born Ontario
Early health. Lifelong health.
Début en santé. Longue vie en santé.

Children's Hospital of Eastern Ontario in Respect of the Better Outcomes Registry and Network (BORN):

Three-Year Review of the Prescribed Persons and Prescribed Entities

Final
October 2014

Introduction

Established in 2009 to collect, share and rigorously protect critical data about each child born in the province, BORN manages an advanced database that provides reliable, secure and comprehensive information on maternal and child care. The data/information helps professionals in every discipline within the health sector gain vital knowledge they can apply to help facilitate and improve care.

BORN is seeking the continued approval of the BORN Ontario Privacy and Security Management Plan, which includes practices and procedures implemented to protect the privacy of individuals whose personal health information is received by BORN and to maintain the confidentiality of that information.

In seeking this continued approval, this report addresses the elements of the *Three-Year Review of the Prescribed Persons and Prescribed Entities* as set out in the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities, as follows:

- Demonstrates that BORN practices and procedures contain and are compliant to the content set out in "Appendix B"
- Includes details on all Indicators set out in Appendix "C"

Information in this report is current as of October 31, 2013 unless otherwise noted.

Table of Contents

I. Mandatory Requirements and Implementation of, and Adherence to Practices and Procedures

BORN has developed and implemented practices and procedures to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the practices and procedures set out in Appendix "A" of the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities, and is adhering to these practices and procedures.

These practices and procedures contain the content set out in Appendix "B" of the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities. BORN has detailed this compliance in section III Appendix "B": Compliance to IPC Requirements**.**

Adherence to these practices and procedures is acknowledged by all agents of BORN via mandatory annual re-acknowledgement to the BORN Confidentiality Agreement.

II. Statement on Non-compliance

As per the Information and Privacy Commissioner of Ontario process on the Three-Year Review of Prescribed Persons and Prescribed Entities, non-compliance to any of the requirements in Appendix "A" or Appendix "B" of the Manual for the Review and Approval of Prescribed Persons and Prescribed must be treated as follows:

- Provide a rationale on why compliance has not been achieved and outline a strategy for achieving compliance, where the strategy sets out milestones for achieving compliance, the relevant time frames for achieving compliance and the individual responsible for achieving compliance.

The BORN Ontario Privacy and Security Management Plan is non-compliant in the following two areas:

1. **Privacy Policy 12: Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research**
   The BORN privacy policy of the same number and name does not clearly include the following element from "Conditions or Restriction on the Approval":
   - At a minimum, the policy and procedures must require a Data Sharing Agreement to be executed in accordance with the Policy and Procedures for the Execution of Data Sharing Agreements and the Template Data Sharing Agreement prior to any disclosure of personal health information for purposes other than research.

   It is important to note that while the BORN policy and procedure is not clear with respect to the need for a datasharing agreement for this type of disclosure of personal health information, BORN does in fact ensure that data sharing agreements are executed prior to this type of disclosure. The non-compliance is with respect to the *content of the written procedure*, but not with respect to privacy practices in place in the organization.
   Compliance details:
   - Compliance strategy: ensure BORN policy **P-12: Disclosure of Personal Health Information for Purposes Other Than Research** is updated to clearly mandate that a data sharing agreement must be executed prior to the disclosure of any personal health information.
   - Milestone for achieving compliance: February, 2014
     - Update as of February 28, 2014: policy updated to include execution of data sharing agreements.
   - Individual responsible for achieving compliance: BORN Privacy Officer

2. **Organizational Policy 08: Business Continuity and Disaster Recovery Planning**
   The BORN policy of the same number and name is in progress as follows:

   - BORN's head office is located in the Centre For Practice Changing Research building on the campus of the Children's Hospital of Eastern Ontario (CHEO), and CHEO is the System Hosting Provider for the BORN system and all personal health information. As such, BORN is included in the following CHEO business continuity and disaster recovery planning tools:
     - CHEO Emergency Preparedness Manual, including business continuity planning
     - CHEO IT Disaster Recovery Plan (draft version), which addresses:
       - Data Centre protections

