Information
and Privacy
Commissioner of
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 2008

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Three-Year 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* ("the *Act*") is a consent-based statute, meaning that persons or organizations in the health sector defined as "health information custodians"[1] may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates, subject to limited exceptions where the *Act* permits or requires the collection, use or disclosure to be made without consent. One such disclosure that is permitted without consent is the disclosure of personal health information to prescribed entities pursuant to section 45 of the *Act*.

Statutory Provisions Relating to the Disclosure to Prescribed Entities

Subsection 45(1) of the *Act* permits health information custodians to disclose personal health information to a prescribed entity, without consent, 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. The following entities, including registries maintained within these entities, have been prescribed for purposes of subsection 45(1) of the *Act*:

- Cancer Care Ontario;
- Canadian Institute for Health Information;
- Institute for Clinical Evaluative Sciences; and
- Pediatric Oncology Group of Ontario.

In order for a health information custodian to be permitted to disclose personal health information to a prescribed entity without consent, the prescribed entity must have in place practices and procedures approved by the Information and Privacy Commissioner/Ontario ("IPC") to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information pursuant to subsection 45(3) of the *Act*.

These practices and procedures must also be reviewed by the IPC every three years from the date of their initial approval, pursuant to subsection 45(4) of the *Act*, in order for a health information custodian to be able to continue to disclose personal health information to a prescribed entity without consent, and in order for a prescribed entity to be able to continue to collect, use and disclose personal health information without consent as permitted by the *Act*.

1 Persons or organizations described in subsection 3(1) of the *Act* that have custody or control of personal health information as a result of or in connection with performing the powers, duties or work of the person or organization.

Initial Review of the Practices and Procedures of the Prescribed Entities

In 2005, the IPC reviewed the practices and procedures implemented by each of the prescribed entities to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information. Following this review, the IPC approved the practices and procedures of each of the prescribed entities effective October 31, 2005.

While the IPC was satisfied that the prescribed entities had practices and procedures in place that sufficiently protected the privacy of individuals whose personal health information they received and sufficiently protected the confidentiality of that information, the IPC did make certain recommendations to further enhance these practices and procedures. The recommendations made during the initial review of the Pediatric Oncology Group of Ontario, which were the subject of an earlier report of the IPC and which are set out in Appendix "A" to this report, have all since been addressed by the Pediatric Oncology Group of Ontario.

Three-Year Review of the Practices and Procedures of the Prescribed Entities

Subsection 45(4) of the *Act* requires the IPC to review the practices and procedures implemented by each of the prescribed entities every three years from the date that they were initially approved by the IPC, being October 31, 2005, and to advise whether the prescribed entities continue to meet the requirements of the *Act*. As a result, the IPC was again required to review the practices and procedures implemented by the prescribed entities and to advise whether they continued to meet the requirements of the *Act* on or before October 31, 2008.

Process Followed for the Three-Year Review

By letter dated January 28, 2008, the Assistant Commissioner for Personal Health Information requested each prescribed entity to forward certain documentation to the IPC, set out in Appendix "B" to this report, to enable the IPC to commence its review of the practices and procedures implemented to protect the privacy of individuals whose personal health information is received and to protect the confidentiality of that information. Upon receipt, the requested documentation was reviewed by the IPC and additional documentation and necessary clarifications were requested. The Pediatric Oncology Group of Ontario submitted the requested documentation on May 12, 2008, and submitted additional documentation on June 24, 2008.

Once the additional documentation and necessary clarifications were received, an on-site meeting was held to discuss the practices and procedures implemented by the prescribed entity and to provide the IPC with an opportunity to ask questions arising from the documentation. The on-site meeting with the Pediatric Oncology Group of Ontario was held on July 3, 2008.

Following the on-site meeting, each prescribed entity was informed of the action that it was required to take prior to the continued approval of its practices and procedures. Once all necessary action was taken, the IPC prepared a draft report. The draft report was submitted to the prescribed entity for review and comment prior to the report being finalized and posted on the IPC website.

It must be emphasized that the review by the IPC was limited to personal health information collected, used and disclosed by the prescribed entity pursuant to its function as a prescribed entity under section 45 of the *Act* and not with respect to any other role or responsibility that the prescribed entity may have assumed under the *Act*.

Description of the Pediatric Oncology Group of Ontario

The Pediatric Oncology Group of Ontario ("POGO") is a not-for-profit, multi-disciplinary, multi-centre collaboration of health professionals representing the pediatric programs that treat children with cancer in the Province of Ontario. POGO was established in 1983 to improve the circumstances of children with cancer, as well as their families and caregivers, through the development and implementation of an accessible and well integrated childhood cancer system.

In 1995, POGO became the principal advisor to the Ministry of Health and Long-Term Care on matters relating to childhood cancer care and control in the Province of Ontario. In this capacity, POGO plans for pediatric oncology needs, coordinates the allocation of funding, maintains the provincial pediatric oncology database known as POGONIS, conducts analyses focusing on childhood cancer and develops evidence-based standards and guidelines for childhood cancer care.

Three-Year Review of the Pediatric Oncology Group of Ontario

1. Privacy and Security Governance and Accountability Framework

The Executive Director of POGO, who reports directly to the Board of Directors, is ultimately accountable for ensuring that POGO complies with the *Act* and with the privacy and security policies, procedures and practices implemented. The Executive Director is also responsible for updating the Board of Directors on privacy and security matters on an annual basis or more often as required.

Day-to-day responsibility for managing the privacy program and for protecting the confidentiality and security of personal health information has been delegated to two Privacy Officers who report directly to the Executive Director. The Privacy Officers are responsible for developing, implementing, reviewing and ensuring adherence to the privacy and security policies, procedures and practices implemented and for ensuring compliance with the *Act*. The Privacy Officers are

also responsible for developing and delivering privacy training; for fostering privacy awareness; for conducting privacy audits; for ensuring the execution of confidentiality, data sharing and researcher agreements; and for documenting, investigating and remediating privacy complaints and breaches.

