Information
and Privacy
Commissioner
of Ontario

Review of the Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network:

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

Ann Cavoukian, Ph.D.
Commissioner
August 2011

Information and Privacy Commissioner of Ontario

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

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

Table of Contents

Statutory Provisions Relating to the Disclosure to Prescribed Persons 1

Review Process 2

Description of the Prescribed Person 3

Findings of the Review 4

1. Privacy Documentation 4
2. Security Documentation 13
3. Human Resources Documentation 18
4. Organizational and Other Documentation 21

Summary of Recommendations 22

Statement of IPC Approval of Practices and Procedures 22

Review of the Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network:

A Prescribed Person 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 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 persons that compile or maintain registries of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances pursuant to subsection 39(1)(c) of the *Act*.

Statutory Provisions Relating to the Disclosure to Prescribed Persons

Subsection 39(1)(c) of the *Act* permits health information custodians to disclose personal health information, without consent, to a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances. The following persons have been prescribed for purposes of subsection 39(1)(c) of the *Act*:

- Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network;
- Cancer Care Ontario in respect of the Ontario Cancer Screening Registry;
- Cardiac Care Network of Ontario in respect of its registry of cardiac services;
- INSCYTE Corporation in respect of CytoBase;
- Hamilton Health Sciences Corporation in respect of the Critical Care Information System;
- Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network; and
- Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank.

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.

In order for a health information custodian to be permitted to disclose personal health information to a prescribed person without consent, the prescribed person must have in place practices and procedures approved by the Information and Privacy Commissioner of 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 13(2) of Regulation 329/04 to 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 13(2) of Regulation 329/04 to the *Act*, in order for a health information custodian to be able to continue to disclose personal health information to a prescribed person without consent, and in order for a prescribed person to be able to continue to collect, use and disclose personal health information without consent as permitted by the *Act*.

Review Process

The *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("*Manual*"), issued by the IPC in 2010, outlines the process that will be followed by the IPC in reviewing the practices and procedures implemented by prescribed persons and prescribed entities to protect the privacy of individuals whose personal information they receive and to maintain the confidentiality of that information. The *Manual* sets out the detailed obligations imposed on prescribed persons and prescribed entities arising from the review and approval process. The *Manual* requires prescribed persons and prescribed entities to have in place practices and procedures to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. At a minimum, the prescribed person or prescribed entity must submit to the IPC the documentation described in Appendix "A" to the *Manual* containing the minimum content described in Appendix "B" to the *Manual*.

The Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network submitted the required documentation on April 13, 2011. Upon receipt, the IPC conducted a detailed review of all the documentation in order to ensure that it complied with the *Manual* requirements. Following the review, on May 16, 2011, the IPC submitted comments to the Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network describing necessary clarifications and minor revisions required by the IPC. Necessary clarifications and revisions were submitted by the prescribed person on June 8, 2011 and June 20, 2011.

An on-site meeting was held, on June 27, 2011, to discuss the practices and procedures implemented by the prescribed person; to provide the IPC with an opportunity to ask questions arising from the documentation provided; and to review the physical, technological and administrative security measures implemented by the prescribed person.

Following the document review and on-site meeting, the Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network was informed of the action that it was required to take prior to the approval of its practices and procedures. Once all necessary action was taken, the IPC prepared a draft report that was submitted to the prescribed person for review and comment.

It must be emphasized that the review by the IPC was limited to personal health information collected, used and disclosed by the prescribed person pursuant to its function as a prescribed person under subsection 39(1)(c) of the *Act* and not with respect to any other role or responsibility that the prescribed person may have.

Description of the Prescribed Person

The Children's Hospital of Eastern Ontario ("CHEO") and the Ministry of Health and Long-Term Care established the Better Outcomes Registry and Network ("BORN") to build and manage the maternal/child registry; to build a source of accurate and timely maternal-infant information for facilitating and improving the provision of health care to pregnant women and children in Ontario; and for analysis of maternal-newborn data to support decision making by health care providers and planners.

The BORN system is a single data holding that is comprised of personal health information collected from health information custodians including laboratories providing prenatal and newborn screening, hospitals, midwives, and outpatient clinics. The personal health information collected includes health numbers, demographic information and clinical information about fetuses, newborn babies, children, and their mothers, including pregnancy history, medical history, and a summary of the care provided during pregnancy, labour, birth and the newborn period.

BORN uses the information it collects for the purposes of identifying where appropriate care has not been received and facilitating access to care and treatment for mothers, infants and children; facilitating continuous improvement of healthcare delivery tools to minimize adverse outcomes; raising alerts where maternal and/or newborn outcomes are statistically discrepant with accepted norms; to create reports and tools to allow health care providers to compare themselves with peers and/or benchmarks thereby enabling them to improve care; knowledge translation to improve the quality and efficiency of care for mothers, infants and children; and creating reports that can be used to provide the Ministry of Health and Long-Term Care, Local

Health Integration Networks and public health units with comprehensive and timely information to support effective planning and management of health care delivery for mothers, babies and children in Ontario.

BORN discloses personal health information to health information custodians when facilitating access to care and treatment for mothers, babies and children, for example to ensure appropriate screening is offered in a meaningful timeframe. BORN also discloses personal health information to prescribed entities for the management, evaluation, monitoring or planning for the health system and to researchers for research purposes.

