Information
and Privacy
Commissioner/
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the Pediatric Oncology Group of Ontario:

A Prescribed Entity under the *Personal Health Information Protection Act*

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Review of the Pediatric Oncology Group of Ontario:
A Prescribed Entity under the *Personal Health Information Protection Act*

The *Personal Health Information Protection Act, 2004* (*PHIPA*) came into effect on November 1, 2004. The Information and Privacy Commissioner of Ontario (IPC) has been designated as the oversight body responsible for ensuring compliance with *PHIPA*. *PHIPA* establishes rules for the collection, use and disclosure of personal health information by health information custodians that protect the confidentiality of, and the privacy of individuals with respect to, that personal health information. In particular, *PHIPA* provides 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 *PHIPA*.

Responsibilities of Prescribed Entities

Section 45(1) of *PHIPA* 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 section 45(3).

Section 45(3) of *PHIPA* 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. Section 45(3) further requires each prescribed entity to ensure that these practices and procedures are approved by the IPC prior to November 1, 2005, in order for health information custodians to be able to disclose personal health information to the prescribed entity without consent and for the prescribed entity to:

- be able to collect personal health information from health information custodians;
- use personal health information as if it were a health information custodian for purposes of section 37(1)(j) or section 37(3) of *PHIPA*;
- disclose personal health information as if it were a health information custodian for purposes of sections 44, 45 and 47 of *PHIPA*;
- 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 purposes of section 43(1) (h).

Section 18(2) of Regulation 329/04 to *PHIPA*, further requires each prescribed entity to make publicly available a plain language description of its functions including 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.

Mandate of the IPC with Respect to Prescribed Entities

Prescribed entities must ensure that their practices and procedures to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information are reviewed and approved by the IPC prior to November 1, 2005. Thereafter, the IPC must review these practices and procedures every three years from the date of approval.

Review Process

The IPC met with all of the prescribed entities on two occasions to outline the process that would be followed by the IPC for the review of these practices and procedures. The process was to include a review of documentation relating to the practices and procedures of the prescribed entity to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of that information, as well as a visit to the primary site where personal health information was held by the prescribed entity. The IPC provided the prescribed entities with a preliminary checklist of privacy and security measures that the IPC would be looking for during the course of its review. The checklist included the following:

Human Resources

- Confidentiality agreements
- Disciplinary procedures for violations
- Clearly defined roles and responsibilities
- Appointed contact persons for privacy and security
- Ongoing education and training program for all staff, employees, affiliates, volunteers, etc. on security and privacy policies and procedures
- Third party agreements (with health information custodians, researchers, etc.)

Privacy

- Privacy policies and procedures that describe how the organization adheres to each fair information practice
- Privacy brochure – available upon request to the public
- Privacy Impact Assessments – for programs/database holdings

- Internal/external privacy audits
- Privacy crisis management protocols
- Data linkage protocols
- Procedures for de-identifying data
- Retention schedules and disposal procedures
- Inventory of all data holdings of personal health information
- Protocol for reviewing proposals in terms of their privacy impacts
- Mechanism for reviewing and updating privacy policies and procedures

Security

- Comprehensive security program including physical, technical and administrative measures
- Access control procedures – authentication and authorization
- Perimeter control
- Electronic access control
- Secure transfer procedures
- Audit trails
- Internal/external security audits
- Disaster Recovery Plan
- Mechanism for reviewing and updating security policies and procedures

The prescribed entities were informed that they were required to implement privacy and security measures and safeguards commensurate with the nature of the work undertaken by the prescribed entity, the amount and sensitivity (e.g., level of identifiability) of the information in the custody and control of the prescribed entity and the number and nature of the individuals who have access to personal health information. The scope of the review was to include practices and procedures relating to all personal health information in the custody and control of the prescribed entity. The review was not limited to personal health information collected, used and disclosed by the prescribed entity for purposes of section 45 of *PHIPA*.