POGO has also established a Data Security Committee that is comprised of senior members of POGO including the Executive Director, Medical Director, Privacy Officers and Information Security Manager. The Data Security Committee is responsible for overseeing, reviewing, recommending and approving the creation of new privacy and security policies, procedures and practices and for recommending, reviewing and approving amendments to existing privacy and security policies, procedures and practices.

2. Overview of Privacy and Security Policies and Procedures

POGO has developed a privacy policy, the *Privacy and Data Security Code*, which describes the status of POGO as a prescribed entity under the *Act* and the obligations that arise from this status. The *Privacy and Data Security Code* further sets out the purposes for which POGO collects, uses and discloses personal health information and the accountability framework for ensuring compliance with the *Act* and for ensuring adherence to the privacy and security policies, procedures and practices implemented. POGO has also implemented numerous privacy and security policies and procedures that support the *Privacy and Data Security Code*.

Pursuant to the *Review of Policies and Procedures Policy*, all these privacy and security policies and procedures must be reviewed on an annual basis by both the Privacy Officers and the Data Security Committee. In the event that amendments are required, these amendments must be made by the Privacy Officers and the amended policies and procedures must be forwarded to the Data Security Committee for approval prior to implementation.

Privacy Breach Policy

POGO has developed and implemented a *Privacy Breach Policy* to address the discovery, containment, notification, investigation and remediation of information breaches. An information breach is defined as the collection, retention, use or disclosure of personal health information in contravention of the *Act*, in violation of the privacy and security policies and procedures implemented by POGO or in breach of the *Confidentiality and Non Disclosure Agreement* that must be signed by all persons affiliated with POGO.

The *Privacy Breach Policy* requires every person that discovers an information breach to commence the containment process and to notify his or her program manager and the Privacy Officers of the information breach. However, it is unclear what information with respect to the information breach must be reported to the program manager and the Privacy Officers and the format in which it must be reported. It is recommended that this be clarified in the *Privacy Breach Policy*.

The Privacy Officers are then responsible for notifying other members of the Breach Team, including the Executive Directive and Medical Director. The Breach Team will then determine the extent of the information breach, determine the process for notification, determine when notification will be undertaken, undertake notification and determine whether an internal information breach should be documented. It is unclear in what circumstances an internal information breach will not be documented. Documentation of an information breach is critically important for both managing information breaches and for preventing similar breaches in future. It is therefore recommended that the *Privacy Breach Policy* be amended to require that all information breaches be documented.

The *Privacy Breach Policy* further requires POGO to notify its Board of Directors and the Ministry of Health and Long-Term Care of an information breach. It is recommended that the *Privacy Breach Policy* also require that the health information custodian who disclosed the personal health information to POGO be notified of an information breach in order that the health information custodian may notify the individuals to whom the personal health information relates, when required pursuant to subsection 12(2) of the *Act*. Currently, the *Privacy Breach Policy* states that the health information custodian will only be notified "if required."

The *Privacy Breach Policy* further requires that an investigation of the information breach be conducted and that following the investigation, that recommendations be made to prevent a similar information breach in future. In particular, the *Privacy Breach Policy* states that in the event of an external information breach, one of the recommendations may include amendments to existing policies and procedures. It is unclear why this recommendation is limited to external information breaches. An internal information breach may nonetheless require amendments to policies and procedures in order to prevent a similar information breach in future and therefore it is recommended that the *Privacy Breach Policy* be amended accordingly.

Disciplinary Action – Privacy Infractions Policy

POGO has implemented a policy, the *Disciplinary Action - Privacy Infractions Policy*, to address discipline in the event of an information breach, including the procedures to be followed and the criteria to be used in determining appropriate disciplinary action.

The *Disciplinary Action - Privacy Infractions Policy*, however, uses inconsistent terminology to describe the information breach. At times it is referred to as a "privacy infraction/breach," at other times it is referred to as a "privacy infringement/breach" and still at other times it is referred to as a "breach/conflict/privacy infringement." It is recommended that one consistent term be used throughout the *Disciplinary Action - Privacy Infractions Policy* and that the term selected and the definition adopted be consistent with the term and definition adopted in the *Privacy Breach Policy*.

The *Disciplinary Action - Privacy Infractions Policy* also "encourages" agents to report information breaches. It is recommended that the *Disciplinary Action - Privacy Infractions Policy* be amended to impose a mandatory obligation on all agents to report information breaches or suspected

information breaches to the Privacy Officers in order to ensure that information breaches are contained, investigated and remediated in a timely manner.

Policy and Procedure for De-Identification

POGO has developed and implemented a policy and procedure with respect to the de-identification of personal health information, the *De-Identifying Personal Health Information Policy*, which identifies the information that must be removed and/or truncated in order to de-identify personal health information and that identifies by whom the de-identification will be performed. However, this policy does not address the circumstances when POGO requires that de-identified information be used and the circumstances when the use of personal health information is permitted.

It is recommended that the *De-Identifying Personal Health Information Policy* be amended to require, consistent with the actual practices of POGO, that de-identified information be used for analysis and compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the childhood cancer system pursuant to its function as a prescribed entity under section 45 of the *Act*. It is further recommended that the information that must be removed, encrypted and/or truncated in order to de-identify personal health information and the process used to de-identify personal health information be described.

It is also recommended that the *De-Identifying Personal Health Information Policy* be amended to set out those circumstances, aside from analysis and compiling statistical information for the childhood cancer system pursuant to section 45 of the *Act*, when POGO requires that de-identified information be used and the circumstances when the use of personal health information is permitted and to outline the information that must be removed, encrypted and/or truncated and the process that must be followed in de-identifying personal health information in these circumstances.

Policies Related to the Transmission of Personal Health Information

POGO has developed and implemented an *E-Mail Policy* and a *Secured Faxes (Containing Personal Health Information/Confidential Information) Policy* to outline its expectations relating to the acceptable use of e-mail and facsimile transmissions and to describe the policies, procedures and practices that apply to these transmissions.