Findings of the Review

1. Privacy Documentation

General Privacy Policies, Procedures and Practices

The *Privacy Policy in Respect of CHEO's Status as a Prescribed Person* describes CHEO's status under the *Act* as well as BORN's policies, procedures and practices with respect to the collection, use and disclosure of personal health information. The *Policy* also describes BORN's privacy and security accountability framework. The President and Chief Executive Officer of CHEO has ultimate accountability for ensuring compliance with the *Act*, its regulation, and the privacy and security policies, procedures and practices implemented and has delegated day-to-day responsibility to the BORN Leadership Team, which consists of the Executive Lead (CHEO VP), the Medical Director, the Scientific Director and the Operations Director. The BORN Leadership Team has delegated the day-to-day management of the privacy and security program to the Privacy Officer. The *Policy* states that BORN has administrative, technical and physical safeguards to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. It also states that steps are taken to protect personal health information against theft, loss, unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

The *Ongoing Review of Privacy and Security Policies and Procedures Policy* describes the process for the development of new documents and for the revision of previously issued documents including the document review and approval process. The Privacy Officer initiates a review of privacy and security policies and procedures annually, or when personal health information in BORN's custody or control has been lost, stolen, used or disclosed without proper authorization; when an order, fact sheet, guideline or best practice is issued by the IPC; or when amendments are made to the *Act* and its regulation that are relevant to CHEO as a prescribed person

Transparency

The *Transparency of Privacy Policies and Procedures Policy* specifies that BORN provides information relating to the BORN privacy and security policies and procedures to the public and other stakeholders through the BORN website. The Privacy Officer ensures that the information on the website includes the *Privacy Policy in Respect of CHEO's Status as a Prescribed Person;* Frequently Asked Questions related to BORN privacy policies and procedures; results from the IPC review of BORN's privacy policies and procedures; a list of data holdings of personal health information maintained by BORN; summaries of privacy impact assessments conducted by BORN; and the name, title, mailing address and contact information of the Privacy Officer to whom inquiries, concerns or complaints regarding compliance may be directed.

Collection of Personal Health Information

The *Collection of Personal Health Information and Statements of Purpose for Data Holdings Containing Personal Health Information Policy* states that BORN only collects personal health information if the collection is permitted by the *Act* and its regulation. It also states that BORN collects only the minimal amount of personal health information required to achieve the purposes of the registry and does not collect personal health information if other information will serve the purpose. The Data Dictionary Review Committee has responsibility for determining the nature of the personal health information required to enable BORN to fulfill its mandate, the list of data elements and any sub-elements, the health information custodians from whom the data elements will be collected, and the statements of purpose for each data element in relation to the identified purposes of the registry. The Privacy and Security Committee reviews and approves the proposed list of data elements, the list of health information custodians from whom the data elements will be collected and the statements of purpose. Final review and approval is by the Leadership Team. The Privacy Officer must ensure that a signed *Data Sharing Agreement* is executed before data is collected.

The *List of Data Holdings Containing Personal Health Information* describes the types of health information custodians from whom personal information is collected (e.g. laboratories and hospitals) and describes the unique data collections that are provided by the health information custodians (e.g. prenatal screening laboratory, ultrasound and results information).

The *Statements of Purpose for Data Holdings Containing Personal Health Information* describes why BORN was established and describes the core uses of the registry. It outlines the five types of information that are required to be collected in order to achieve the purposes of the BORN registry. The five types of required information are identifiers, health status, health risk factors, care provided and health outcomes. Details and examples of all five types of information are also provided. The *BORN Data Dictionary* document maps each data element collected by the

BORN system to one of the examples included in the *Statements of Purpose for Data Holdings Containing Personal Health Information* to illustrate the requirement for the data element to be collected.

Use of Personal Health Information

The *Limiting Agent Access to and Use of Personal Health Information Policy* states that BORN prohibits agents from accessing and using personal health information except as necessary for employment or contractual responsibilities and requires agents to access and use the minimal amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities with BORN. All agents must apply to the Privacy Officer for approval to access and use personal health information by completing an *Agent Data Access Form*. There are six levels of access (e.g. authorization to read, authorization to use). Based on criteria, which are set out in the *Policy*, the Privacy Officer makes recommendations to the Privacy and Security Review Committee, which has final review and approval regarding access and use of personal health information. All approved accesses and uses of personal health information are subject to an automatic expiry after one year, or sooner based on request. The BORN System Administrator maintains a *Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information*.

The *Use of Personal Health Information for Research Policy* states that BORN permits the use of personal health information for research purposes as authorized under the *Act* where BORN agents meet the requirements for research provided in section 44 of the *Act* and its regulation and where the purpose for the use is in accordance with the stated purpose for the registry. BORN agents requesting the use of personal health information as part of a research data set must submit a completed *Data Request Form*, a research plan and a copy of the decision of a Research Ethics Board that approved the research plan, to the Scientific Manager. A review is conducted to determine whether aggregate or de-identified record-level data could meet the identified research need. Agents requesting use of de-identified or aggregate data remain bound by the *Confidentiality Agreement* signed by all BORN agents. A *Log of Approved Uses of Personal Health Information for Research* is maintained.

Disclosure of Personal Health Information

The *Disclosure of Personal Health Information for Purposes other than Research Policy* states that BORN discloses record-level data for purposes other than research only for the purpose of carrying out a statutory or legal duty, for the purpose for which the health information custodian was authorized to disclose the information, to a prescribed entity or to a health data institute. Where BORN is disclosing to a health information custodian that a necessary screening procedure for a mother or a newborn has been missed, the BORN system produces an alert report that is available to the clinical program impacted by the missed screen. Where BORN is

disclosing to a health information custodian that a woman tested positive during her pregnancy for gestational diabetes and requires follow-up screening following the birth of her child, the BORN system produces a report that is sent to the primary health care provider detailing that the patient requires the follow-up screening test. The BORN Manager of Health Informatics decides, in consultation with the Privacy Officer, which specific instances warrant disclosure and creates alert reports only for those instances.