A site visit was to be scheduled within one month of the IPC receiving the documentation from the prescribed entity. The purpose of the site visit was to provide the prescribed entities with

an opportunity to provide additional information to the IPC and to clarify their practices and procedures, and to provide the IPC with an opportunity to:

- review the physical, technological and administrative security measures implemented;
- ask questions about the documentation provided; and
- discuss privacy and security matters with appropriate staff of the prescribed entity.

Following the document review and site visit, each prescribed entity was to be informed of any action that it needed to take prior to having its practices and procedures approved by the IPC. Once all necessary action had been taken or if no action was necessary, the IPC would prepare a draft report that would be submitted to the prescribed entity for review and comment. If the IPC was satisfied that the entity had implemented practices and procedures that were sufficient to protect the privacy and confidentiality of personal health information, a letter of approval would be issued prior to November 1, 2005.

Description of the Prescribed Entity

The Pediatric Oncology Group of Ontario (POGO) is a prescribed entity under section 45 of *PHIPA*.

The Pediatric Oncology Group of Ontario (POGO) is a non-profit corporation founded in 1983 by a group of pediatric oncologists to provide a voice for childhood cancer control and treatment in the Province of Ontario. POGO's objective is to ensure that all of Ontario's children have equal access to state-of-the-art diagnosis, treatment and required ancillary services for cancer and have the greatest prospects for cancer survival with an optimal quality of life.

POGO is a multi centre collaboration of the oncology programs at the five pediatric hospitals in the Province of Ontario: The Hospital for Sick Children, McMaster Children's Hospital, Children's Hospital of Western Ontario, Kingston General Hospital and Children's Hospital of Eastern Ontario 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.

Through partnerships with Ontario's Ministry of Health and Long-Term Care (MOHLTC) and the childhood cancer community, POGO makes policy development and planning recommendations to the MOHLTC on pediatric cancer care and control based on comprehensive provincial data, scientific evidence and extensive clinical experience.

In 1985, POGO determined that none of the sources of data on childhood cancer available at that time provided sufficient or adequate information required for proper policy development and planning. Responding to this gap, POGO established and continues to maintain POGONIS – the Pediatric Oncology Group of Ontario Networked Information System – a registry capturing selective, standardized data on all childhood cancer cases in Ontario including demographic,

diagnosis, treatment and death information. Data in POGONIS is collected electronically from the five pediatric hospitals in Ontario that provide treatment for childhood cancer as well as the five satellite clinics operated by community hospitals (which deliver cancer care closer to the homes of children with cancer) and the seven pediatric and adult Aftercare programs affiliated with the pediatric hospitals that monitor and promote the health of survivors of childhood cancer.

Each of the five pediatric hospitals in Ontario that disclose personal health information to POGO have the ability to view the personal health information of their own patients to enable them to track statistics regarding their patients and the services provided.

Personal health information in POGONIS is used by POGO to monitor the:

- Incidence and prevalence of childhood cancer;
- Demand for care of pediatric oncology programs;
- Nature and specifics of pediatric cancer treatment;
- Services provided in pediatric and adult Aftercare programs; and
- Long-term effects of childhood cancer and its treatment.

Personal health information in POGONIS is also used by POGO to:

- Estimate the incidence of childhood cancer in Ontario;
- Plan new programs and ensure decisions about where to locate these new programs are well informed;
- Undertake population-based research;
- Project the number of children to be treated for cancer in the future;
- Forecast staff requirements needed to treat these children; and
- Understand where the children live in relation to where they are treated in order to facilitate the strategic location of treatment.