However, while the purpose of the *E-mail Policy* is to outline the acceptable use of e-mail and to outline those circumstances where the use of e-mail is not acceptable, the *E-mail Policy* does not address whether or not personal health information may be collected, used or disclosed by e-mail transmission. It is recommended that this be addressed. Further, in the event that personal health information is permitted to be collected, used and disclosed by e-mail transmission, which appears to be the case based on the *Encryption Policy* implemented by POGO, it is recommended that the *E-mail Policy* be amended to require that the personal health information be encrypted,

consistent with Order HO-004 issued by the IPC and consistent with the *Encryption Policy* implemented by POGO.

Further, with respect to the *Secured Faxes (Containing Personal Health Information/Confidential Information) Policy*, while the policy addresses the receipt and distribution of facsimile transmissions containing personal health information and establishes safeguards and standard operating procedures in this regard, such as the designation of a machine in a secure area that is not generally accessible to receive incoming facsimile transmissions and the designation of individuals who are responsible for handling incoming facsimile transmissions, it does not address whether or not personal health information may be disclosed by facsimile transmission.

It is recommended that the *Secured Faxes (Containing Personal Health Information/Confidential Information) Policy* be amended to address whether personal health information may be disclosed by facsimile transmission and if it is permitted, to stipulate when such information may be disclosed by facsimile transmission and the safeguards and standard operating procedures that must be implemented to protect personal health information from unauthorized disclosure. In adopting safeguards and standard operating procedures, it is recommended that POGO have regard to the *Guidelines on Facsimile Transmission Security* produced by the IPC.

3. Information Available Related to Privacy and Security Policies and Procedures

POGO makes information about its privacy and security policies, procedures and practices readily available on its website, **www.pogo.ca**, including the *Privacy and Data Security Code,* a brochure entitled *Pediatric Oncology Group of Ontario Privacy Statement*, Frequently Asked Questions entitled *Frequently-Asked Questions and Answers About Information Privacy Protection at POGO* and contact information for the individuals responsible for ensuring compliance with these policies, procedures and practices and to whom complaints or inquiries can be made. Privacy and security policies and procedures are also made readily available to staff on a centralized intranet resource.

Currently, the information made available to the public, staff and other stakeholders does not clearly distinguish between POGO's collection and use of personal health information pursuant to its function as a prescribed entity under section 45 of the *Act* and its collection and use of personal health information for research purposes pursuant to section 44 of the *Act*. The failure to clearly distinguish between the purposes for which POGO collects and uses personal health information leads to a lack of clarity as to the policies, procedures and practices and the statutory conditions that apply to the collection and use of the personal health information.

For example, if the purpose of the collection or use of personal health information is research, the *Act* requires POGO to prepare a research plan that meets the requirements of the *Act* and its regulation and to obtain research ethics board approval of the research plan. It further requires, where personal health information is being collected for research purposes, that an agreement be entered into with the health information custodian, the prescribed person pursuant to subsection

39(1)(c) of the *Act* or the other prescribed entity pursuant to section 45 of the *Act* from which the personal health information will be collected.

It is recommended that POGO develop and implement a policy to set out the criteria that will be used by POGO in deciding when a collection or use of personal health information is for research purposes pursuant to section 44 of the *Act* and when a collection or use of personal health information is for purposes of analysis or compiling statistical information with respect to the childhood cancer system pursuant to its function as a prescribed entity under section 45 of the *Act*. It is further recommended that the policy outline the policies, procedures and practices and the statutory conditions that apply in each context.

It is also recommended that all information made available to the public and stakeholders be amended to clearly set out the purposes for which POGO is collecting and using personal health information, the statutory authority for such collection and use and the policies, procedures and practices and the statutory conditions that apply to the collection and use of the personal health information. This information should further be amended to clearly distinguish between POGO's collection and use of personal health information pursuant to its function as a prescribed entity under section 45 of the *Act* and its collection and use of personal health information for research pursuant to section 44 of the *Act*.

4. Collection, Use and Disclosure of Personal Health Information

Collection

In respect of its function as a prescribed entity pursuant to section 45 of the *Act*, POGO collects personal health information from the five specialized pediatric cancer centres in the Province of Ontario: The Hospital for Sick Children, McMaster Children's Hospital, Kingston General Hospital, the Children's Hospital of Eastern Ontario and the Children's Hospital of Western Ontario.

It also collects personal health information from the six community hospitals that operate "satellite programs" to provide pediatric cancer care closer to the homes of children with cancer and from the seven aftercare clinics that follow up with survivors of childhood cancer in order to identify and address the long term effects of childhood cancer and its treatment. Personal health information is also collected from other entities prescribed pursuant to section 45 of the *Act*.

The personal health information collected includes demographic, diagnosis, treatment and death information for all childhood cancer in the Province of Ontario and the late effects of cancer and its treatment. The demographic information collected includes the full name, address, postal code, date of birth, gender and health card number of the individual. The diagnosis information collected includes cancer type, date of diagnosis and histology information. The treatment information collected includes the type of treatment and the date and place of treatment. Finally, the death information collected includes the date of death and the cause and location of death.

The personal health information collected is retained in the Pediatric Oncology Group of Ontario Networked Information System, also known as POGONIS.

Use

Personal health information collected for purposes of its function as a prescribed entity under section 45 of the *Act* is de-identified prior to its use by removing personal identifiers such as name, address and health card number and by inserting an identifier, known as the POGO identification number. Personal health information is de-identified by one of three individuals who have access to personal health information for purposes of removing personal identifiers, for purposes of inserting the POGO identification number and for purposes of record linkage.

This de-identified information is then used by POGO for purposes of analysis and compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the childhood cancer system pursuant to section 45 of the *Act*. In particular, the de-identified information is used for the purposes of:

- Analyzing demographics, incidence, prevalence and epidemiology of childhood cancer;
- Identifying trends and the long-term effects of childhood cancer and its treatment;
- Developing evidence based standards and guidelines for childhood cancer care;
- Identifying gaps in the delivery of cancer care services; and
- Developing, planning, implementing and evaluating new treatment programs.