The *Disclosure of Personal Health Information for Purposes other than Research Policy* states that a prescribed entity or health data institute requesting disclosure of personal health information for non-research purposes must complete a *Data Request Form*, which is reviewed by the Scientific Manager, to determine if the disclosure is permitted or required under the *Act* and its regulation, to determine if the purpose for the disclosure is in accordance with the stated purposes for the BORN registry, to confirm that the personal health information is reasonably required for the purpose and that no other information would suffice, and to confirm that the amount of information requested is limited to the minimum amount reasonably required to meet the purpose. A *Data Sharing Agreement* must be executed with the prescribed entity or health data institute. Individuals or organizations requesting disclosure of de-identified and/or aggregate data for non-research purposes must complete a *Data Request Form*, which is reviewed by the Scientific Manager. The Scientific Manager also undertakes a review to determine the residual risk of re-identification. Where the de-identified or aggregate data is being requested by a prescribed entity or health data institute, a *Data Sharing Agreement* must be executed.

The *Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements Policy* states that BORN permits the disclosure of personal health information for research purposes as authorized under the *Act* and its regulation. BORN will not disclose personal health information for research purposes if other information will serve the research purpose and will not disclose more personal health information than is reasonably necessary to meet the identified research purpose. Researchers must meet the requirements for research disclosure provided in section 44 of the *Act* and its regulation. Researchers requesting disclosure of de-identified data, aggregate data or personal health information must submit a completed *Data Request Form*, a research plan and a copy of the decision of the Research Ethics Board that approved the research plan, to the Scientific Manager for review. Researchers requesting disclosure of personal health information must also obtain written approval from the Disclosure of Personal Health Information Review Committee and must also receive CHEO Research Ethics Board Approval. A *Research Agreement* must be executed with researchers requesting disclosure of personal health information. A *Log of Research Agreements* is maintained.

The *Template Research Agreement* contains a number of provisions including those related to the permitted uses and disclosures of personal health information; the technical, administrative and physical safeguards; the procedure to be followed in the event of a breach; audits that may be done to ensure compliance with the agreement; and the secure transfer, retention, and disposal

of personal health information. It also contains schedules to the *Agreement* including a list of data to be provided to the researcher and a *Confidentiality Agreement* that must be signed by all persons who will have access to personal health information.

Data Sharing Agreements

The *Data Sharing Agreements Policy* requires the execution of a data sharing agreement when BORN is collecting personal health information from health information custodians for the purposes of BORN, and when BORN is disclosing personal health information for purposes other than research. Data sharing agreements are managed and executed by the Privacy Officer. A *Log of Data Sharing Agreements* is also maintained. There are two *Template Data Sharing Agreements,* one for disclosure of personal health information and one for collection of personal health information.

The *Template Data Sharing Agreements* contain provisions including those related to the use and disclosure of personal health information; the security of personal health information; data breaches; and responsibilities relating to the secure transfer, retention, and disposal of personal health information. They also contain schedules, including a list of data elements that will be provided by BORN or to BORN and a *Confidentiality Agreement* that must be signed by all persons who will have access to personal health information.

Agreements with Third Party Service Providers

The *Executing Agreements with Third Party Service Providers in Respect of Personal Health Information Policy* requires a written agreement to be entered into with third party service providers prior to permitting access to and use of personal health information including those that are contracted to retain, use, transfer or dispose of records of personal health information, and those that are contracted to provide services to enable CHEO, in respect of BORN, to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information. Agreements with third-party service providers are initiated by the appropriate BORN Director according to CHEO procurement policies. The Privacy Officer reviews the request and creates an agreement based on the *Template Agreement for All Third Party Service Providers*. The applicable BORN Director executes the agreement. The Privacy Officer updates the *Log of Agreements with Third Party Service Providers*.

The *Template Agreement for All Third Party Service Providers* contains a number of provisions including those related to the permitted uses and disclosures of personal health information; security of personal health information; the procedure to be followed in the event of breaches; inspections that may be done to ensure compliance; and responsibilities relating to the secure transfer, retention, return and disposal of personal health information. It also contains schedules to

the *Agreement* including a list of data elements to be accessed, used and/or disclosed in the course of providing specified services and a *Confidentiality Agreement* that must be signed by agents of the third party service provider who will have access to personal health information.

Data Linkage and Data De-identification

The *Linkage of Records of Personal Health Information Policy* states that BORN permits linkage of personal health information for identifying where appropriate care has not been received and facilitating access to care and treatment for mothers, infants and children; facilitating continuous improvement of healthcare delivery tools to minimize adverse outcomes; raising alerts where maternal and/or newborn outcomes are statistically discrepant with accepted norms; looking across the continuum of care of an individual or population to improve the quality and efficiency of care for mothers, infants, and children; and creating reports that can be used to provide the Ministry of Health and Long-Term Care, Local Health Integration Networks and public health units with comprehensive and timely information to support effective planning and management of health care delivery for mothers, babies, and children in the province.

BORN permits linkage of records of personal health information solely in the custody of BORN for the exclusive purposes of BORN; records of personal health information in the custody of BORN with records of personal health information to be collected from another person or organization for the exclusive purposes of BORN; records of personal health information solely in the custody of BORN for the purposes of disclosure to another person or organization; and records of personal health information solely in the custody of BORN with records of personal health information to be collected from another person or organization for the exclusive purposes of that other person or organization.

A linking and matching algorithm has been developed to automate the process of linking information where sufficient information exists within the BORN system. Where a potential link is found (where there is likely a match but there is insufficient information to be certain) human interaction is required to complete the work. A designated BORN agent manages the queue of potential linked records. The Manager of Health Information manages the *Log of Approved Linkages of Records of Personal Health Information*.

