Policies were updated where changes were required and revisions noted. See Indicators Part 1: General Privacy Policies for detailed changes.
		2015: Other Privacy Audits				
		Description	Review Date	Recommendations	Date Each Recommendation was Addressed	Manner Each Recommendation Addressed or Proposed Manner
		Topic Reviews				
		The Senior Database Administrator and IT Team to review Data linkage policies to ensure they were accurate and up to date	15-Jan-15	Review, edit or create applicable policies and procedures. In particular, review and edit Policy 9.2.18 to include the tracking of all linkages of POGO data using the Linkage System via the PRU database. Review Policy 9.1.12 to ensure accurate.	23-Jan -15	The Senior Database Administrator and IT Team reviewed and edited Policy 9.2.18 (Confidentiality and Security of Data). They also created an extra log in the PRU database.

Appendix 1: Privacy, Security, and Other Indicators

		They also reviewed other applicable policies				They provided Administrative Assistant to Privacy Officers with instructions on how to update log.
		The Privacy Officers reviewed the PIA Short Form that is applicable to all POGO Programs PIAs	10-Mar 15	Review and modify to create a more concise form that s reflects privacy, security, human resources and organizational polices.	10-Mar 15	The Privacy Officers added a column for staff to indicate what PI and PHI data elements they collect/have access to. The new form was communicated to staff by email and at a staff meeting prior to conducting annual 2015 staff PIA reviews.
		Internal Privacy and Security Policies and Procedure Review				
		The Privacy Officer reviewed all policies and procedures in Section 9 of the POGO Privacy Binder: 9.1 Privacy 9.3 Human Resources 9.4 Organizational Policies	Jan to Dec 2015	Review and edit (where applicable) all policies and note where updates were needed. Note changes in the revision section at the bottom of each policy.	Jan to Dec 2015	The Privacy Officers reviewed each policy over the course of the year. Policies were updated where changes were required. See Indicators Part 1: General Privacy Policies
		2016: Other Privacy Audits				
		Description	Review Date	Recommendations	Date Each Recommendation was Addressed	Manner Each Recommendation Addressed or Proposed Manner

Appendix 1: Privacy, Security, and Other Indicators

		The Privacy Officers reviewed the Fundraising: Donor information and Raiser's Edge Database	2-Jun-16	1) Review PIA with Chief Development Officer; 2) Confirm level of security for donor receipts; 3. Review security of database (Raiser's Edge); 4) review and confirm security regarding mailing lists; 5) Review and confirm there is limited access to the electronic Fundraising folder; and 6) Ensure any printed donor reports are shredded post use.	2-Jun-16	The Privacy Officers met with the Chief Development Officer to address the recommendations. All were confirmed. No further privacy and security recommendations made.
		The Privacy Officer reviewed 'Third-party Research Requests from CYP-C' with the Senior Adviser, Policy & Clinical Affairs, and POGO Scientist:	27-Jan-16	1) Develop POGO 'Review of Third-party Researcher Use of Ontario Data Contained Within CYC-P National Database'; 2) Create an additional form that provides questions or request for further clarification; and 3) Create a template for approval letters. .	11-Feb-16	It was determined that the Senior Database Administrator receives third-party research requests and proposals. The Privacy Officers developed the letter for further questions or requests for clarification regarding the project. This letter was reviewed and completed by POGO's Senior Adviser, Policy and Clinical Affairs, POGO Scientist, and Senior Database Administrator. It was determined that in the future, the approval letter would be forwarded to the researcher who requests the data, and cc'ing the head of CYP-C If clarification was warranted, the request form would be sent to the researcher requesting the data, cc'ing the head of CYP-C.
		Topic Reviews				
		The Privacy Officers reviewed the Data Access Protocols: Levels of Access for	15-Apr-16	Review the level of access for each POGO agent to ensure their access is consistent with POGO policy 9.1.6 (Levels of Access).	May-16	Privacy Team reviewed each agent's access level and ensured in both the log and policy. Log amended accordingly.

Appendix 1: Privacy, Security, and Other Indicators

		each agent to ensure they were appropriately placed		Ensure the Levels of Access Log is updated where applicable.		
		The Privacy Officers reviewed the procedures for PHI data security on mobile devices: i.e. phones, laptops & back-up tapes	25-Mar-16	Meet with Systems & network Analyst to review, edit policy and procedures re Policy #9.2.7 for mobile devices.	25-Mar-16	Privacy Officers reviewed procedures with System & Network Analyst. There were no changes to the policy and its procedure.
		Internal Privacy and Security Policies and Procedure Review				
		The Privacy Officers reviewed all policies and procedures in Section 9 of the POGO Privacy Binder: 9.1 Privacy 9.3 Human Resource 9.4 Organizational Policies	Jan to Oct 2016	Review and edit (where applicable) all policies and procedures. Note where updates were needed in the revision section at the bottom of each policy .	Jan to Dec2016	The Privacy Officers reviewed each policy over the course of the year. Policies were updated where changes were required and noted in the revision section of the policy. See Indicators Part 1: General Privacy Policies
Privacy Breaches	- The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity - There have been 28 notification of privacy breaches or suspected privacy breaches since the prior review.					