With respect to research, POGO either uses personal health information or de-identified information for research purposes, depending on the nature of the research undertaken. Where de-identified information is used, personal identifiers such as name, address and health card number are removed and a unique study number is inserted. The master record that links the study number to the personal identifiers is stored separately from the de-identified information.

POGO has advised that prior to any collection or use of personal health information for research purposes and prior to any use of de-identified information for research purposes, POGO requires that a written research plan be prepared in accordance with the requirements of the *Act* and its regulation, that a *Project-Specified Privacy Impact Assessment Form* be completed and that the research plan be approved by its Research Steering Committee as well as by a research ethics board.

POGO has implemented an *Ethics Review Process Policy* that requires all research undertaken by POGO to receive research ethics board approval. However, the *Ethics Review Process Policy* does not address the other statutory requirements that must be satisfied prior to the use of personal health information for research purposes, namely the requirement to prepare a research plan in compliance with the *Act* and its regulation. It also does not address the other conditions that a researcher who uses personal health information is required to adhere to pursuant to subsection 44(6) of the *Act*. These requirements are not addressed in any other policy

or procedure implemented by POGO, although adherence to these requirements is consistent with the actual practices of POGO.

It is recommended that the *Ethics Review Process Policy* be amended to address all the requirements in the *Act* and its regulation that must be satisfied prior to the use of personal health information for research purposes and that must be adhered to in using personal health information for research purposes. It should also be amended to ensure consistency with the actual practices of POGO. In particular, the *Ethics Review Process Policy* should state that prior to using personal health information and de-identified information for research purposes, POGO requires that a *Project-Specified Privacy Impact Assessment Form* be completed and that the research plan be approved by the Research Steering Committee of POGO in addition to satisfying the requirements in the *Act* and its regulation. The *Ethics Review Process Policy* should also be amended to set out the circumstances in which personal health information is used for research purposes and the circumstances in which de-identified information is used for research purposes.

Disclosure

POGO discloses personal health information in a number of circumstances where the disclosure is permitted or required by law, including in the circumstances set out below.

Personal health information is disclosed to the health information custodians who provided the personal health information to POGO, provided it does not contain any additional identifying information, and to other prescribed entities pursuant to section 45 of the *Act* for the purpose of analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the health system. In addition, personal health information is disclosed for research purposes.

Prior to the disclosure of personal health information for research purposes, POGO advised that it requires the researcher to submit a written application, a copy of a 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 research plan. POGO indicated that it also requires the researcher to complete a *Project-Specified Privacy Impact Assessment Form*.

The research plan and *Project-Specified Privacy Impact Assessment Form* must be reviewed and approved by the Research Steering Committee prior to any disclosure for research purposes. If the Research Steering Committee approves the disclosure, POGO stated that it requires the researcher to execute both a *Researcher Agreement* and a *Confidentiality and Non Disclosure Agreement*.

It is recommended that the *Ethics Review Process Policy*, which currently only addresses the use of personal health information for research purposes, be amended to address the disclosure of personal health information for research purposes. In particular, it is recommended that the *Ethics Review Process Policy* be amended to address all the statutory requirements that must be satisfied prior to the disclosure of personal health information for research purposes, as well

as all the other conditions that POGO imposes prior to any such disclosure of personal health information.

5. Retention and Destruction of Personal Health Information

POGO retains records of personal health information collected pursuant to its function as a prescribed entity under section 45 of the *Act* for long-term analysis, subject to the terms and conditions in *Data Sharing Agreements* entered into with health information custodians or other prescribed entities from which the personal health information was collected. Records of personal health information collected by POGO for research purposes are retained for as long as necessary to fulfill the purposes for which it is collected, as set out in the *Project Specified Privacy Impact Assessment Form* and the research plan approved by the research ethics board.

Destruction of Records of Personal Health Information

POGO has developed and implemented a *Document Shredding Policy* that requires all confidential information in paper format, including records of personal health information in paper format, to be destroyed by shredding. The type of shredding employed is crosscut shredding. POGO has also developed and implemented a *Retention and Destruction of Data Policy* which requires that all records of personal health information in electronic format, such as CD, DVD, magnetic tape or floppy diskette, be physically destroyed thereby rendering the media unusable.

Tracking Dates of Destruction

The *Retention and Destruction of Data Policy* requires that the destruction dates of records of personal health information collected by POGO for research purposes, as set out in the *Project Specified Privacy Impact Assessment Form* and the research plan approved by the research ethics board, be tracked in the POGO Research Unit Research Database.

The Database Administrator is responsible for monitoring the destruction dates, for generating a report every three months to flag pending destruction dates, for notifying the principal investigator of the pending destruction date and for requesting the principal investigator to sign a document attesting to destruction. The Database Administrator is also responsible for generating a report that will be provided to the Privacy Officers and the Information Security Manager if the destruction date has passed without the principal investigator "signing off" on destruction. The Privacy Officers and the Information Security Manager are then responsible for following up with the principal investigator and for destroying the information within one week of the report.

The *Retention and Destruction of Data Policy* however, does not set out the required content of the document attesting to destruction that must be signed by the principal investigator. It is recommended that the *Retention and Destruction of Data Policy* be amended to stipulate the required content of the document attesting to destruction that must be executed, and at a minimum, that this content include the date, time, location and method of secure destruction employed.

Further, the *Retention and Destruction of Data Policy* requires the Information Security Manager to generate a yearly report from the POGO Research Unit Research Database that lists the destruction dates of all records of personal health information collected by POGO for research purposes and requires the Information Security Manager to compare this report to back up tapes on file in order to verify that all backup tapes containing that information have been destroyed.

6. Administrative Safeguards Implemented

In addition to privacy and security policies and procedures, POGO has implemented the following administrative safeguards to protect personal health information against theft, loss and unauthorized use, disclosure, copying, modification or disposal.