The *De-identification and Aggregation Policy* states that BORN prohibits the use of personal health information if other information, namely de-identified and/or aggregate information, will serve the identified purpose, and contains a definition of de-identified information, aggregate information and identifying information. Where information is aggregated, but includes information about individuals in groups of five or less, the information will not be released. De-identification occurs in consultation with the CHEO Electronic Health Information Laboratory ("EHIL"). EHIL assesses the level of re-identification risk using the empirical analysis Privacy

Analytics Re-Identification Risk Assessment and De-identification Tool ("PARAT") for all uses and disclosures of de-identified and/or aggregate data. In addition, de-identified and/or aggregate data, including information of cell-sizes of five or less, is reviewed by the Scientific Manager prior to every use or disclosure to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized to identify an individual.

Privacy Impact Assessments

The *Privacy Impact Assessments Policy* states that Privacy Impact Assessments ("PIAs") will be conducted on existing programs, processes and systems when there are significant changes related to the collection, access, use or disclosure of personal health information; in the design of new programs, processes and systems involving personal health information; and on any other programs, processes and systems with privacy implications, as recommended by the Privacy Officer. The *Policy* also stipulates the minimum required content of PIAs. The Privacy Officer, in conjunction with the Manager of Health Informatics, develops a timetable to ensure PIAs are reviewed and refreshed on an on-going basis, and are repeated every three years at a minimum. The Privacy Officer submits completed PIAs and recommendations to the Privacy and Security Review Committee and the Leadership Team for review at their monthly meetings. When written approval of the Leadership Team has been received, the Privacy Officer implements the recommendations arising from the PIA. The Privacy Officer maintains a *Log of Privacy Impact Assessments Initiated/Completed* and a *Log of Privacy Impact Assessments Not Undertaken*, which sets out, among other things, the reason the PIA was not undertaken and the agent responsible for the decision.

Privacy Audit Program

The *Privacy Audit Policy* states that the Privacy Officer conducts regular privacy audits to assess organizational compliance with privacy policies and procedures to ensure that they continue to reflect the requirements of the *Act* and its regulation as well as privacy best practices; to assess compliance of agents permitted to access and use personal health information; and on external parties to assess compliance with *Research Agreements, Data Sharing Agreements* and *Agreements for Third Party Service Providers*. The Privacy Officer develops and implements the annual privacy audit plan. Upon completion of each privacy audit, the Privacy Officer provides a copy of the audit report and action plan to the BORN Director, the Privacy and Security Review Committee and the Leadership Team for review and comment. When written approval of the Leadership Team has been received, the Privacy Officer implements the action plan, monitors implementation and provides monthly status updates. The Privacy Officer includes results of each privacy audit, recommendations of each privacy audit and the status of implementation of the recommendations of each privacy audit in the quarterly reports and the Annual Report on Privacy and Security, which are provided to the Privacy and Security Review Committee and

the Leadership Team, with the Annual Report also being provided to the CEO of CHEO. The Privacy Officer also maintains the *Log of Privacy Audits*.

Privacy Breaches, Inquiries and Complaints

The *Privacy Breach Management Policy* contains a definition of a privacy breach. The *Policy* requires agents to notify the Privacy Officer as soon as reasonably possible of any privacy breach or suspected privacy breach. A verbal notification must be followed up as soon as possible by completion of a *Breach Reporting Form*. The Privacy Officer, together with the appropriate agents, works immediately to confirm and further contain the breach. When it has been determined that a privacy breach has occurred, the Privacy Officer immediately notifies the BORN Director who, along with the Privacy Officer, reviews the containment measures implemented to determine that the privacy breach has been effectively contained. As soon as reasonably possible, the BORN Director forwards the Privacy Officer's notification and a description of any further containment efforts to the Leadership Team. Within 24 hours of a privacy breach the Privacy Officer completes a *CHEO Incident Report*. The Privacy Officer forwards the *Incident Report* to the CHEO Chief Privacy Officer. These incidents are reviewed by the CHEO Quality Committee Board of Directors three times per year.

The *Privacy Breach Management Policy* requires the health information custodian or other organization that disclosed the personal health information to BORN to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization. After consultation with the BORN Director, the Privacy Officer notifies the Ministry of Health and Long-Term Care of the privacy breach. When the breach has been contained, consideration is given to reporting the breach to the IPC.

The *Privacy Breach Management Policy* states that the Privacy Officer, together with the appropriate BORN agents, must initiate a comprehensive investigation which must be completed within four weeks from the time the breach was reported. The Privacy Officer also prepares a comprehensive report which includes recommendations for corrective measures arising from the investigation. When the Leadership Team approves the recommendations, the Privacy Officer assigns agents to implement changes, establishes implementation timelines, and monitors and tracks these activities to ensure that the recommendations are implemented within the stated timelines. The Privacy Officer provides a written status report and a copy of the *Log of Privacy Breaches* to the Privacy and Security Committee on a monthly basis. The Privacy Officer includes a description of the nature and extent of privacy breaches, the causes of the privacy breaches and the recommendations and status of implementation of the recommendations in the quarterly report to the Privacy and Security Review Committee and the Leadership Team and in the Annual Report on Privacy and Security.

The *Breach Management Protocol* defines a privacy breach, and states that BORN agents who discover a potential breach should act quickly to limit the breach and must support the evaluation of the situation. The Privacy Officer is responsible for notification of the breach and for preventing further breaches.

The *Privacy Complaints Policy* describes BORN's privacy complaint management process. Information regarding the process for making a privacy complaint is available on all public communications materials. Communications materials also indicate that complaints regarding BORN's compliance with the *Act* and its regulation can be directed to the IPC. If a complaint cannot be addressed satisfactorily through a phone discussion or face-to-face meeting, the Privacy Officer requests that the complainant fill out a *Complaint Form*. Within seven days of receipt of the *Complaint Form*, the Privacy Officer must assess the complaint and determine whether the complaint is a privacy complaint that should be investigated, or whether the complaint is a privacy breach and should be addressed as per the *Privacy Breach Management Policy*. A complaint is subject to further investigation if the privacy complaint relates to an action on the part of BORN agents that could constitute a breach of BORN policy or procedures or the requirements of the *Act* and its regulation; relates to an activity on the part of BORN agents that could be contrary to industry best practices or directives, publications or communications from the IPC; or is well-founded for any other reason. A letter is sent to the complainant acknowledging the complaint and advising whether or not further investigation will be undertaken.