        - Cooling System
        - Power Distribution
        - Fire/Smoke detection and suppression
        - Full description of all hardware, including phone systems
        - Contact list and communication protocol (where the BORN Director is included in the list of Key Vendor Contacts)
        - Assessment and containment phases
        - Full shutdown and recovery steps

- To further support business continuity and disaster recovery planning, BORN has in place:
    - Contact list for all employees maintained onsite and offsite; currently being updated to ensure personal e-mail addresses and phone numbers are captured for all BORN staff should internal e-mail be affected by an outage.
    - **BORN Ontario: Outage Communication Process**, for both scheduled and unscheduled outages, including a back-up e-mail system should the CHEO network be affected by an outage.

Compliance details:

- All existing pieces of business continuity and disaster recovery tools and procedures currently in place and in use are being merged into a single BORN policy on Business Continuity and Disaster Recovery Planning. This policy will contain all the content set out in Appendix B to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities.
- Milestone for achieving compliance: June 2015.
- Individual responsible for achieving compliance: BORN Privacy Officer and BORN System Hosting Provider.

III. Appendix "B": Compliance to IPC Requirements

BORN Compliance to IPC Manual Part 1 – Privacy Documentation

1.1 Privacy Policy in Respect in Respect of CHEO's Status as a Prescribed Person

As a prescribed person under the Act, BORN has developed and implemented an overarching privacy policy in relation to the personal health information it receives: **Privacy Policy in Respect of CHEO's Status as a Prescribed Person**.

Status under the Act
The privacy policy describes BORN's status under the act as follows:

- The Children's Hospital of Eastern Ontario is a prescribed person in respect of BORN as per section 13(1) of Ontario Regulation 329/04-General (Regulation) enacted under the *Personal Health Information Protection Act, 2004* for the purposes of facilitating or improving the provision of health care for mothers, infants, and children.

The privacy policy defines the duties and responsibilities that arise from BORN's status as a prescribed person, which include as per section 13(2) of Ontario Regulation 329/04-General (Regulation):

- To have in place practices and procedures to protect the privacy of individuals whose personal health information BORN receives
- To maintain the confidentiality of that information
- These practices and procedures must be approved by the Information and Privacy Commissioner of Ontario every three years
- The BORN privacy policy commits BORN to complying with the provisions and regulation of the *Personal Health Information Protection Act, 2004* applicable to a person holding a registry

Privacy and Security Accountability Framework
The privacy policy designates the President and Chief Executive Officer of CHEO as having ultimate accountability for ensuring compliance with the Act and its regulation and ensuring compliance with BORN's privacy and security policies and procedures. The privacy policy indicates that the President and Chief Executive Officer of CHEO delegates day-to-day responsibility for ensuring compliance with the Act and its regulation and for ensuring compliance with BORN privacy and security policies and procedures to the BORN Leadership Team. The privacy policy further indicates that the Leadership Team delegates day-to-day management of the privacy program to the Privacy Officer and day-to-day management of the security program to the Manager of Health Information, who report to the Leadership Team on all related privacy and security matters.

BORN's privacy policy clearly defines some of the key activities of the privacy and security programs, including:

- Management of the privacy and security program, including monitoring compliance, conducting regular audits and providing reports to senior management and recommendations for changes to policies or procedures
- Execution of privacy training
- Execution and oversight of privacy impact assessments
- Responding to inquiries or complaints related to BORN privacy practices
- Any and all related privacy and security oversight

- Further, the BORN privacy policy indicates that the Privacy Officer works with the CHEO Chief Privacy Officer, the Scientific Manager and the Manager of Health Informatics, and that the following committees form an integral part of the privacy and security framework:
    - Privacy and Security Review Committee
    - Data Collection Review Committee
    - Disclosure of Personal Health Information Review Committee

Collection of Personal Health Information
Prescribed persons under section 39(1)c of the Act are permitted to collect personal health information for the purpose of facilitating and improving the provision of health care. BORN's privacy policy clearly identifies that BORN, as a prescribed person under the Act, collects personal health information only for the purpose of facilitating and improving the provision of health care to mothers, babies and children in the province of Ontario.