Privacy and Security Training

POGO has implemented a *Staff Education and Training Policy* that requires all new staff and affiliates, including scientists, fellows and students, to receive privacy orientation. Privacy orientation is provided by the Privacy Officers and is recorded in a *Staff Education and Training Log*. The privacy orientation includes an overview of the privacy program, discusses the privacy policy implemented and discusses the responsibilities of staff and affiliates in the event of a breach.

With respect to ongoing training, the *Staff Education and Training Policy* states that the Privacy Officers will conduct "regular" workshops for staff regarding the application of the policies and procedures implemented. The meaning of "regular" is not defined, although from a review of the documentation submitted for purposes of this review, it appears that two such workshops are conducted each year in the form of an agenda item at staff meetings.

It is unclear however, when the initial privacy orientation is provided, namely whether it is provided prior to being given access to personal health information, and the consequences for failing to attend. It is further unclear whether the orientation is limited to privacy orientation or whether it also includes security orientation. In addition, with respect to the ongoing training, it is unclear whether the ongoing training includes both privacy and security training, whether attendance is mandatory, how POGO keeps track of attendance, who is responsible for tracking attendance and the consequences for failing to attend. The frequency of the ongoing training is also not documented.

It is recommended that POGO amend the *Staff Education and Training Policy* to encompass both privacy and security orientation for new staff and affiliates, as well as ongoing privacy and security training. In particular, it is recommended that the *Staff Education and Training Policy* be amended to set out when the initial privacy and security orientation will be provided, namely prior to being given access to personal health information, and the frequency of the ongoing privacy and security training. It is further recommended that the *Staff Education and Training Policy* be amended to emphasize that attendance at the initial privacy and security orientation, as well as ongoing privacy and security training, is mandatory and to describe the process that

will be used to track attendance, including who will track attendance and the consequences for failing to attend.

It is also recommended that the initial privacy and security orientation be expanded to explain the:

- Status of POGO under the *Act* and its regulation and the obligations that arise therefrom;
- Terms "personal health information," "health information custodian," and "prescribed entity" and their relevance in the context of POGO;
- Privacy and security policies and procedures implemented by POGO and the obligations imposed on staff and affiliates as a result of these policies and procedures;
- Provisions in the *Confidentiality and Non Disclosure Agreement*, including the provisions requiring staff and affiliates to familiarize themselves with and to comply with the privacy and security policies and procedures implemented;
- Responsibilities imposed on staff and affiliates by the *Privacy Breach Policy* to identify, notify appropriate individuals at POGO of, and contain an information breach;
- The roles and responsibilities of the Privacy Officers; and
- The physical, administrative and technical safeguards implemented by POGO, including the responsibilities of staff and affiliates in implementing these safeguards.

With respect to ongoing privacy and security training, it is recommended that the ongoing privacy and security training be formalized and that it include role-based training in order to ensure that staff understand how to apply the privacy and security policies, procedures and practices in their day-to-day work. It is also recommended that the ongoing training address any new privacy and security policies, procedures and practices implemented by POGO and address significant amendments to existing privacy and security policies, procedures and practices.

Confidentiality Agreements

The *Confidentiality Agreement Policy* requires every person affiliated with POGO, including employees, scientists, fellows, students, consultants and contractors, to sign a *Confidentiality and Non Disclosure Agreement* upon the commencement of the relationship with POGO, and prior to being given access to personal health information, and thereafter on an annual basis. The Privacy Officers are responsible for ensuring that every person affiliated with POGO executes a *Confidentiality and Non Disclosure Agreement* and for tracking execution of these agreements through the *Confidentiality and Non Disclosure Agreement Form Log*.

By signing the *Confidentiality and Non Disclosure Agreement*, all persons affiliated with POGO agree to comply with the privacy and security policies and procedures implemented by POGO and to comply with all applicable privacy legislation, including the *Act*. They further agree

not to use confidential information, including personal health information, except as necessary to perform their functions and to not disclose confidential information except as required by law. They also undertake to use reasonable measures to safeguard confidential information against theft, loss and unauthorized collection, use, disclosure, modification or disposal and to promptly notify POGO upon becoming aware of a breach of the *Confidentiality and Non Disclosure Agreement*.

Data Sharing Agreements

POGO has entered into a *Data Sharing Agreement* with each of the five specialized pediatric cancer centres from which it collects personal health information. The *Data Sharing Agreement* limits the uses and disclosures that can be made of the personal health information by POGO, outlines the administrative, technical and physical measures that will be implemented by POGO to safeguard the personal health information and requires POGO to notify the centres in the event of an information breach. POGO has not entered into a *Data Sharing Agreement* with the six community hospitals that operate "satellite programs" or the seven aftercare clinics that provide care and services to survivors of childhood cancer and from which POGO also collects personal health information. It is recommended that POGO enter into a *Data Sharing Agreement* with these hospitals and clinics.

POGO also enters into a *Data Sharing Agreement* with other entities prescribed pursuant to section 45 of the *Act* prior to collecting personal health information from, or disclosing personal health information to, the other prescribed entity. Currently, POGO has entered into a data sharing agreement with the Institute for Clinical Evaluative Sciences and Cancer Care Ontario.

It is recommended that the *Data Sharing Agreement* with other entities prescribed pursuant to section 45 of the *Act*, be amended to clearly set out the purpose of the collection of personal health information by POGO or the disclosure of personal health information by POGO, as the case may be. In particular, the *Data Sharing Agreement* should set out whether the personal health information that will be collected or disclosed by POGO, as the case may be, is being collected or disclosed for research purposes pursuant to section 44 of the *Act* or for the purpose of analysis or compiling statistical information with respect to the health system pursuant to section 45 of the *Act*.

If the purpose of the collection or disclosure of personal health information is research, the *Data Sharing Agreement* should evidence that a research plan has been prepared in compliance with the *Act* and its regulation and that a research ethics board has approved the research plan. It should also address the conditions or restrictions imposed with respect to the use, security, disclosure, return or disposal of the personal health information in accordance with subsection 44(5) of the *Act* and the obligations imposed on researchers pursuant to subsection 44(6) of the *Act*.