Review of the Prescribed Entity

Documents Reviewed

POGO provided the IPC with a binder of documents on September 2, 2005, including:

Organizational Materials

- POGO Brochures

- POGO Privacy Brochure
- Fact Sheets related to the Aftercare programs, the Pediatric Oncology Financial Assistance Program, POGONIS, POGO Programs and Services, the POGO Research Unit, the Successful Academic and Vocational Transition Initiative, the Provincial Pediatric Oncology Plan and the Provincial Pediatric Oncology Satellite Program
- POGO Organizational Chart
- Lists of POGO's Board of Directors, staff and committees
- Appointment of Privacy Officers
- Security Delegation Roles and Responsibilities
- Privacy Delegation Chart
- Data Security Committee Membership
- Permitted Data Flows for 45(1) Entity Status
- Privacy and Data Security Code
- Privacy and Data Procedures
- Privacy and Data Security Handbook
- Confidentiality Agreement
- Signed Confidentiality Agreement Form Log
- Consent to Use Photographs/Video

Administrative, Clinical and Other Datasets Held at POGO

- POGONIS Overview
- POGO Data Holdings
- POGONIS Data Request Form

Data Security Architecture and Related Documents

- Data Sharing Agreement for POGO Partners
- Physical Security Measures
- Organizational Security Measures
- Key Tracking Log
- Access Control Card Tracking Log

- Equipment Inventory
- Software Inventory
- Access Levels
- Data Linkage Protocol
- Retention and Destruction of Data
- POGONIS Security Controls and Performance
- Structural Changes to POGONIS Room
- Agreement with Electronic Service Provider

Internal and External Audits

- POGO Privacy Audit Program

Risk Assessment/Disaster Recovery Plan Draft

- Disaster Recovery Plan
- Privacy Crisis Management Protocol

Privacy Impact Assessments

- Privacy Impact Assessment Short Form– Project-Specific for Aggregate Data
- Privacy Impact Assessment Long Form– Project-Specific for all POGO Projects
- Privacy Impact Assessment Logs For Staff and Research Projects

Privacy Complaints

- Internal Privacy Complaint Form
- External Privacy Complaint Form
- Privacy Complaints Log
- Amendment Notification Log

Staff Education

- Staff Education and Training Policy

List of Policies and Procedures

- Access to Records
- Physical/Office Security
- Retention and Destruction of Data
- Privacy Breach
- Confidentiality Agreement
- Disciplinary Action – Privacy Infractions
- Review of Security Policies and Procedures
- Delegation of Roles and Responsibilities
- Staff Education and Training
- Confidentiality and Security of Data
- Ethics Review process
- Document Shredding
- Password
- Levels of Access
- Authorship

Website Pages

- Overview of POGO and Personal Health Information
- POGONIS Data Request Form
- Privacy Brochure
- POGO Privacy and Data Security Code
- POGO Privacy Commitment
- Privacy Officer Contact Information
- External Privacy Complaint Form

Other

- 2003-04 Annual Report
- The Case for a Provincial Chair in Childhood Cancer Control

The IPC requested revisions to some of the above mentioned documentation. The revised documentation was submitted on October 12, 2005.

Site Visit

IPC representatives conducted a site visit at POGO on September 29, 2005.

IPC representatives toured POGO with the Senior Associate, Research & Planning and the Database Administrator and Research Assistant, who serve as co-Privacy Officers. Focused presentations and discussions took place with POGO representatives as follows:

Introduction to POGO	Medical Director
Description of Data Holdings	Database Administrator/Research Assistant
Fundraising	Senior Communications Officer
Physical Building Security	Building Manager
Organizational Security Measures	Senior Associate, Research & Planning, Database Administrator/Research Assistant and Information Security Manager
Technical Security Measures	Database Administrator /Research Assistant, the Vice President, Engineering of Artificial Intelligence in Medicine, and Information Security Manager
Work Flow Procedure Management	Database Administrator/Research Assistant, the Vice President, Engineering of Artificial Intelligence in Medicine, and Information Security Manager

Findings of the Review

Human resources

All staff at POGO (including employees, scientists, adjunct scientists, fellows, students and administrative staff) are required to sign Confidentiality Agreements upon hiring, and thereafter, on an annual basis. In addition, persons affiliated with POGO for business purposes (consultants, visiting scientists, research collaborators, service providers, vendors and contractors) are required to sign Confidentiality Agreements prior to being given access to personal health information.