The types of personal health information collected by BORN, and from whom, are articulated in the BORN privacy policy and include demographic information and clinical information about fetuses, newborn babies, children and their mothers (including pregnancy history, medical history and a summary of care provided during pregnancy, labor, birth and the newborn period).

The policy sets out that personal health information is collected from health information custodians involved in the care of children, babies and their mothers.

The privacy policy is clear that the collection of personal health information by BORN is consistent with the Act and its regulation, that BORN will not collect personal health information if other information will serve the purpose, and that BORN will not collect more personal health information than is reasonably necessary to meet the purpose.

BORN has implemented policies to ensure that the amount and the type of personal health information collected is limited to that which is reasonably necessary for its purpose and the privacy policy refers to these policies, which are:

- **P-04: Collection of Personal Health Information**, which mandates a rigorous review process by the Data Collection Review Committee
- **P-06: Statements of Purpose of for Data Holdings Containing Personal Health Information**

The BORN privacy policy indicates that the list of BORN data holdings is posted on the BORN website and that an individual may obtain further information in relation to the purposes, data elements and data sources for each data holding from the Privacy Officer, whose contact information is also available on the BORN website.

Use of Personal Health Information
The purposes for which BORN uses personal health information are defined in the BORN privacy policy as follows:

- Identify where appropriate care has not been received and facilitate access to care and treatment for mothers, infants and children (e.g. identifying missed screens and informing the relevant health care provider in order to enable them to offer parents appropriate care for their baby)
- Facilitate continuous improvement of screening thresholds to minimize missed cases
- Raise alerts where maternal and/or newborn outcomes are clinically or statistically discrepant with accepted norms
- Identify strategies to improve the quality and efficiency of care for mothers, infants and children

- Create reports that can be used to provide the Ministry of Health and Long-Term Care, Local Health Integration Networks (LHIN) and Public Heath Units with comprehensive and timely information to support effective planning and management of health care delivery for mothers, babies and children in the province
    - Information provided in reports to the Ministry, Local Health Information Networks and Public Health does not contain personal health information or identify individuals; they only present an overview of aggregated health care data. The reports are carefully reviewed to ensure there is no risk of re-identification through small cell counts or other forms of possible residual disclosure as per policy **P-24: De-Identification and Aggregation**. The reports are made available through the BORN website at www.BORNOntario.ca.

The policy is clear that BORN ensures each identified use of personal health information is consistent with the uses of personal health information permitted by the Act and its regulation, that BORN does not use personal health information if other information will serve the purpose and does not use more personal health information than is reasonably necessary to meet the purpose, using de-identified or aggregate information wherever possible.

The policy also articulates that BORN may use personal health information to conduct research only when the strict requirements of the Act are adhered to, including review by a Research Ethics Board as per BORN Policy **P-10: Use of Personal Health Information for Research**, where in turn BORN permits the use of personal health information for research purposes by BORN agents only when the requirements of section 44 of the Act are met.

The BORN privacy policy indicates that BORN remains responsible for personal health information used by its agents, and that access and use by BORN agents is strictly controlled. Agents are trained on their privacy obligations and sign a Confidentiality Agreement acknowledging the requirements to use only the information necessary for their work, to keep personal health information secure at all times and to notify BORN of any discovered or suspected breach. The privacy policy identifies the following policies in support of these responsibilities:

- **Policy P-08: Limiting Agent Access to and Use of Personal Health Information**
- **Policy P-29: Privacy Breach Management**
- **Policy HR-01 and HR-03: Privacy and Security Training and Awareness**
- **Policy HR-05: Execution of Confidentiality Agreement by Agents**

Disclosure of Personal Health Information

The BORN privacy policy lists the groups to whom and the purposes for which personal health information is typically disclosed, and establishes that any disclosure is in accordance with the Act and its regulation.