The *Data Sharing Agreement* should also require that the records of personal health information either be returned in a secure manner and to stipulate the secure manner in which the records of personal health information must be returned or to require that the records of personal health

information be destroyed in a secure manner when the terms of the *Data Sharing Agreement* require the records to be returned or destroyed. Further, with respect to secure destruction, the *Data Sharing Agreement* should provide a definition of secure destruction consistent with subsection 1(5.1) of Regulation 329/04 to the *Act* and require that a certificate of destruction be provided setting out the date, time, location and method of secure destruction employed and bearing the signature of the person who performed the secure destruction.

Procedures and Practices With Respect to Research

Prior to any use or disclosure of personal health information for research purposes, POGO requires that a written research plan be prepared in compliance with the *Act* and its regulation, that a *Project-Specified Privacy Impact Assessment Form* be completed and that the research plan be reviewed and approved by the POGO Research Steering Committee and a research ethics board. Further, prior to the disclosure of personal health information for research purposes, POGO requires that a *Researcher Agreement* and a *Confidentiality and Non Disclosure Agreement* be executed.

The *Project-Specified Privacy Impact Assessment Form* was developed by POGO in order to ensure that the researcher, through the completion of the *Project-Specified Privacy Impact Assessment Form*, addresses all the requirements in the *Act* and its regulation that must be satisfied prior to the use or disclosure of personal health information for research purposes. However, the *Project-Specified Privacy Impact Assessment Form* does not appear to address all the required content of research plans in section 16 of Regulation 329/04 to the *Act*, in particular it does not set out:

- An explanation as to why the research cannot reasonably be accomplished without the personal health information (section 16(4) of Regulation 329/04);
- An explanation as to why consent to the disclosure of the personal health information is not being sought from the individual to whom the personal health information relates (section 16(6) of Regulation 329/04); and
- Whether the researcher has applied for the approval of another research ethics board and if so, the response to or status of the application (section 16(11) of Regulation 329/04).

It is therefore recommended that the *Project-Specified Privacy Impact Assessment Form* be amended to reflect the requirements for research plans in section 44 of the *Act* and its regulation.

The *Researcher Agreement*, which must be executed prior to any disclosure of personal health information for research purposes, outlines the conditions and restrictions imposed by POGO with respect to the use, security, disclosure, return or disposal of personal health information. It is recommended that the *Researcher Agreement* be amended, as set out below, to ensure uniformity in the terminology used, to ensure that the terminology used is consistent with the *Act*, to ensure that personal health information is transferred to the researcher in a secure manner and to require the researcher to return or dispose of the personal health information in a secure manner on or before the date set out in the research plan.

Article 1, which sets out the definitions for terms that will be used in the *Researcher Agreement*, contains a definition of the term "personal health information" yet the remainder of the *Researcher Agreement* does not use the term "personal health information" but rather "PHI," which is not a defined term. Article 1 also defines "REB" as having the meaning set out in the *Act* yet the acronym "REB" does not appear in the *Act*. It also provides a definition of "applicable law" which does not refer to the *Act* and its regulation. It is recommended that the *Researcher Agreement* be amended to consistently use the term "personal health information," to use the term "research ethics board" and to define the term in a manner consistent with the definition in the *Act* and to amend the definition of "applicable law" to include the *Act* and its regulation.

Further, Article 3.3 of the *Researcher Agreement* states that POGO will provide personal health information to the researcher according to the method, mode and frequency agreed to in writing. It is recommended that Article 3.3 explicitly state that the personal health information will be provided to the researcher in a secure manner and to set out the secure manner in which the personal health information will be provided to the researcher.

It is also recommended that Article 4 of the *Researcher Agreement*, which deals with the restrictions or conditions imposed on a researcher with respect to the use, security, disclosure, return or disposal of personal health information be amended in the following respects.

It is recommended that Article 4 be amended to require the researcher not to make contact or attempt to make contact, either directly or indirectly, with the individual to whom the personal health information relates and to comply with the conditions specified by the research ethics board when personal health information is being disclosed for research purposes without consent. Such an amendment is required in order to ensure consistency with subsections 44(6)(a) and (e) of the *Act*.

Articles 4.2(b) and 4.2(j) of the *Researcher Agreement* permit a researcher to use and disclose personal health information collected for research purposes for purposes other than the research purposes, when the use or disclosure is permitted by the privacy policy implemented by POGO or otherwise permitted in writing by POGO. It is recommended that Articles 4.2(b) and 4.2(j) be amended to ensure consistency with subsections 44(6)(b) and (d) of the *Act*, which only permit a researcher to use personal health information for the purposes set out in the research plan approved by the research ethics board and to disclose personal health information where required by law.

In addition, it is recommended that Article 4.4 of the *Researcher Agreement*, which requires the researcher to either return or dispose of the personal health information "when it is no longer required for research purposes," be amended to require the researcher to either return or dispose of the personal health information in accordance with the *Project-Specified Privacy Impact Assessment Form* and the research plan approved by the research ethics board.

It is also recommended that Article 4.4 be amended to provide that if the researcher elects to return the personal health information, that it must be returned in a secure manner and to set out the secure manner in which the personal health information must be returned. If, on the other

hand, the researcher elects to dispose of the personal health information, it is recommended that Article 4.4 explicitly state that the personal health information must be destroyed in a secure manner, to provide a definition of secure destruction consistent with subsection 1(5.1) of Regulation 329/04 to the *Act* and to require the researcher to provide a certificate of destruction setting out the date, time, location and method of secure destruction employed and bearing the signature of the researcher.

Privacy Audit Program

POGO has implemented a privacy audit program that includes three types of audits: program area privacy compliance audits, privacy topic audits and external privacy compliance audits. Each of these audits and the procedure used in conducting these audits, are described in a document entitled the *POGO Privacy Audit Program*. The Privacy Officers are responsible for conducting the privacy audits, for preparing a report that is presented to the Data Security Committee and for summarizing the reports into an *Annual Privacy Audit Program Report* for presentation to the Board of Directors.