The Confidentiality Agreement advises the person signing of the consequences of a breach, namely, that a breach of confidentiality may result in discipline for staff up to and including dismissal and, in the case of persons affiliated with POGO for business purposes, may result

in termination of their relationship with POGO. In addition, by signing the Confidentiality Agreement, each person agrees to comply with POGO's privacy and security policies, procedures and practices. However, the Confidentiality Agreement does not reference *PHIPA* or personal health information which is extremely important given POGO's status as a prescribed entity under *PHIPA*. Accordingly, we recommend that the Confidentiality Agreement be amended to contain references to *PHIPA* and personal health information.

At POGO there are clearly defined roles with respect to privacy and confidentiality. The Board of Directors has overall responsibility for privacy matters. The Executive Director of POGO is accountable for operational compliance with POGO privacy policies, procedures and practices and reports to the Board of Directors. The POGO Medical Director assists the Executive Director with privacy matters, reviews project-specific privacy impact assessments, and is a member of a team that investigates and resolves privacy complaints and breaches. A Data Security Committee has been established to oversee, review, recommend and approve POGO privacy policies and procedures.

Two employees have been appointed as Privacy Officers to develop and oversee the day-to-day administration of POGO privacy policies, procedures and practices, to monitor compliance with these privacy policies, procedures and practices, to provide privacy training and orientation and to coordinate investigations of privacy issues, complaints and breaches. POGO also employs an external Privacy Advisor to help resolve or mediate privacy issues and complaints that cannot be addressed internally. The Privacy Advisor reports directly to the Board of Directors.

POGO has an ongoing privacy and security training program. Staff are required to receive privacy orientation prior to commencement of employment and prior to being given access to personal health information. In addition, each member of the staff is provided with a Privacy Brochure and Privacy Handbook. Frequent reminders about privacy are included in communications and media clippings which are provided to staff and researchers. Regular workshops on POGO's policies and procedures are also provided.

It is the IPC's understanding that the privacy and security training program has not yet been fully implemented and that some persons affiliated with POGO have not yet undergone privacy and security training specific to *PHIPA*. The IPC recommends that the training program should be fully implemented as soon as possible.

POGO has agreements with each of the five pediatric hospital partners which govern the disclosure of personal health information to POGO, the use and disclosure of that personal health information by POGO and access by the five pediatric hospitals to the personal health information of their own patients that was disclosed to POGO.

POGO is also in the process of developing agreements with other prescribed entities under section 45 of *PHIPA* for purposes of analysis and compiling statistical information with respect to the management, evaluation, monitoring, planning or allocation of resources for all or part of the health system and agreements with prescribed persons under section 39(1) (c) of *PHIPA* for purposes of facilitating or improving the provision of health care. POGO is also in the

process of developing research agreements for the disclosure of personal health to researchers. It is recommended that these agreements be developed in accordance with the requirements of *PHIPA* and its regulations and be forwarded to the IPC for review and comment prior to the implementation and execution of any such agreements.

POGO also has an agreement with the company that provides the POGONIS Information Management Software to POGO for use at both the head office of POGO and at the five pediatric hospitals, the five satellite clinics and the seven pediatric and adult aftercare programs.

Privacy

POGO has a comprehensive *Privacy and Data Security Code* which is readily available to the public on POGO's website. POGO's Privacy and Confidentiality Statement, privacy brochure and contact information for the Privacy Officers is also posted on the website.

A series of Questions and Answers for the website are also under development that address the collection, use and disclosure of personal health information by POGO and the practices and procedures implemented by POGO to protect the privacy of individuals whose personal health information it collects and to maintain the confidentiality of that information. It is recommended that POGO forward a copy of its proposed Questions and Answers to the IPC for review and comment, prior to posting them on its website.