The following groups and purposes of disclosure are outlined in the policy:

- To health information custodians, when facilitating access for mothers, babies and children for care and treatment; for example, to ensure appropriate screening is offered in a meaningful timeframe
- To a prescribed entity for the management, evaluation, monitoring or planning for the health system
- To researchers for research purposes as defined in the *Personal Health Information Protection Act, 2004*. Personal health information is provided to researchers only if de-identified information is not sufficient to conduct the research. The research plan must be approved by a Research Ethics Board, meet the requirements set out in the *Personal Health Information*

Protection Act, 2004, and be approved by the Scientific Manager and the Disclosure of Personal Health Information Review Committee who ensure that the minimum amount of personal health information and the least identifiable information is disclosed.

The privacy policy refers to the following policies as the source of information for disclosure of personal health information:

- **Policy P-12: Disclosure of Personal Health Information for Purposes Other Than Research**
- **Policy P-13: Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements**
- **Policy P-24: De-Identification and Aggregation**

The BORN privacy policy lists the groups to whom and the purposes for which **de-identified and/or aggregate** personal health information may be disclosed, which agent at BORN is responsible for reviewing all information prior to disclosure and that the review must ensure that it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual.

The Disclosure of Personal Health Information section of the BORN privacy policy clearly states that BORN does not disclose personal health information if other information serves the purpose and does not disclose more personal health information than is reasonably necessary to meet the purpose. The policy also identifies the following policies that have been implemented with respect to the disclosure of de-identified and/or aggregate personal health information:

- Policy **P-12: Disclosure of Personal Health Information for Purposes Other Than Research**
- Policy **P-13: Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements**
- Policy **P-24: De-Identification and Aggregation**

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

With respect to paper records of personal health information, the BORN privacy policy provides a clear mandate on how they must be retained, converted to electronic format, transferred and securely disposed of.

With respect to electronic records of personal health information, the BORN privacy policy provides a clear mandate on how they are maintained in identifiable format, when and where they are converted to a de-identified format, how they may be securely transferred and disposed of.

Implementation of Administrative, Technical and Physical Safeguards

The BORN privacy policy commits BORN to having in place 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. The policy further clarifies that BORN takes steps to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal. The privacy policy refers to related policies that work together to implement BORN's administrative, technical and physical safeguards which include:

- **Policy S-01: Information Security Policy**
- **Policy S-09: Passwords**
- **Policy S-13: Back-up and Recovery of Records of Personal Health Information**
- **Policy S-14: Acceptable Use of Technology**
- **Policy HR-05: Execution of Confidentiality Agreements by Agents**

Inquiries, Concerns or Complaints Related to Information Practices

The BORN privacy policy refers all inquiries, concerns or complaints related to its privacy policies and procedures and BORN's compliance with the Act and its regulation to the BORN Privacy Officer, whose contact information, including e-mail address, mailing address, and phone number is readily available on the BORN website and throughout BORN's privacy policies.

The BORN privacy policy also states that individuals may direct complaints regarding the compliance of BORN to the Information and Privacy Commissioner of Ontario and provides the IPC mailing address, telephone number and fax number.

Transparency of Practices in Respect of Personal Health Information
The BORN privacy policy indicates that individuals may consult the BORN website for BORN privacy policies and that they may also contact the BORN Privacy Officer.