Program area privacy compliance audits assess the compliance of a program area with the privacy policy implemented by POGO, namely, the *Privacy and Data Security Code*. In selecting program areas for audit, priority is given to those program areas that hold particularly sensitive personal health information. The Pediatric Oncology Group of Ontario Networked Information System, also known as POGONIS, is subject to a program area privacy compliance audit on an annual basis.

Privacy topic audits involve the review of a particular topic across the organization to verify compliance with the *Privacy and Data Security Code*. In selecting activities for privacy topic audits, priority is given to those activities determined to be high-risk in terms of protecting the privacy of individuals whose personal health information is received. A minimum of one privacy topic audit is conducted on annual basis. To date, privacy topic audits have been conducted on small cell suppression, data linkage policies, third party agreements and the *Privacy Breach Policy*.

External privacy compliance audits assess the compliance of a recipient of personal health information with the terms and conditions of the *Confidentiality and Non Disclosure Agreement* and *Researcher Agreement*. On an annual basis, the Privacy Officers randomly select ten percent of recipients for purposes of such an audit. In conducting external privacy audits, priority is given to the sensitivity and amount of personal health information provided and to whether personal health information will be used to link to other information.

Based on the *POGO Privacy Audit Program* document, it appears that the program area privacy compliance audits and privacy topic audits only assess compliance with the privacy policy implemented by POGO, the *Privacy and Data Security Code.* It is recommended that the *POGO Privacy Audit Program* be amended to expand the audit program to assess compliance with all privacy policies and procedures implemented by POGO, and not simply the *Privacy and Data Security Code*, in order to ensure a more robust privacy audit program.

Security Audit Program

POGO conducts a number of security audits including reviews of access rights to data holdings containing personal health information, reviews of audit logs and threat and risk assessments.

Access to data holdings, including data holdings containing personal health information, is monitored by the Database Administrator in collaboration with the Information Security Manager. A record of staff members that have access to each data holding is maintained, including the level of access, and this is reviewed on an annual basis to determine whether access rights should be terminated, for example, when it is no longer required or the relationship with POGO has ended.

Further, all access to systems containing personal health information are recorded in a log that includes the date and time of login, the login account name and the date and time of sign-out. An audit log is also maintained of the date and time of all inserts, edits and deletions, the name of the user account that performed the action and a record of the field value changes relating to the action.

These security reviews, however, are not consolidated in one document that sets out the process for conducting each of these reviews, the mechanism and format for reporting the findings of each review, to whom the findings of the review are reported and the procedure used in tracking the findings of the review and whether these findings were addressed. It is recommended that POGO develop and implement a security audit program policy and procedure that sets out the types of security audits that will be conducted, the frequency of each audit, the procedure used in conducting each audit, the person responsible for conducting each audit, the mechanism and format for reporting the findings of the audit, to whom the findings will be reported and the procedure to track the findings of the audit and how each finding was addressed.

7. Physical Safeguards Implemented

POGO is located in a locked facility with twenty-four hour internal and external video monitoring and tracked card access that divides the facility into varying levels of security with each successive level being more secure and restricted to fewer individuals. In order to access the server room, individuals must successfully pass through multiple levels of security.

8. Technical Safeguards Implemented

In addition to de-identifying personal health information prior to analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the childhood cancer system pursuant to section 45 of the *Act*, POGO has implemented other technical safeguards to protect personal health information in its custody or control.

The technical safeguards implemented include multiple firewalls, network encryption and intrusion detection systems and the authentication of user identification and user passwords

prior to accessing applications containing personal health information. They also include the separation of the server containing personal health information from the local area network, a *Password Policy* consistent with current industry standards and a mandatory, standardized and system-wide password-protected screen saver after a timeout period of fifteen minutes.

POGO has also installed encryption software on all laptop computers to ensure that personal health information is being encrypted as the personal health information is being entered on the laptop computer and has developed and implemented an *Encryption Policy* which requires all personal information, including all personal health information, on mobile devices and all personal information, including personal health information, sent by e-mail transmission to be encrypted.

It is recommended however, that the *Encryption Policy* be amended to set out the circumstances in which personal information, including personal health information, may be stored on a mobile device or may be sent by e-mail transmission.

It is further recommended that the *Encryption Policy* be amended to state that only the minimum amount of personal information required must be stored on a mobile device or sent by e-mail transmission, to require personal information to be de-identified to the fullest extent possible, to require the e-mail transmission and the mobile device to be password protected using a strong password and to require the password for the mobile device to be different from the passwords for the files containing personal information. The *Encryption Policy* should further stipulate a time-frame within which the personal information must be securely deleted from the mobile device and e-mail transmission and to set out the method by which personal information must be deleted.

POGO also retained the services of a third party to conduct a threat and risk assessment and vulnerability assessment on its information technology infrastructure and related applications. This threat and risk assessment, completed on June 19, 2008, concluded that the risk level for the information technology infrastructure and related applications was low, but made recommendations to improve the overall security of personal health information at POGO. It is recommended that POGO implement all the recommendations made in the threat and risk assessment.

Summary of Recommendations

It is recommended that POGO address the recommendations detailed in this report prior to the next review of its practices and procedures. In summary, it is recommended that POGO:

1. In respect of its policies to document, contain, investigate and remediate information breaches and to provide notification in the event of an information breach:

    (a) Amend the *Privacy Breach Policy* to identify what information with respect to an information breach must be reported to the Privacy Officers and the format for

this report, to require that all information breaches be documented, to require notification to the health information custodian who provided the personal health information in the event of an information breach and to ensure that amendments to existing policies and procedures be considered for both internal and external breaches; and

(b) Amend the *Disciplinary Action - Privacy Infractions Policy* to ensure consistency of terminology and to impose a mandatory obligation on agents to report information breaches or suspected information breaches.

2. Amend the *De-Identifying Personal Health Information Policy* to require that de-identified information be used for purposes of its function as a prescribed entity under section 45 of the *Act*; to set out the other circumstances when de-identified information must be used; to describe the information that must be removed, encrypted and/or truncated in order to de-identify personal health information and to outline the process that will be followed in de-identifying personal health information.