Appendix 1: Privacy, Security, and Other Indicators

	since the prior review by the Information and Privacy Commissioner of Ontario.	
	▪ With respect to each privacy breach or suspected privacy breach: – The date that the notification was received, – The extent of the privacy breach or suspected privacy breach, – Whether it was internal or external, – The nature and extent of personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the health information custodians or any other organizations, – The date that the investigation was commenced. The date that the investigation was completed,	▪ Please see table below.

Appendix 1: Privacy, Security, and Other Indicators

	– 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.	
--	---	--

Appendix 1: Privacy, Security, and Other Indicators

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr Mgmt Notif'd	Description of Recommendations & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
8-Jan-14	Unsecured email sent with PHI	Internal	Identifiable information relating to █████ patients	N/A	Permanently deleted email from both POGO and █████ servers	8-Jan-14	8-Jan-14	8-Jan-14	8-Jan-14	All records of the email were permanently deleted off of all systems
10-Feb-14	Unsecured email sent with PHI	Internal	Identifiable information relating to death notification	N/A	Permanently deleted email from both POGO and █████ servers	10-Feb-14	N/A	10-Feb-14	10-Feb-14	All records of the email were permanently deleted off of all systems
14-Feb-14	Unsecured email sent with PHI	Internal	Identifiable information relating to death notification	N/A	Permanently deleted email from POGO, █████ email	14-Feb-14	N/A	14-Feb-14	14-Feb-14	All records of the email were permanently deleted off of all systems
28-Feb-14	Unsecured email sent with PHI	Internal	Child's first initial and last name, as well as general treatment information	N/A	Permanently deleted email from system(s) by both █████ and █████	28-Feb-14	N/A	28-Feb-14	28-Feb-14	All records of the email were permanently deleted off of all systems
11-Mar-14	Unsecured email sent with PHI	Internal	Child's first and last name	N/A	Permanently deleted email from system(s) by both █████ and █████	17-Mar-14	N/A	11-Mar-14/17-Mar-14	17-Mar-14	All records of the email were permanently deleted off of all systems

Appendix 1: Privacy, Security, and Other Indicators

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr MgmtNotif'd	Description of Recommendations & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
16-May-14	██████ sent an email to ██████ which contained PHI (full patient name)	Internal	Child's first and last name	N/A	Permanently deleted emails from system(s) by ██████ and ██████	16-May-14	N/A	16-May-14	16-May-14	All records of the email were permanently deleted off of all systems
15-Jul-14	Unsecured email sent to POGO containing PHI	Internal	PHI: Patient/family name	N/A	Agents asked to permanently delete two emails (█████ initial email and ██████ response) from both deleted and trash folders. This was confirmed as complete.	15-Jul-14	N/A	15-Jul-14	15-Jul-14	All emails permanently deleted from all systems
21-Aug-14	an email with two full patient names sent by ██████ (POGO) and ██████ and one other recipient ██████	Internal	Two full patient names (from ██████)	N/A	All agents to permanently delete all copies of the message (i.e., ██████ and 1 other ██████ employee)	21-Aug-14	N/A	21-Aug-14	21-Aug-14	All emails permanently deleted from all systems
21-Nov-14	a Social Worker at ██████ emailed 3 scanned POFAP registration forms to ██████ at POGO	Internal	3 full patient/family names and related information (as is included on the registration form)	N/A	█████ to double deleted the email and request that the Social Worker do the same. She confirmed.	21-Nov-14	N/A	21-Nov-14	21-Nov-14	All emails permanently deleted from all systems
8-Dec-14	Interlink Nurse put the name of the child in the request for hotel form along with the parent name. Explained in the email that the family doesn't usually use the hotel program. A parent signed the consent but it is vague and we ask on the form for the parent's name	Internal	Full name of child, parent	N/A	All parties asked to double-delete email	8-Dec-14	N/A	8-Dec-14	8-Dec-14	All emails permanently deleted from all systems

Appendix 1: Privacy, Security, and Other Indicators

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr MgmtNotif'd	Description of Recommendations & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
9-Dec-14	On Tuesday, Dec 9 C () put the child's first initial and last name in an email about a transfer. We have both double deleted. Sent her the transfer policy.	Internal	Child first initial and last name	NA	Agent asked to double delete email	9-Dec-14	N/A	9-Dec-14	9-Dec-14	All emails permanently deleted from all systems
6-Jan-15	2 emails containing PHI sent to 3 recipients	Internal	Patient info	N/A	Double delete all copies of the email	6-Jan-15	N/A	6-Jan-15	6-Jan-15	All agents permanently deleted all copies of email
11-Mar-15	1 email containing PHI sent to 1 recipient	Internal	Patient Info	N/A	Double delete all copies of the email	11-Mar-15	N/A	11-Mar-15	11-Mar-15	All agents permanently deleted all copies of email
23-Apr-15	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	23-Apr-15	N/A	23-Apr-15	23-Apr-15	All agents permanently deleted all copies of email
19-Jun-15	1 email containing POGONIS chart number sent to 1 recipient	Internal	POGONIS Chart number sent via email	N/A	Double delete all copies of the email	19-Jun-15	N/A	19-Jun-15	19-Jun-15	All agents permanently deleted all copies of email
19-Jun-15	1 email containing PHI sent to 2 recipients	Internal	Patient info	N/A	Double delete all copies of the email	19-Jun-15	N/A	19-Jun-15	19-Jun-15	All agents permanently deleted all copies of email
2-Oct-15	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	2-Oct-15	N/A	2-Oct-15	2-Oct-15	All agents permanently deleted all copies of email
20-Oct-15	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	20-Oct-15	N/A	20-Oct-15	20-Oct-15	All agents permanently deleted all copies of email; reissue POFAP Privacy Policy
29-Oct-15	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	29-Oct-15	N/A	29-Oct-15	29-Oct-15	All agents permanently deleted all copies of email; reissue POFAP Privacy Policy
6-Nov-15	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	6-Nov-15	N/A	6-Nov-15	6-Nov-15	All agents permanently deleted all copies of email; reissue POFAP Privacy Policy
5-Jan-16	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	5-Jan-16	5-Jan-16	5-Jan-16	5-Jan-16	All agents permanently deleted all copies of email and were informed of POGO policy