1.2 Policy and Procedures for Ongoing Review of Privacy and Security Policies, Procedures and Practices

BORN has developed and implemented a joint policy for the ongoing review of privacy and security policies and procedures to ensure ongoing review. The purpose of the review is to determine whether amendments are needed or whether new policies and procedures are required and to ensure that BORN meets or exceeds industry standards and best practices. As per the policy, the Privacy Officer initiates a review of privacy and security policies and procedures annually, or:

- When a serious breach has occurred in which personal health information in BORN's custody or control has been lost, stolen or disclosed without proper authorization
- When an order, fact sheet, guideline or best practice is issued by the Information and Privacy Commissioner
- When amendments are made to the *Personal Health Information Protection Act, 2004* and its regulation that are relevant to BORN as a prescribed registry

The procedure to be followed in undertaking the review is detailed in its presentation of what must be considered including:

- Subject matter expert consultation
- Existing recommendations
- Industry standards and best practices
- Recommendations arising from complaints, enquiries, privacy and security audits and breaches, privacy impact assessments, orders, recommendations, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner
- Amendments to the Act and its regulation
- Whether privacy and security policies and procedures continue to be consistent with actual practices
- Whether there is consistency between and among the privacy and security policies and procedures implemented

The policy identifies what roles in BORN are responsible for reviewing and approving amended policies and procedures, how and by whom updates are to be communicated, including communication materials available to the public and other stakeholders and what documentation must be retained as evidence of review.

The policy indicates a three-month time period for annual reviews.

The policy states that BORN agents must comply with this policy and procedures and that compliance is audited on an ongoing basis by the Privacy Officer in accordance with **P-27: Privacy Audits** and **S-15: Security Audits**.

1.3 Policy on the Transparency of Privacy Policies, Procedures and Practices

BORN has developed and implemented a policy on the transparency of its privacy policies and procedures for the public and stakeholders; this policy is available on the BORN website.
BORN's policy on transparency of its privacy policies and procedures requires the Privacy Officer to work with the Communications Lead to provide information to the public and stakeholders on BORN policies and procedures in language that is clear and non-technical.

As per BORN policy, the following information must be made available on the BORN website and/or brochures:

- A description of BORN privacy policies
- Results from the Information and Privacy Commissioner 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
- Name, title, mailing address and contact information of the Privacy Officer to whom inquiries, concerns or complaints regarding compliance may be directed

The policy further mandates that the following items appear either on the Privacy section of the BORN website and/or in the Privacy Frequently Asked Questions within the Privacy section of the BORN website:

- Status of BORN as a prescribed registry under the Act and its regulation and the duties and responsibilities arising from this status
- A description of the policies and procedures implemented in respect of personal health information
- Types of personal health information collected
- Health information custodians from whom this information is typically collected
- The purposes for which personal health information is collected and used
- The circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to whom it is typically disclosed
- The legal authority for the collections, uses and disclosures
- Administrative, technical and physical safeguards implemented to protect the information against theft, loss, and unauthorized use, disclosure, copying, modification or disposal

1.4 Policy and Procedure for the Collection of Personal Health Information AND Statements of Purpose for Data Holdings Containing Personal Health Information

BORN has in place a combined policy **P-04: Collection of Personal Health Information and P-06: Statements of Purpose for Data Holdings Containing Personal Health Information** to limit the collection of personal health information in accordance with the requirements set forth by the Act and best practices for privacy protection. The policy covers the nature of the personal health information collection, from whom it will be collected and the secure manner in which it will be collected.
The policy clearly states that BORN collects personal health information as follows:

- The collection is permitted by the Act and its regulation
- Does not collect personal health information if other information will serve the purpose of the registry

- Collects the minimum amount of personal health information required to achieve the purpose of the registry

The BORN policy further states that BORN collects only data that has been identified through a rigorous review process as defined in the procedure, where the purpose of the review is to identify the minimum data elements necessary to achieve the registry purpose of facilitating and improving the provision of health care to mothers, infants and children.

The policy identifies that agents must comply with the policy and that compliance is audited on an ongoing basis by the Privacy Officer in accordance with the BORN policy on Privacy Audits.
The policy requires agents to notify the Privacy Officer at the first reasonable opportunity of a privacy breach or suspected breach as per the policy on Privacy Breach Management and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per the policy on Security Breach Management.