3. In respect of its policies governing the transmission of personal health information, amend the *E-mail Policy*, *Encryption Policy* and *Secured Faxes (Containing Personal Health Information/Confidential Information) Policy* pursuant to the comments in this report.

4. Differentiate between the collection and use of personal health information for research purposes pursuant to section 44 of the *Act* and the collection and use of personal health information pursuant to its function as a prescribed entity under section 45 of the *Act* by:

(a) Developing and implementing a written policy to establish criteria that will be used in deciding when a collection and use of personal health information is for research purposes pursuant to section 44 of the *Act* and when it is for purposes of its function as a prescribed entity pursuant to section 45 of the *Act*, including the policies, procedures and practices and the statutory conditions that apply in each context; and

(b) Amending the information made available to the public and other stakeholders to clearly set out the purposes for which POGO is collecting and using personal health information, the statutory authority for such collection and use and the policies, procedures and practices and the statutory conditions that apply to the collection and use of the personal health information.

5. Amend its policies, practices and procedures relating to the use and disclosure of personal health information for research purposes and relating to the disposal of personal health information collected for research purposes by amending the *Ethics Review Process Policy*, the *Project-Specified Privacy Impact Assessment Form*, the *Researcher Agreement* and the *Retention and Destruction of Data Policy* pursuant to the comments in this report.

6. With respect to privacy and security orientation and ongoing privacy and security training:

   (a) Amend the *Staff Education and Training Policy* to encompass both initial privacy and security orientation as well as ongoing privacy and security training, to set out when the initial privacy and security orientation will be provided, to set out the frequency of the ongoing privacy and security training, to emphasize that attendance is mandatory and to describe the process that will be used to track attendance;

   (b) Amend the content of the initial privacy and security orientation pursuant to the comments provided in this report; and

   (c) Provide ongoing and formalized privacy and security training which includes role-based training and which addresses new privacy and security policies, procedures and practices implemented by POGO and significant amendments to existing privacy and security policies, procedures and practices.

7. Enter into *Data Sharing Agreements* with each of the hospitals that operate satellite programs and with each of the hospitals that operate aftercare clinics from which POGO collects personal health information and amend the template *Data Sharing Agreement* used to collect personal health information from and to disclose personal health information to other prescribed entities under section 45 of the *Act* pursuant to the comments in this report.

8. Expand the privacy audit program to assess compliance with all privacy policies, procedures and practices implemented by POGO and develop and implement a security audit program policy and procedure.

9. Implement all the recommendations made in the threat and risk assessment completed on June 19, 2008.

Statement of Continued Approval of Practices and Procedures

The IPC is satisfied that POGO continues to have in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and that sufficiently maintain the confidentiality of that information. Accordingly, effective October 31, 2008, the IPC is satisfied that POGO continues to meet the requirements of the *Act*.

APPENDIX "A"

RECOMMENDATIONS FROM THE INITIAL REVIEW

The IPC made the following recommendations during the initial review of the practices and procedures implemented by POGO that were approved by the IPC effective October 31, 2005:

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

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

3. Develop a data sharing agreement between POGO and other section 45 entities under the *Act* and prescribed persons pursuant to section 39(1) (c) of the *Act* that accords with the requirements in the *Act*.

4. Develop a research agreement for the disclosure of personal health information for research purposes that accords with the requirements of the *Act* and its regulation.

5. Develop the Questions and Answers about personal health information privacy protection at POGO and forward 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.

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

APPENDIX "B"

DOCUMENTATION REQUESTED

Privacy

- Privacy policies and procedures and the mechanism for reviewing and updating these policies and procedures
- Overview of privacy program and privacy audit program
- Reports on internal or external privacy audits conducted or completed
- Policies, procedures and protocols for privacy breaches and complaints
- Policies, procedures and protocols for data de-identification and data linkage including when, how, the purposes for which and by whom it will be de-identified or linked
- Information about the privacy training program for new and current employees, affiliates and volunteers including when it is provided, its content (copies of training material) and the mechanism to ensure that employees, affiliates and volunteers have been trained
- Information available to the public relating to privacy (i.e. brochures, frequently asked questions) and where it is made available
- Policies, procedures, protocols and agreements relating to research
- Privacy impact assessments for data holdings or programs including information relating to whether privacy impact assessments have been completed for all data holdings or programs, and if not, which have been completed and which remain outstanding

Security

- Security policies and procedures setting out the administrative, technical and physical safeguards and the mechanism for reviewing and updating these policies and procedures
- Policies, procedures and protocols for ensuring that personal health information is protected against theft, loss and unauthorized use or disclosure, including:
    - access control (authentication/authorization)
    - perimeter control, electronic control
    - encryption, firewalls and virus scanners

- secure transfer procedures
- password policies
- audit trails

- Information about the nature, scope and frequency of audits of access to data holdings
- Policies, procedures, protocols and agreements related to the secure retention, disposal and destruction of personal health information including retention schedules
- Policies, procedures and protocols related to sending and receiving personal health information including by facsimile, email transmission and other methods
- Policies, procedures and protocols for personal health information on portable or mobile devices such as laptop computers, personal digital assistants and flash drives
- Reports on internal or external threat and risk assessments
- Business continuity and disaster recovery plans
- Information about the security training program for new and current employees, affiliates and volunteers including when it is provided, its content (copies of training material) and the mechanism to ensure employees, affiliates and volunteers have been trained
- Reports on internal or external security audits conducted or completed

Organizational and Other Documentation

- Inventory of data holdings of personal health information
- Respective roles and responsibilities for privacy and security including information about the appointed contact persons for privacy and security and to whom they report and information about the terms of reference for privacy and security committees
- Confidentiality, non-disclosure, data sharing, research and third party agreements
- Policies, procedures and protocols relating to the execution of these agreements, including procedures to track and monitor their execution
- Disciplinary policies/procedures for violations
- Detailed documentation evidencing the completion of each recommendation set out in the report of the Information and Privacy Commissioner of Ontario dated October 2005