Appendix 1: Privacy, Security, and Other Indicators

Date Notif'n Received	Extent of Breach	Internal or External	Nature & Extent of PHI	Date Snr MgmtNotif'd	Description of Recommendations & Containment Measures	Date(s) Containment Implemented	Date(s) HICs/ Other Orgs Notified	Date Investigation Commenced & Completed	Date(s) Recomm Addressed	Manner Recommendation(s) Addressed or Proposed Manner
11-Mar-16	2 emails sent containing PHI to 2 recipients	Internal	Patient info	N/A	Double delete all copies of the email	11-Mar-16	11-Mar-16	11-Mar-16	11-Mar-16	All agents permanently deleted all copies of email and were informed of POGO policy
17-Mar-16	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	17-Mar-16	17-Mar-16	17-Mar-16	17-Mar-16	All agents permanently deleted all copies of email and were informed of POGO policy; telephone call made to sender to discuss privacy compliance
28-Jun-16	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Save the list, give it a password; double delete all copies of the email	28-Jun-16	28-Jun-16	28-Jun-16	29-Jun-16	All agents permanently deleted all copies of email and were informed of POGO policy; privacy training to be booked to discuss privacy compliance and provide refresher
7-Jul-16	1 email containing PHI sent to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	7-Jul-16	7-Jul-16	7-Jul-16	7-Jul-16	All agents permanently deleted all copies of email and were informed of POGO policy
18-Jul-16	1 email containing PHI attached to an email to 1 recipient	Internal	Patient info	N/A	Double delete all copies of the email	18-Jul-16	18-Jul-16	18-Jul-16	18-Jul-16	All agents permanently deleted all copies of email and were informed of POGO policy
6-Oct-16	1 email containing PHI attached to an email to 1 recipient	Internal	Hospital chart number	N/A	Double delete all copies of the email	6-Oct-16	6-Oct-16	6-Oct-16	6-Oct-16	All agents permanently deleted all copies of email and were informed of POGO policy
18-Oct-16	1 email containing PHI sent to recipient	Internal	Patient MRN and names	N/A	Double delete all copies of the email	18-Oct-16	18-Oct-16	18-Oct-16	18-Oct-16	All agents permanently deleted all copies of email and were informed of POGO policy

Appendix 1: Privacy, Security, and Other Indicators

Privacy Complaints	▪ The number of privacy complaints received since the prior review by the Information and Privacy Commissioner of Ontario.	▪ 0 privacy complaints received.
	▪ Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint investigated: – The date that the privacy complaint was received, – The nature of the privacy complaint, – The date that the investigation was commenced, – The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation, – The date that the investigation was completed, – A brief description of each recommendation made,	▪ N/A

Appendix 1: Privacy, Security, and Other Indicators

	– The date each recommendation was addressed or is proposed to be addressed, – The manner in which each recommendation was addressed or is proposed to be addressed, and – The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.	
	▪ Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint not investigated: – The date that the privacy complaint was received, – The nature of the privacy complaint, and – The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.	▪ N/A

Appendix 1: Privacy, Security, and Other Indicators

Part 2 – Security Indicators

Categories	Security Indicators	POGO 2016	
General Security Policies and Procedures	The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.	Date	Policies Reviewed
		March 2014	9.2.3; 9.2.4; 9.2.6; 9.2.21, 9.3.18.
		April 2014	9.2.1; 9.2.2; 9.2.5; 9.2.7; 9.2.10; 9.2.20; 9.2.22; 9.2.26.
		November 2014	9.2.15; 9.2.18; 9.2.19.
		January 2015	9.2.4; 9.2.5; 9.2.6; 9.2.9; 9.2.10; 9.2.15; 9.2.17; 9.2.18; 9.2.19; 9.2.20; 9.2.22; 9.2.21; 9.2.26; 9.2.27, 9.3.18, 9.4.7.
		May 2015	9.2.1; 9.2.2; 9.2.3; 9.2.5; 9.2.7; 9.2.8; 9.2.11; 9.2.13.
		September 2015	9.2.15, 9.3.18, 9.4.7.
		January 2016	9.2.1;9.2.2; 9.2.3; 9.2.4; 9.2.5; 9.2.6; 9.2.7; 9.2.8;9.2.9; 9.2.10; 9.2.11; 9.2.13; 9.2.15; 9.2.17; 9.2.18; 9.2.19; 9.2.20; 9.2.21; 9.2.22; 9.2.24; 9.2.26; 9.2.27, 9.3.18, 9.4.7.
		February 2016	9.2.24.
		April 2016	9.2.3, 9.3.18, 9.4.7.
		October 2016	9.2.9