The *Privacy Complaints Policy* states that if a complaint will be investigated, within 30 days of receipt of the *Complaint Form*, the Privacy Officer must complete an investigation, document the findings (including recommendations to address the concern identified in the complaint) and forward a report to the BORN Director with a copy going to the Communications Lead. The BORN Director reviews the report and forwards it to the Leadership Team. Once Leadership Team approval has been obtained, the Privacy Officer is responsible for the implementation of the recommendations. Within 45 days of receiving the *Complaint Form*, the Privacy Officer notifies the complainant of the investigation findings, any measures that have/will be taken, and the complainant's right to make a complaint to the IPC. The Privacy Officer provides a status report to the BORN Director, Leadership Team and BORN staff on a monthly basis during the implementation of the recommendations, and upon completion of the implementation of the recommendations. The Privacy Officer includes a description of the complaints received and actions taken in the quarterly report to the Privacy and Security Review Committee and the Leadership Team and in the Annual Report on Privacy and Security. The Privacy Officer also maintains the *Log of Privacy Complaints and Privacy Inquiries*.

The *Privacy Inquiries Policy* states that BORN responds to all privacy inquiries. Information regarding the process for making a privacy inquiry is available in all public communications materials. The Privacy Officer receives and reviews all inquiries to determine if the inquiry relates to a privacy breach and should be addressed as per the *Privacy Breach Management*

Policy, or relates to a privacy complaint and should be addressed as per the *Privacy Complaints Policy.* Responses to all inquires are provided in writing. The Privacy Officer maintains the *Log of Privacy Complaints and Privacy Inquiries*.

2. Security Documentation

General Security Policies and Procedures

The *Information Security Policy* states that the Privacy Officer is responsible for the implementation and oversight of a comprehensive information security program that includes administrative, physical and technical safeguards consistent with industry standards. The security program includes policies and procedures for the ongoing review of the security policies, procedures and practices implemented; for ensuring physical security of the premises; for the secure retention, transfer and disposal of records of personal health information; to establish access control and authorization; for monitoring; for network security management; for back-up and recovery; related to the acceptable use of information technology; for information systems acquisition, development and maintenance; for information security breach management; to establish protection against malicious and mobile code; and a security governance framework. The Privacy Officer, in conjunction with the Manager of Health Informatics, implements a program for continuous assessment and verification of the effectiveness of the security program.

The *Ongoing Review of Privacy and Security Policies and Procedures Policy* describes the process for the development of new documents and for the revision of previously issued documents including the document review and approval process. The Privacy Officer initiates a review of privacy and security policies and procedures annually, or when personal health information in BORN's custody or control has been lost, stolen, used or disclosed without proper authorization; when an order, fact sheet, guideline or best practice is issued by the IPC; or when amendments are made to the *Act* and its regulation that are relevant to CHEO as a prescribed person.

Physical Security

The *Ensuring Physical Security of Personal Health Information Policy* describes the physical safeguards implemented by BORN to protect records of personal health information (e.g. locked doors, swipe cards, alarms etc.). All agents must apply to the Privacy Officer for approval to access the premises and locations within the premises where records of personal health information are retained by completing an *Agent Data Access Form*. The Privacy Officer considers whether access is required in order for the agent to carry out their employment or contractual responsibilities. Where the Privacy Officer approves an application for access, the Privacy Officer forwards to the Privacy and Security Review Committee for review and approval, documentation dealing with the level of access recommended, conditions or restrictions to be imposed, the timeframe that applies to the authorization (if less than one year), the rationale for the recommendations, the completed *Agent Data Access Form* and the job specification or contract. All approved accesses

are subject to an automatic expiry after one year. When the Privacy Officer receives approval from the Privacy and Security Review Committee, the Privacy Officer forwards the relevant information to the agent's supervisor, the Manager of Health Informatics and the Hosting Provider and works with the Hosting Provider to supply the identification cards, access cards and/or keys to the premises and locations within the premises and enters the information in the *Log of Agents with access to the Premises.*

The agent and his/her supervisor must notify the Privacy Officer as soon as a decision is taken to terminate or to make any changes in the agent's role that would impact the level of access required. Agents must notify their supervisor and the Privacy Officer at the first reasonable opportunity of any theft, loss or misplacement of identification cards, access cards and/or keys. The Privacy Officer determines the safeguards required to be implemented (cancelling card access, changing access codes or re-keying premises based on assessment of risk), assigns responsibility for implementation to the appropriate BORN agent, and updates the *Log of Agents with Access to the Premises*, as required.

All visitors must have visible identification badges and are required to sign in and record their name, date and time of arrival, time of departure and the name of the agent(s) with whom the visitors are meeting. Visitors must be accompanied by an agent at all times, must wear identification badges and must ensure that the identification badge is returned prior to departure.

Retention, Transfer and Disposal

The *Secure Retention of Records of Personal Health Information Policy* states that records of personal health information in electronic format are retained only as long as necessary to fulfill the purpose for which the personal health information is collected, to a maximum of 28 years, in order to permit longitudinal analysis for the purposes of improving the provision of care to mothers, infants and children. Records of personal health information held by researchers must not be retained for a period longer than set out in the *Research Agreements*. Paper records held by BORN are only kept long enough to effect a transfer to secure electronic format and are then securely destroyed. This is an interim state pending full electronic adoption when there will be no collection, use or disclosure of personal health information in paper format. The Privacy Officer has responsibility for the secure retention of records of personal health information.