The *Privacy and Data Security Code* is supplemented with a *Privacy and Data Security Procedure* to operationalize the privacy policies implemented by POGO in relation to such matters as limiting the collection, use and disclosure of personal health information, the retention of personal health information and the safeguards to protect the privacy of individuals whose personal health information it collects and to maintain the confidentiality of that information. The *Privacy and Data Security Code* is also supplemented by a *Privacy and Data Security Handbook* which enables all persons affiliated with POGO (including employees, scientists and students) to become acquainted with the privacy policies, procedures and practices implemented by POGO including the authorized uses and disclosures of personal health information.

POGO has also developed a comprehensive framework for conducting privacy audits. The privacy audit program will consist of three types of reviews: POGO Program Area Privacy Compliance Reviews (Internal), Privacy Compliance Reviews (External) and POGO Privacy Topic Reviews (Internal). The intent of the privacy audit program is to assess compliance with POGO policies, procedures and practices and to demonstrate privacy compliance to health information custodians who disclose personal health information to POGO and the public.

POGO Program Area Compliance Reviews will assess compliance with POGO policies and procedures to identify and address potential issues at the program level. External Privacy Compliance reviews will assess data recipients' compliance with agreements such as Research Agreements and Non-Disclosure/Confidentiality Agreements. POGO Privacy Topic Reviews will select a particular privacy topic and review it across the POGO organization, verifying compliance with appropriate privacy policies, procedures and practices regarding the topic. A three year

schedule for implementing the privacy audit program has been developed. The privacy audit program should be implemented according to this proposed schedule.

POGO has implemented a policy for managing privacy breaches and handling complaints from the public. The privacy breach protocol emphasizes containment of the breach, notification of appropriate persons and implementing or amending policies, procedures or practices to avoid similar privacy breaches in the future. Complaints about POGO's compliance with its privacy policies, procedures and practices are made to the Executive Director who forwards the complaints to the Privacy Officers for investigation. A complaint form has been developed and is available on POGO's website for use by individuals who wish to complain about POGO's compliance with its privacy policies, procedures and practices. It is the Privacy Officers' responsibility to investigate and respond to complaints and to provide the individual with a summary of the nature and scope of the investigation and, if appropriate, the measures implemented to address the complaint.

POGO also has a protocol for undertaking data linkages. When primary research is undertaken, data linkages require the consent of the individual and approval of a research ethics board (REB). Data linkages are carried out by the System Administrator. Once the data is linked, individuals are assigned a unique study number and the master record that links the study number to personal identifiers is stored separately under lock and key. Only encrypted data is used. When research is undertaken with administrative data, all linkages are performed in a secure system. Again, only encrypted data are provided to researchers.

POGO also has processes in place for de-identifying personal health information before use. A limited number of specified individuals at POGO have access to personal health information. All personal identifiers are stripped or encrypted prior to data being used for the day-to-day activities of POGO. Although the IPC was informed that this was POGO's practice, the specific details of this policy were not set out clearly in the documentation provided. The IPC recommends that a formal written policy specifying when, how and by whom personal health information is de-identified should be developed and forwarded to the IPC for review and comment.

In terms of retention and destruction of data, retention schedules are set out on a project-by-project basis. A destruction policy ensures that copies of all datasets are destroyed by researchers once they are no longer needed. POGO has a policy for destroying personal health information on various types of media.

POGO has developed a project-specific privacy impact assessment form. All requests for aggregate data must be accompanied by a project-specific privacy impact assessment form. In addition, all requests for person level data from POGONIS must be accompanied by a more detailed project-specific privacy impact assessment form.

In terms of REB approval, this is not required for the use of the POGONIS anonymized aggregated data. However, when primary data is collected by POGO, institutional and/or university REB approval is sought. In addition, to ensure the privacy of all individuals, the results of all research

projects are reported using aggregated data. Only data with a cell size greater than five are reported to the public.