Appendix 1: Privacy, Security, and Other Indicators

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.			
	9.2.4	Threat and Risk Assessment	Updated procedure for moderate to high impact Vulnerabilities.
	9.2.13	Change Management	Additions to System Patch Management procedures.
	9.2.17	Information Security Incident Management Process	Medium and High category procedures updated.
	9.2.19	Document Shredding	Revisions to the procedures as per IPC Manual.
	Section 4 Audits: 4.1	POGO Privacy and Security Audit Program	Based on IPC recommendations of October 2014, POGO modified the Security Audit Program to address all the requirements of the Manual, pages 99 – 100.
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.	- A Business Continuity and Disaster Recovery Plan and its associated policies: #9.4.7 Business Continuity and Disaster Recovery Plan October 2015 and #9.4.12 BCDR Plan Essential Services October 2015 were further developed and implemented as a result of the 2013 review. This policy includes: - The purpose of the BCDR Plan - The nature and scope of the BCDR Plan - The individuals responsible for: updating and testing the Plan; notifying POGO agents and external stakeholders of interruption; maintaining contact lists; assessing level of severity, completing necessary document, and disseminating appropriately; conducting impact assessments; conducting damage assessment; resumption and recovery procedures and implementation; and for taking inventory of all business functions and office equipment, and IT specifications. - The frequency with which testing and maintenance are to be completed.		
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.	Date	Nature of Communication	
	24 January 2014	Communication of amendments to Privacy and Security policies and the need for BCDR at Board of Directors meeting. Amendments communicated for the following security policies:9.2.4, 9.2.6, 9.2.7, 9.2.8, 9.2.9, 9.2.10, 9.2.11, 9.2.13, 9.2.15, 9.2.18, 9.2.19, 9.2.24.	

Appendix 1: Privacy, Security, and Other Indicators

		21 February 2014	E-mail communication to staff regarding newly created Code of Conduct, Policy 9.3.8.All POGO staff asked to review and sign.
		14 March 2014	Presentation to Interlink Nurses and Social Workers highlighting new security policies and procedures. Amendments communicated for the following security policies: 9.2.1, 9.2.3, 9.2.5, 9.2.6, 9.2.7, 9.2.8, 9.2.9, 9.2.15, 9.2.17, 9.2.18, 9.2.19, 9.2.20, 9.2.21, 9.2.22.
		6 June 2014	POGO Privacy Newsletter distributed to POGO staff and agents which included highlighting of new policies and procedures.
		20 January 2015	Amendments to policies made throughout 2014 communicated to staff at a regularly scheduled staff meeting. Amendments communicated for the following security policies: 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.2.7, 9.2.10, 9.2.15, 9.2.17, 9.2.18, 9.2.19, 9.2.20, 9.2.21, 9.2.22, 9.2.26.
		30 January 2015	Directors updated on amendments made to Privacy and Security policies and procedures at a regularly scheduled Board of Directors meeting. Amendments communicated for the following security policies: 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.2.7, 9.2.10, 9.2.15, 9.2.17, 9.2.18, 9.2.19, 9.2.20, 9.2.21, 9.2.22, 9.2.26.
		4 February 2015	E-mail communication sent to Interlink Nurses regarding updates to Privacy and Security policies and procedures. Amendments communicated for policy 9.2.7.
		8 April 2015	Interlink Nurse privacy and security training to update on amendments made specific to Interlink practices. Amendments communicated for the following security policies: 9.2.1, 9.2.6, 9.2.7, 9.2.9, 9.2.17, 9.2.18, 9.2.19, 9.2.20, 9.2.21,
		16 June 2015	Amendments to Privacy and Security policies and procedures communicated to staff at a regularly scheduled staff meeting. Amendments communicated for the following security policies: 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.2.7, 9.2.8, 9.2.9, 9.2.10, 9.2.11, 9.2.13, 9.2.15, 9.2.17, 9.2.18, 9.2.19, 9.2.20, 9.2.21, 9.2.22, 9.2.26, 9.2.27.
		17 November 2015	The roll out of the BCDR Plan, its use, and testing measures with BCDR Planning, Executive Control and Business Resumption teams as per policies 9.4.7 and 9.4.12
		29 January 2016 and 21 March 2016	BCDR training for Tier 1 staff and Board of Directors as per policies 9.4.7 and 9.4.12; Discussed POGO Risk Assessment-Survey results, Annual Privacy Report and BCDR shared at Board of Directors meetings.
		9 February 2016	BCDR training for Tier 2 staff as per policies 9.4.7 and 9.4.12
		16 February 2016 and 21 March 2016	BCDR training for Tier 3 staff as per policies 9.4.7 and 9.4.12