The *Secure Retention of Records of Personal Health Information on Mobile Devices Policy* states that personal health information will not be stored on mobile computing equipment except in very specific and exceptional circumstances. Personal health information in the custody and control of BORN may be accessed remotely only where an agent is accessing personal health information for the purpose of using the data for registry purposes. In order to retain personal health information on a mobile device or to access personal health information remotely, the agent must make a request to the Privacy Officer. If approval is obtained, the agent must first

sign the *Agreement for Use of Mobile Devices/Remote Access*, which requires the agent to adhere to specific conditions, including not remotely accessing or retaining personal health information on the mobile device if other information, such as de-identified or aggregate information, will serve the purpose and not retaining or accessing personal health information for longer than necessary to meet the identified purpose. The Privacy Officer enters all approvals in the *Log of Agent Use of Mobile Devices/Remote Access*.

The *Secure Transfer of Records of Personal Health Information Policy* states that records of personal health information must be transferred in a secure manner and using only approved methods. Apart from one exception, which is presently being phased out, paper-based transfers of personal health information are not permitted and agents are not permitted to transfer personal health information by fax. For personal health information transferred on removable media, the Scientific Manager reviews the information to ensure it is consistent with the approved request, ensures that the disk is encrypted and password protected, and uses a bonded courier. The recipient must call to confirm receipt of the data and to obtain the password to decrypt the data set. When receipt has been confirmed, the Scientific Manager updates the *Data Tracking Log*. Personal health information collected electronically from health information custodians is transferred only over the eHealth Ontario ONE network and is protected by a virtual private network. When personal health information is transferred between BORN and prescribed entities, BORN uses the secure network provided by the prescribed entity.

The *Secure Disposal of Records of Personal Health Information Policy* requires records of personal health information to be disposed of in a secure manner. Disposed of in a secure manner means that the records are destroyed in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstances. Records of personal health information in paper format are disposed of using a cross-cutting shredding method and incineration to eliminate the possibility of reconstructing the documents. Records of personal health information in electronic form and/or removable devices are disposed of by physically damaging the item to render it useless. If re-use is being considered, wiping utilities software specific to the media form factor will be employed.

Information Security

The *Password Policy* requires agents to develop and use strong passwords when accessing information systems, technologies, equipment, resources, applications and programs containing personal health information, regardless of whether they are leased, owned or operated by BORN. The *Policy* describes standards for password composition, password protection and password expiry.

The *System Control and Audit Logs Policy* states that the access, use, modification and disclosure of personal health information in the custody and control of BORN are monitored on an on-

going basis. The BORN Application Service Provider is responsible for system design in order to ensure that audit logs capture the date and time of any operation or action, the name of the user that performed the operation or action and the changes to values, if any, and for the day-to-day maintenance of the information in the system control and audit logs. The BORN System Hosting Provider ensures that the system does not allow the audit log to be tampered with, that the audit controls remain operational at all times, that the audit history is retained on-line such that it can be reviewed for a period of two years from the date of the event, and that each event is retained in the logs. The Manager of Health Informatics runs the audit reports on an as-needed basis, ensures appropriate supervision of the operation of the system control and audit logs, monitors the logs on a monthly basis and provides a report regarding the monitoring of the system control and audit logs to the Privacy Officer on a monthly basis. The Privacy Officer determines the nature and scope of events to be audited, and monitors that all audits are logged in the audit logs. The Privacy Officer also reports to the Privacy and Security Committee on a monthly basis the nature and type of audits undertaken, the findings of the audits, the efforts undertaken to address the findings, and the status of these efforts. The *Policy* also describes the common elements of each audit report and describes specific audit report areas.

The *Patch Management Policy* states that software patches and other software upgrades are reviewed on an ongoing basis and implemented where appropriate in order to ensure that BORN provides a secure operational environment. The System Hosting Provider reviews Microsoft patches for security updates and critical updates as well as for patches applicable to the hardware comprising the BORN system. The Application Service Provider stays abreast of patches applicable to off-the-shelf software in the BORN system. The *Policy* describes the process for obtaining approval for patches, and for testing and implementing patches.

The *Change Management Policy* states that requests for changes to the operational environment are subject to a thorough review and approval process. The *Policy* specifies the process related to change request submission (through the use of a *Change Request Form*), as well as change request review and implementation. The Manager of Health Informatics is responsible for reviewing change requests and for securely maintaining the *Log of Change Requests*. If the Manager of Health Informatics approves a change that entails a possibility of a privacy or security risk, the Privacy Officer is informed and approval from the Privacy and Security Review Committee is required to proceed.

The *Back-up and Recovery of Records of Personal Health Information Policy* states that the BORN System Hosting Provider provides data protection and recovery service. The Application Service Provider is responsible for testing of the restored data for completeness. The System Hosting Provider collects nightly differential backup from the servers, performs a full backup once a week and once a month takes a complete set of full backup and stores it as a monthly backup. Monthly backup tapes are retained for two rolling years and quarterly backup tapes

are retained for another two years. Every quarter, a recovery test is performed to ensure that the data protection process remains adequate.

The *Acceptable Use of Technology Policy* describes the uses of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by BORN that are prohibited without exception and those that are permitted only with prior approval.

Security Audit Program

The Security Audits Policy states that BORN conducts the following types of security audits to assess compliance with security policies and procedures: threat risk assessments (both internal and external); vulnerability assessments; penetration testing; ethical hacks; audits of security controls (implemented and planned) to assess effectiveness; and reviews of system control and audit logs. The Privacy Officer develops an annual plan for security audits which is reviewed and approved by the Privacy and Security Review Committee. The Manager of Health Informatics undertakes the security audits and provides a written report to the Privacy Officer for each audit completed. The Privacy Officer assigns agents to address the recommendations arising from the security audit; sets out timelines for completion; and monitors to ensure that recommendations are implemented within the timeframes. The Privacy Officer maintains a *Log of Security Audits* and *Consolidated Log of Recommendations*, forwards the *Log of Security Audits* to the Privacy and Security Review Committee every month, and includes a description of security audits, recommendations and actions taken in quarterly reports to the Privacy and Security Committee and the Leadership Team, and in the Annual Report on Privacy and Security.