Security

POGO has implemented a comprehensive security program including physical, technical and administrative measures. Access to the facility and to each office is restricted with keys. Not all members of the staff have a key to enter the facility. Movement of individuals within the facility is controlled with access control cards. Staff is only allowed to access areas that they require access to for purposes specific to their job functions. The POGO office is locked outside of business hours, with access restricted to those with an access control card outside of office hours. The office is monitored with video surveillance, 24 hours a day. The camera is monitored by the Privacy Officers. Access to the room containing POGONIS is restricted to a limited number of designated persons. The building where the POGO office is located is continuously monitored by video surveillance.

In terms of information system security, access to data housed at POGO must be approved by the Executive Director or designate. Access to data is provided on a need-to-know basis. Data media that contain personal identifiers are accessible only to designated persons (i.e., System Administrator and Database Administrator). Access to all systems is controlled with passwords. All passwords are constructed in accordance with a strict policy.

All documents and portable media, which contain personal identifiers, are stored in locked cabinets when not in use. All data are delivered to POGO directly by researchers or by bonded couriers. Data tapes and cartridges are kept in fireproof safes.

Remote users of POGONIS use a dial-up or a virtual private networks (VPN) connection. Access to POGONIS is controlled with user accounts and passwords. Passwords expire after a specified period of time. The POGONIS desktop application automatically shuts down after a specified period of inactivity. Remote users of POGONIS are only permitted to access personal health information relating to patients who received health care within their facility. There is an audit trail of all data inserts, edits and deletes by user account which are checked on a regular basis.

At the start of a project, a POGO Privacy Officer meets with research team members to review precautions and safeguards with respect to confidentiality and security.

The Data Security Committee is responsible for reviewing all privacy and security policies and procedures on an annual basis and amending or creating new policies as required.

Although the security measures that have been implemented by POGO appear to be adequate, one concern that was raised by the IPC is that the measures that have been put in place are not based upon a comprehensive threat and risk assessment (TRA). The IPC recognizes that information security requires ongoing vigilance and a commitment to continuous improvement. Given the volume and sensitivity of the personal health information in the custody or control of POGO, it would be desirable for POGO to adopt a more comprehensive and systemic information

security management program. In this light, we encourage POGO to carry out (preferably by an independent party) a comprehensive, organization-wide threat and risk assessment. Such a threat and risk assessment would help identify all risks, both external and internal, and provide a strong basis for prioritizing those risks and developing an action plan to mitigate them. Recurring threat and risk assessments are also valuable for measuring progress and ensuring continued improvement.

Summary of Recommendations

Major Recommendations

Based on the review of the documentation and the site visit, there are no major recommendations that require rectification or resolution by POGO prior to November 1, 2005.

Other Recommendations

Based on the review of the documentation and the site visit, the IPC is making the following recommendations that POGO is not required to act upon/resolve prior to November 1, 2005:

1. Amend the Confidentiality Agreement to include references to *PHIPA* and personal health information.

2. Ensure that all agents of POGO complete *PHIPA* privacy and security training.

3. Develop a data sharing agreement between POGO and other section 45 entities under *PHIPA* and prescribed persons pursuant to section 39(1) (c) of *PHIPA* that accords with the requirements in *PHIPA* and forward the agreement to the IPC for review and comment prior to the implementation and execution of the agreement.

4. Develop a research agreement for the disclosure of personal health information for research purposes that accords with the requirements of *PHIPA* and its regulations and forward the agreement to the IPC for review and comment prior to the implementation and execution of the agreement.

5. Develop the Questions and Answers about personal health information privacy protection at POGO and forward it to the IPC for review and comment prior to posting on the POGO website.

6. Implement the privacy audit program in accordance with the proposed three year schedule.

7. Develop a formal written policy specifying when, how and by whom personal health information is de-identified and forward the policy to the IPC for review and comment prior to its implementation.

8. Conduct periodic comprehensive threat and risk assessments, with emphasis on both internal and external threats to security.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that POGO has in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Accordingly, effective October 31, 2005, the practices and procedures of POGO have been approved by the IPC.