Appendix 1: Privacy, Security, and Other Indicators

		6 April 2016	Presentation regarding amendments to Privacy and Security policies and procedures for SAVTI Counsellors. Amendments communicated for the following security policies: 9.2.7, 9.2.8, 9.2.9, 9.2.18, 9.2.19, 9.2.20, 9.2.21, 9.2.22,		
	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.	- POGO Privacy and Data Security Code updated and made available on POGO website in January 2014, following IPC review. - POGO Privacy and Data Security Code updated in September 2016 to include the BCDR Plan in Principle 7.3 Safeguards.			
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.	Date of Audit of Agents	Date Each Recommendation was Addressed	Recommendations Arising from Audit	The manner in which each recommendation was addressed
		September 2014	October 2014	Recommendations for how to keep office locked securely re. building cleaning staff.	Email was sent October 2014.
		September 2015	October 2015	Recommend completing a new key inventory.	Full key inventory completed October 2015.
		August 2016	September 2016	Full access card replacement occurred due to building upgrades.	All key cards replaced and updated with regard to level of access.
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.	Type of Security Audit		Frequency	
		Review of all Security Policies and Procedures		Annually by POGO Privacy Officers and IT team	
		POGO System/Security Audits		Biweekly on Monday by POGO System Administrator (82 audits in total over a period of 3 years)  POGO System Review-25Aug17.do	

Appendix 1: Privacy, Security, and Other Indicators

		POGONIS Security Audit	Biweekly on Tuesday by POGO Database Administrator (82 audits in total over a period of 3 years)  Appendix-POGONIS Security Audit dates																															
		Threat and Risk Assessments of POGO IP Addresses - Vulnerability - Penetration - Ethical Hacks	Annually or with scheduled system changes; conducted POGO System Administrator and reviewed by POGO Privacy Officers. (36 audits in total over a period of 3 years)																															
	▪ The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit: - A description of the nature and type of audit conducted, - The date of completion of the audit, - A brief description of each recommendation made, - The date that each recommendation was addressed or is proposed to be addressed, and - The manner in which each recommendation was addressed or is expected to be addressed.	▪ There were 200 security audits completed since the prior review, excluding policy reviews. <u>2014</u> <table><tr><th>Security Audits</th><th>Review Date</th><th>Findings/ Recommendations</th><th>Date Completed</th><th>Manner Each Recommendation Addressed or Proposed Manner</th></tr><tr><td colspan="5">Internal Privacy and Security Policies and Procedure Review</td></tr><tr><td>Policies in Section 9 of the POGO Privacy Binder: 9.2 Security Policies</td><td>Jan to Dec 2014</td><td>See Indicators Part 2 : General Security Policies</td><td>Dec 2014</td><td>See Indicators Part 2: General Security Policies</td></tr><tr><td colspan="5">POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)</td></tr><tr><td>Remote Desktop Connection</td><td>4-Nov-13</td><td>RDC V6 used by some Data Managers and it doesn't support disconnect after Idle time through gateway.</td><td>4-Nov-13</td><td>Automated screen lock implemented for RDC users</td></tr><tr><td>FTP server</td><td>4-Mar-14</td><td>Users leave files on FTP server for long time</td><td>4-Mar-14</td><td>Users get reminders to delete unused files</td></tr></table>			Security Audits	Review Date	Findings/ Recommendations	Date Completed	Manner Each Recommendation Addressed or Proposed Manner	Internal Privacy and Security Policies and Procedure Review					Policies in Section 9 of the POGO Privacy Binder: 9.2 Security Policies	Jan to Dec 2014	See Indicators Part 2 : General Security Policies	Dec 2014	See Indicators Part 2: General Security Policies	POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)					Remote Desktop Connection	4-Nov-13	RDC V6 used by some Data Managers and it doesn't support disconnect after Idle time through gateway.	4-Nov-13	Automated screen lock implemented for RDC users	FTP server	4-Mar-14	Users leave files on FTP server for long time	4-Mar-14	Users get reminders to delete unused files
Security Audits	Review Date	Findings/ Recommendations	Date Completed	Manner Each Recommendation Addressed or Proposed Manner																														
Internal Privacy and Security Policies and Procedure Review																																		
Policies in Section 9 of the POGO Privacy Binder: 9.2 Security Policies	Jan to Dec 2014	See Indicators Part 2 : General Security Policies	Dec 2014	See Indicators Part 2: General Security Policies																														
POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)																																		
Remote Desktop Connection	4-Nov-13	RDC V6 used by some Data Managers and it doesn't support disconnect after Idle time through gateway.	4-Nov-13	Automated screen lock implemented for RDC users																														
FTP server	4-Mar-14	Users leave files on FTP server for long time	4-Mar-14	Users get reminders to delete unused files																														