Information Security Breaches

The *Security Breach Management Policy* contains a definition of a security breach. The *Policy* requires agents to notify the Privacy Officer as soon as reasonably possible of any security breach or suspected security breach. Problems with security may be identified by the System Hosting Provider (who monitors and identifies risks such as perimeter, firewall and other external attacks), the Application Service Provider (who monitors and identifies risks to access to portal and threats to the BORN system itself), or an individual reporting inappropriate access or use. The System Hosting Provider and Application Service Provider must notify the Privacy Officer of any identified risks. An individual who provides a verbal notification of a security breach or suspected security breach must also complete a *Breach Reporting Form* as soon as possible.

The Privacy Officer, together with the Manager of Health Informatics, the Hosting Provider, and Application Service Provider (as applicable), works immediately to further contain the breach. If it has been determined that a security breach has occurred, the Privacy Officer, as soon as reasonably possible, notifies the BORN Director who, in consultation with the Privacy Officer

and the relevant agent, reviews the containment measures implemented to determine that the security breach has been effectively contained. As soon as reasonably possible, the BORN Director forwards the Privacy Officer's notification and a description of any further containment efforts to the Leadership Team. Within 24 hours of a security breach, the Privacy Officer completes a *CHEO IS Vector Form*.

The *Security Breach Management Policy* requires the health information custodian or other organization that disclosed the personal health information to BORN to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization. The Privacy Officer, in consultation with the BORN Director, considers notifying the Ministry of Health and Long-Term Care of the security breach and considers whether to report the breach to the IPC. The Privacy Officer meets with BORN staff to inform them of the nature and extent of the breach, and keeps them informed as the investigation and remediation proceeds. For all security breaches, the Privacy Officer e-mails updates to the Leadership Team, the Communications Lead and the CHEO Chief Privacy Officer, on a regular basis.

The *Security Breach Management Policy* states that the Privacy Officer, together with the appropriate BORN agents, must initiate a comprehensive investigation, which must be completed within four weeks from the time the breach was reported. The Privacy Officer also prepares a comprehensive report which includes recommendations for corrective measures arising from the investigation. When the Leadership Team approves the recommendations, the Privacy Officer assigns agents to implement changes, establishes implementation timelines, and monitors and tracks these activities to ensure that the recommendations are implemented within the stated timelines. The Privacy Officer provides a written status update and a copy of the *Log of Information Security Breaches* to the Privacy and Security Committee on a monthly basis. The Privacy Officer includes a description of the nature and extent of security breaches, the causes of the security breaches and the recommendations and status of implementation of the recommendations in the quarterly report to the Privacy and Security Review Committee and the Leadership Team and in the Annual Report on Privacy and Security.

3. Human Resources Documentation

Privacy and Security Training and Awareness

The *Privacy and Security Training and Awareness Policy* states that agents accessing personal health information must complete an initial privacy and security orientation prior to being given access to personal health information. All agents must also attend annual privacy and security training and additional training as required by the Privacy Officer. Working closely with the Manager of Health Informatics, the Privacy Officer prepares the training materials and delivers the initial privacy and security orientation. Ongoing privacy and security training is formalized

and standardized and includes role-based training. Agents must sign an attendance sheet at each training session. The Privacy Officer enters the information from the attendance sheet in *the Log of Attendance at Privacy and Security Training*. All agents are required to attend an annual BORN-hosted privacy and security workshop, which raises awareness of the privacy and security program. The Privacy Officer and the Manager of Health Informatics are each required to attend a minimum of one external privacy/security training session each year as approved by the Director of BORN.

Confidentiality Agreements

The *Execution of Confidentiality Agreements by Agents Policy* requires BORN agents to execute *Confidentiality Agreements* at the commencement of their employment, contractual or other relationship with BORN and prior to being given access to personal health information. *Confidentiality Agreements* are renewed annually on completion of annual privacy and security training. The Privacy Officer monitors and maintains the *Log of Executed Confidentiality Agreements with Agents*.

The *Template Confidentiality Agreement with Agents* requires the agent to comply with BORN's privacy and security policies and procedures as well as with the *Act* and its regulation. The agent must agree not to access and use personal health information in the custody and control of BORN, except as directed by BORN and as required to carry out employment, contractual or other responsibilities; not to access or use personal health information if other information will serve the purpose; not to access and use more personal health information than is reasonably necessary to meet the purpose; not to attempt to use personal information, or information derived from personal health information, to identify an individual; not to attempt to decrypt information that is encrypted; not to attempt to identify an individual based on prior knowledge; and not to make any unauthorized transmissions, copies or disclosures of personal information. The agent must acknowledge having received privacy training and access to privacy policies and procedures, must agree to access and use computers, software, databases and other information technologies related to the collection, storage and protection of personal information only as permitted by BORN, and must act diligently at all times to protect personal information. The agent must agree to report breaches to the Privacy Officer as soon as reasonably possible. The agent must agree to return all BORN property, including records of personal information and all identification cards, access cards and/or keys, on or before the date of termination of employment, contractual, or other relationship.