Appendix 1: Privacy, Security, and Other Indicators

		POGONIS Security Audit (Note: non-suspicious findings are not listed)				
		POGONIS production database biweekly review, database alert file	21-Oct-13	Some database configuration changes such as increasing number of cursors, and database restarts. Also some external connection refusals were seen in the alert log.	21-Oct-13	Configuration changes were temporary changes and implemented by POGO Database Administrator due to automatic signing of some forms (i.e. running database procedures: POGO_BATCH_SIGN, POGO_BATCH_SIGN_UPDATED). Nothing was done by unauthorized people. External direct connections to POGONIS database are strictly restricted, these are tests by POGO Database Administrator to ensure that restriction trigger (LOGON_TRIGGER) is working well.
		POGONIS production database biweekly review, database alert file server).	6-Jan-14	An error in Oracle server alert log: "Time drift detected. Please check VKTM trace file for more details.", even after the workaround done in Dec 10 to fix that error.	6-Jan-14	This does not affect the daily POGONIS operation. A workaround was done to fix this on Dec 10, 2013. https://forums.oracle.com/thread/2304662 . This workaround helped reducing the number of errors significantly but did not help stopping it at all. Further investigations will be done.
		POGONIS production database biweekly review, audit log at database level	23-Jan-14	No actions were seen in audit log, at all, with in this review period (Jan 6-Jan 24)	24-Jan-14	Checked that auditing is working properly by an ALTER SYSTEM test command, and ensured that auditing mechanism is working. There is no problem.
		POGONIS production database biweekly	11-Feb-14	1. ALTER USER by SY (POGO DBA) 2. TRUNCATE TABLE by SY	11-Feb-14	1. Password change. 2. Database view objects that used for temporarily (POGO_CASELOAD_AFU_D

Appendix 1: Privacy, Security, and Other Indicators

		review, audit log at database level				ATA, POGO_CASELOAD_LTFU_D ATA). Both actions were done by POGO Database Administrator, so there are no unauthorized activities.
		POGONIS production database biweekly review, audit log at database level	22-Apr-14	Object creations by POGO DBA (POGO_Chemo_from_PO GONIS1).	22-Apr-14	This is not an un-authorized action, so there is no problem. Object creations, drops and table truncations by POGO DBA during planned application version update on April 22.
		POGONIS production database biweekly review, audit log at database level	7-May-14	Object creations by POGO DBA (POGO_Chemo_from_PO GONIS1).	7-May-14	No suspicious actions in database audit logs. Object creations, drops and table truncations by POGO DBA during planned application version update on April 22.
		POGONIS production database biweekly review, application server local drive checking, PCRTERM C and D Drives (POGONIS application server local hard drives).	9-Jun-14	Older copies of PCR2 executable files (older versions were kept as backups of the PCR2 application) in drive C.	9-Jun-14	Currently Data Managers don't have access C drive, but we don't encourage POGO administrators to keep extra files under C or D drives. Older copies of PCR2 executable files were deleted, although they weren't PHI files.
		POGONIS production database biweekly review, audit log at database level	8-Jul-14	Some index creations by pcr2sys with OS account OraAdmin. And truncation of two tables.	8-Jul-14	These were done when we had POGONIS connection problem, and were done by POGO Database Administrator. No suspicious actions in database audit logs.
		POGONIS production database biweekly	12-Nov- 14	Some objects were dropped by POGO DBA.	12-Nov- 14	These were invalid objects and obsolete therefore deleted.

Appendix 1: Privacy, Security, and Other Indicators

		review, audit log at database level				
		POGONIS production database biweekly review, audit log at database level	23-Dec-14	Object creations (IDX_PCR_PRINT_SIZE, PK_PCR_PRINT_SIZES, PCR_PRINT_PAPER_SIZES due to application upgrade on Dec 9).	23-Dec-14	None. These objects were created as a part of application upgrade. No suspicious actions in database audit logs.
		2015				
		Security Audits	Review Date	Findings/ Recommendations	Date Completed	Manner Each Recommendation Addressed or Proposed Manner
		Internal Privacy and Security Policies and Procedure Review:				
		Policies in Section 9 of the POGO Privacy Binder: 9.2 Security Policies	Jan to Dec 2015	See Indicators Part 2 : General Security Policies	Dec 2015	See Indicators Part: General Security Policies
		POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)				
		Remote Desktop Connection	5-Jan-15	remote desktop connections settings were set up to "less secure" for workstations	5-Jan-15	Remote Desktop Connections settings on all POGO workstations changed to "more secure" options with Network Level Authentication by AD Group Policy
		Remote Desktop Connection	19-Jan-15	remote desktop connections settings were set up to "less secure" for servers	19-Jan-15	Remote Desktop Connections settings on all POGO Windows 2008/2012 servers changed to "more secure" options with Network Level Authentication

Appendix 1: Privacy, Security, and Other Indicators

		Email Servers	16-Feb-15	Intermediate GeoTrust certificate was missing for external OWA.	16-Feb-15	Certificate has been installed on Sophos UTM for Websever Protection
		FTP server	2-Mar-15	Intermediate GeoTrust certificate was missing for FTP server.	2-Mar-15	Certificate has been installed.
		DHCP server	16-Mar-15	Inactive DHCP exist	16-Mar-15	Server has been removed from Active Directory
		Remote Desktop Gateway	30-Mar-15	Secure Scan have detected SSL3 and RC4 Cipher on RD Gateway	30-Mar-15	SSLv3 and RC4 Cipher have been disabled on RD Gateway
		Host Servers	13-Apr-15	Secure Scan have detected old version of "HP System Management Homepage"	13-Apr-15	Newest version have been installed on all HP servers.
		FTP server	27-Apr-15	FTP server SSL certificate has been expired.	27-Apr-15	Certificate has been renewed
		Workstations	12-May-15	MS released more secure new version of Internet Explorer	12-May-15	MS Internet Explorer has been upgraded to version 11 on all desktops
		Webserver	8-Jun-15	Secure Scan have detected SSL3 on Web server	8-Jun-15	SSLv3 has been disabled on Web server
		Domain Controllers	22-Jun-15	Secure Scan have detected SSL3 and RC4 Cipher on Domain Controllers	22-Jun-15	SSLv3 and RC4 Cipher have been disabled on Domain Controllers

Appendix 1: Privacy, Security, and Other Indicators

		Host Servers and Email Servers	6-Jul-15	Secure Scan have detected SSL3 and RC4 Cipher on Virtual Host servers and Exchange Server	6-Jul-15	SSLv3 and RC4 Cipher have been disabled on Virtual Host servers and Exchange Server
		Backup Server	5-Oct-15	Secure Scan have detected SSL3 and RC4 Cipher on SQL database server and Backup Server	5-Oct-15	SSLv3 and RC4 Cipher have been disabled on SQL database server and Backup Server
		Remote Desktop Gateway	19-Oct-15	Secure Scan have detected SHA2 certificate on RD Gateway server	19-Oct-15	SSL Certificate has been renewed with SHA256
		FTP server	2-Nov-15	Secure Scan have detected TLS 1.0 and TLS 1.1 on FTP server	2-Nov-15	TLS 1.0 and TLS 1.1 have been disabled on FTP server
		Workstations	16-Nov-15	Last Service Pack is missing on 1 Desktop	16-Nov-15	Desktop OS updated to most current
		Website Server	28-Dec-15	Wordfence security plug-in reported many brute force attacks on POGO website	28-Dec-15	Wordfence security plug-in has been upgraded to Premium version. Country blocking setup for logon page to protect against brute force attacks
		POGONIS Security Audit (Note: non-suspicious findings are not listed)				
		POGONIS production database biweekly review, audit log at database level	5-Mar-15	Table truncations by user SY(POGO Database administrator) (tables truncated: POGO_CASELOAD_AFU_DATA and POGO_CASELOAD_LTFU_DATA)	5-Mar-15	None. These tables are temporary tables created for dashboard statistics and are reused whenever needed.

Appendix 1: Privacy, Security, and Other Indicators

		Servers Vulnerability Checks, by Tripwire software, run by POGO System Administrator	5-Jun-15	Oracle April 2015 Critical Patch Update Multiple Vulnerabilities (Tripwire ID: 211041)	5-Jun-15	Oracle has released cpuapr2015 (Critical Patch Update April 2015) to address this issue. POGONIS database does not have any JAVA related objects, so we will not be applying this patch.
		POGONIS production database biweekly review, audit log at database level	16-Oct-15	Object creations such as indexes in the database.	16-Oct-15	None. We had a mini-disaster situation on Sept 24, 2015 due to power shutdown in the building. When the power was back, our systems did not start properly. All virtual server files were corrupted and we had to restore virtual servers and databases from the latest tape backups. POGONIS was restored from 1 day earlier backup, these actions (OBJECT CREATIONS) are due to import into PCR2SYS schema.
		<u>2016</u>				
		Security Audits	Review Date	Findings/ Recommendations	Date Completed	Manner Each Recommendation Addressed or Proposed Manner
		Internal Privacy and Security Policies and Procedure Review				
		Policies in Section 9 of the POGO	January to October 2016	See Indicators Part 2 : General Security Policies	October 2016	See Indicators Part 2: General Security Policies

Appendix 1: Privacy, Security, and Other Indicators

		Privacy Binder: 9.2 Security Policies				
		POGO System/Security Audits and Threat and Risk Assessments of POGO IP Addresses (Note: only Medium to High Risk Findings are listed)				
		Email Server	11-Jan-16	Secure Scan have detected SHA2 certificate on Email Server	11-Jan-16	SSL Certificate has been renewed with SHA256
		Workstations	22-Feb-16	Oracle security alert about old Java version	22-Feb-16	Java updated to Java 8 version 73 on all workstations and all previous installers have been removed.
		Firewall	28-Mar-16	Unused Access Rules have been found on Firewall	28-Mar-16	Unused Access Rules have been removed from Firewall
		Firewall	24-Oct-16	DoS attack on ACTS IP address	24-Oct-16	Attack blocked by previously created rules
		POGONIS Security Audit (Note: non-suspicious findings are not listed)				
		POGONIS production database biweekly review, alert log for the database	7-Jun-16	Server crashes (unexpected shutdowns).	7-Jun-16 (incidents in the logs were addressed on the dates of the events, i.e. 25-May-16 and 30-May-16)	Server crash logs on 2016-05-25 and 2016-05-30 due to Toronto hydro power outages in downtown. (Logs like "2016-05-30 20:34pm opiodr aborting process unknown ospid (3384) as a result of ORA-609"). BCDR plans were executed as described in POGO's BCDR binder (i.e. notification of Business & Disaster Operation Team, and the Program Managers, followed by

Appendix 1: Privacy, Security, and Other Indicators

						review of the systems and applications, and finally notification of end users for their final end-user review).	
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,	▪ Not applicable					