Responsibility for Privacy and Security

The *Job Description for Position(s) Delegated Day-to-Day Authority to Manage the Privacy and Security Programs* states that the Privacy Officer is responsible for developing, overseeing implementation and managing the BORN privacy strategy. This includes managing BORN's policies

and procedures governing privacy and security in compliance with the *Act* and best practices; advancing awareness of privacy programs and services; and managing privacy, monitoring and compliance activities. The Manager of Health Informatics is responsible for the development and maintenance of the technology systems. Privacy responsibilities of the Manager of Health Informatics include being a member of the Privacy and Security Review Committee; adhering to, representing and championing the BORN Privacy and Security Management Plan; building a culture of privacy within BORN; managing physical access to personal health information; and execution of security audits.

Termination of Relationship

The *Termination or Cessation of the Employment or Contractual Relationship Policy* requires agents to securely return all property, including records of personal health information, identification cards, access cards, credit cards, computer equipment, books, materials, cell phones and mobile devices, keys and any other CHEO or BORN owned items, on or before the date of termination of employment. Agents and their supervisors are required to notify the BORN Ontario Director and the Privacy Officer of the termination of an employment or contractual relationship two weeks in advance, if possible. The Privacy Officer forwards the name of the agent and the termination date to CHEO Human Resources, who process termination in the payroll system; to security for termination of access in the building; and to the Manager of Health Informatics, who arranges for the withdrawal of access to personal health information on the termination date and updates the *Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information*. The Privacy Officer emails the agent a request for the secure return of all property on or before the termination date and includes a list of all property to be returned. When the agent returns the property to the Privacy Officer, both the agent and Privacy Officer sign the list. The Privacy Officer retains the signed list in the agent's file.

Discipline

The *Discipline and Corrective Action Policy* states that the Privacy Officer investigates all privacy and security related disciplinary matters. The *Confidentiality Agreement*, which must be signed by all agents, states that a breach of the terms of the *Confidentiality Agreement*, BORN policies and procedures, and/or the provisions of the *Act* may result in disciplinary action which can include termination of employment or legal action. The Privacy Officer, in consultation with the BORN Director and CHEO Human Resources, determines the type of disciplinary action appropriate to the issue: oral warning and/or additional privacy and security training; written warning and/or additional privacy and security training; suspension without pay and/or additional privacy and security training; or termination of employment.

4. Organizational and Other Documentation

Governance

The *Privacy and Security Governance and Accountability Framework* states that the Chief Executive Officer of CHEO has ultimate accountability for ensuring compliance with the *Act*, its regulation, and the privacy and security policies and procedures and has delegated day-to-day responsibility to the BORN Leadership Team. The BORN Leadership Team has delegated the day-to-day management of the privacy and security program to the Privacy Officer. The Privacy Officer is supported by the Privacy and Security Review Committee, the EHIL, the Manager of Health Informatics, the Data Dictionary Review Committee, and the Scientific Manager. The Privacy Officer holds monthly meetings with the Privacy and Security Review Committee. The Privacy Officer prepares a quarterly report to the Privacy and Security Review Committee and the Leadership Team, and prepares an Annual Report on Privacy and Security to the Leadership Team, the Chief Executive Officer of CHEO, and the Quality Committee of the CHEO Board of Directors. BORN has *Terms of Reference* for the Privacy and Security Review Committee, Data Dictionary Review Committee, Disclosure of Personal Health Information Review Committee, and Privacy Stakeholders Group. The Terms of Reference describe the mandate, membership and reporting structure, meetings, confidentiality and compensation for each of the committees. *Terms of Reference* are reviewed annually.

Risk Management

The *Corporate Risk Management Framework* states that, on an annual basis, the Privacy Officer undertakes a process to identify risks. The Privacy Officer reviews risks in the following areas: power loss; communication loss; data integrity loss; data loss; accidental errors; computer virus; absence of access privilege by employees; natural disasters; unauthorized system access by outsider; theft or destruction of computing assets; and system failure. The Privacy Officer develops the corporate risk management framework. As well, prior to the commencement of a new project, the Privacy Officer works with the project manager to develop a risk management plan to identify, document and manage the risks inherent in the project. The *Framework* also describes how the Privacy Officer identifies risks, how risks are ranked and the recommended risk mitigation actions. The Privacy Officer monitors the *Corporate Risk Register* on a weekly basis. Amendments to the *Corporate Risk Register* require prior approval of the Leadership Team.

The *Maintaining a Consolidated Log of Recommendations Policy* requires that BORN maintain a consolidated and centralized log of all privacy and security related recommendations. The *Consolidated Log of Recommendations* contains recommendations arising from privacy impact assessments, privacy and security audits, investigation of privacy and security breaches and privacy complaints, investigation of privacy and security issues raised by BORN staff, and recommendations made by the IPC. The Privacy Officer creates and maintains the *Log*, reviews

it on an on-going basis, and forwards it to the Privacy and Security Review Committee and the Leadership Team on a quarterly basis.

Business Continuity and Disaster Recovery

BORN has not yet developed a business continuity and disaster recovery plan. It is recommended that BORN develop and implement a policy and associated procedures, in accordance with the requirements in the *Manual*, to protect and ensure the continued availability of the information technology environment of BORN in the event of short and long-term business interruptions, and in the event of threats to the operating capabilities of BORN, including natural, human, environmental and technical interruptions and threats.

Summary of Recommendations

It is recommended that CHEO in respect of BORN develop and implement a written policy and procedures with respect to business continuity and disaster recovery, in accordance with the requirements in the Manual, prior to the next review of its practices and procedures.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that CHEO in respect of BORN 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 August 8, 2011, the practices and procedures of CHEO in respect to BORN have been approved by the IPC.

In order to synchronize the timing of the IPC's review of CHEO in respect of BORN with the reviews of other prescribed persons, this approval will remain effective until October 30, 2011. Prior to October 1, 2011, BORN should submit to the IPC a letter describing significant changes that have been made to the policies and procedures, if any, so that the IPC may review and approve these practices and procedures effective October 31, 2011 for a further period of three years.

Information and Privacy Commissioner of 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