Appendix 1: Privacy, Security, and Other Indicators

	– 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.	
--	---	--

Appendix 1: Privacy, Security, and Other Indicators

Part 3 – Human Resources Indicators

Categories	Human Resources Indicators	POGO 2016
Privacy and Security Training and Awareness	The number of agents who have received and who have not received initial privacy and security orientation since the prior review by the Information and Privacy Commissioner of Ontario.	Total: 73 - In 2013, 0 new agents (No initial training since November 2013) - In 2014, 15 new agents - In 2015, 32 new agents - In 2016, 26 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.	2013: 52 agents received ongoing privacy and security training 0 agent did not receive privacy training 2014: 80 agents received ongoing privacy and security training 0 agent did not receive privacy training 2015: 104 agents received ongoing privacy and security training 0 agents did not receive privacy training 2016: 73 agents received ongoing privacy and security training 2 new Board of Directors members agents have not yet received privacy training

Appendix 1: Privacy, Security, and Other Indicators

Categories	Human Resources Indicators	POGO 2016	
	The dates and number of communications to agents by the prescribed entity in relation to privacy and security since the prior review by the Information and Privacy Commissioner of Ontario and a brief description of each communication.	In addition to Parts 1 and 2 indicating communication regarding new and amended policies and procedures for Privacy and Security, please see the below chart:	
		Date	Nature of Communication
		6 January 2014	Communication to staff to sign annual Confidentiality Agreement, Policy 9.3.2.
		14 March 2014	Communication to staff reminding them that the POGONIS data centre door must be closed and secured at the end of the day as per policy 9.2.5.
		6 June 2014	Draft Code of Conduct, Policy 9.3.8 provided to POGO Board of Directors with request for input and/or approval Confidentiality Agreement provided with request for signature.
		6 June 2014	POGO Privacy Newsletter distributed to POGO staff and agents which included highlighting of new policies and procedures.
		27 October 2014	Reminder to staff to lock office doors at night and ensure sensitive information is locked away as per policy 9.2.5.
		5 January 2015	Communication to staff to complete annual review of PIA’s as per policy 9.1.14
		12 January 2015	Communication to staff to sign annual Confidentiality Agreement, Policy 9.3.2.
		21 February 2015	Communication to staff regarding the recently approved Code of Conduct, Policy 9.3.8 by the Board of Directors and request to read over and if agreeable to sign-off
		3 March 2015	Code of Conduct, Policy 9.3.8 sent to the new POGO President for review and sign-off
		20 November 2015	Communication to staff regarding policies and their new location on the server. All POGO policies now located on P drive. P:\Public\Staff Policies
		9 December 2015	Communication to staff directing their attention to new and updated privacy and security policies and procedures. Specifically, policies 9.1.22, 9.1.23, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.2.7, 9.2.10, 9.2.15, 9.2.17, 9.2.18, 9.2.19, 9.2.20, 9.2.21, 9.2.22, 9.2.26, 9.3.1
		8 January 2016	Communication to staff to sign annual Confidentiality Agreement, Policy 9.3.2.

Appendix 1: Privacy, Security, and Other Indicators

Categories	Human Resources Indicators	POGO 2016		
		15 August 2016	Communication to staff to complete annual review of PIA’s. Reminders on Sept 27 and October 8, 2016 as per policy 9.1.14	
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.	0 agents required to sign a Confidentiality Agreement annually have failed to do so 1 agent executed Confidentiality Agreements in 2013 between November and December 117 agents executed Confidentiality Agreements in 2014 0 agents required to sign a Confidentiality Agreement annually have not done so in 2014 145 agents executed Confidentiality Agreements in 2015 0 agents required to sign a Confidentiality Agreement annually and who have not done so 102 agents executed Confidentiality Agreements in 2016 23 agents required to sign a Confidentiality Agreement annually and who have not yet done so		
	The date of commencement of the employment, contractual or other relationship for agents that have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.	All 23 agents who have not yet signed a confidentiality agreement have signed an initial confidentiality agreement in the previous year(s) as required per POGO Policies and Procedures. All agents must execute confidentiality agreements by December 2016.		
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.	44 notifications from agents.		

Appendix 1: Privacy, Security, and Other Indicators

Part 4 – Organizational Indicators

Categories	Organizational Indicators	POGO (2016)
Risk Management	The dates that the corporate risk register was reviewed by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.	- Corporate Risk Management Framework revised August 26, 2015, clarifying the senior management team’s role in the identification and assessment of risks. - Corporate Risk Register reviewed by Director of Finance and Administration: - October, 2014 - July, 2015 - August, 2016 - POGO Board of Directors in January 2016
	Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.	- Annual updates by all Program Managers for program-specific risk reviews and assessments. - Update by Board of Directors to identified organizational risks. The Board specifically reviewed 5 (five) areas of concern with the largest changes from the previous review, 2 (two) decreases identified, and 3 (three) increased areas of concern.
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.	- POGO developed the final version of the Business Continuity and Disaster Recovery Plan in July 2015 - The entire plan was tested November 2015 (Executive, Planning, and Resumption Team) and again in January, February and March 2016 (all Staff and Board of Directors) 2 actual disruptions to POGO business occurred on July 18, 2015 and September 24, 2015 due to technological/man-made interruptions.
	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.	- Amendments to communications phone tree and internal notification were made – templates formed for accurate and prompt distribution - System is being developed to keep contacts up to date in hard copy and over web. Will implement to merge benefits of both by end of 2016.