Review and Approval Process
Responsibility for this policy at BORN lies with the Data Collection Review Committee and the Privacy Officer, who is also a member of the committee. The Data Collection Review Committee meets annually, at a minimum, and when new collections are being proposed, in order to review the continued operational necessity for each data element and data holding being collected, for any new data elements to be added to the data holdings, to review the existing statements of purpose and to review any requests for new statements of purpose.

The policy identifies the criteria that must be considered by the Data Collection Review Committee in determining whether to recommend approval of the collection of data elements and/or data holdings and their statements of purpose, which includes:

- The collection is permitted by the *Personal Health Information Protection Act, 2004* and its regulation
- Any and all conditions or restrictions set out in the *Personal Health Information Protection Act, 2004* and its regulation have been satisfied
- Other information, namely de-identified and/or aggregate information, will serve the purpose of the Registry, and
- No more personal health information is being requested than is reasonably necessary to meet the purpose of the Registry

The policy further identifies that final approval lies with the BORN Privacy and Security Review Committee and identifies the criteria that must be considered in determining whether to approve the collection of personal health information which includes:

- The collection is permitted by the *Personal Health Information Protection Act, 2004* and its regulation and that any and all conditions or restrictions set out in the *Personal Health Information Protection Act, 2004* and its regulation have been satisfied
- Other information, namely de-identified and/or aggregate information, will serve the purpose of the Registry
- No more personal health information is being requested than is reasonably necessary to meet the purpose of the Registry
- The rationale or statements of purpose for each data element are linked to the need for the data in relation to the identified purpose of the Registry
- There are any risks identified in privacy impact assessments undertaken by BORN regarding new collections (where applicable)

- Any conditions must be satisfied prior to collection

The decision to approve the collection of personal health information, as per the policy, is communicated via e-mail from the chair of the BORN Privacy and Security Review Committee to the Chair of the Data Collection Review Committee.

Conditions or Restrictions on Approval
The BORN policy on the **Collection of Personal Health Information** sets out that that:

- The Privacy Officer is responsible for ensuring that a signed data sharing agreement is executed before data are collected, or, where revisions are made, that a revised data sharing agreement must be completed before data collection proceeds; BORN statements of purpose are outlined in data sharing agreements
- The Privacy Officer is responsible for ensuring any new statements of purpose are communicated to the Health Information Custodians from whom the personal health information in the data holding was collected
- The chair of the Data Collection Review Committee has responsibility for ensuring that any conditions or restriction on approval identified in the approval from the Privacy and Security Review Committee are satisfied

Secure Retention
Records will be maintained in identifiable form within the transactional database for 28 years and then converted to a de-identified format as per BORN policy S**-05: Secure Retention of Records of Personal Health Information** and **BORN policy P-25 De-Identification and Aggregation**.

Secure Transfer
Secure transfer is outlined in the policy as follows:
Personal health information is collected electronically through secure internet connections and may involve manual data entry and automated extraction and uploading from existing hospital information systems and lab information systems.
See policy S-07: Secure Transfer of Records of Personal Health Information.

Secure Return or Disposal
Secure return and disposal of personal health information is outlined as follows:
BORN maintains personal health information in identifiable format for 28 years and then converts it to a de-identified format. As per all BORN collection data sharing agreements, if it is determined that personal health information is no longer required by BORN for the purpose of improving or facilitating the provision of health care, it will be securely destroyed as per BORN policy **S-08: Secure Disposal of Records of Personal Health Information**. BORN does not return records of personal health information.

1.5 List of Data Holdings Containing Personal Health Information

BORN has in place a policy that includes an up-to-date list of the unique data holdings it maintains. This list includes a brief description of each of the data holdings as follows:

#	Data Holding	Description
1	BORN Information System (BIS)	A single data holding comprised of Personal Health Information collected from the following health information custodians: 1. Prenatal and Newborn screening providers

		2. Hospitals 3. Midwives 4. Outpatient clinics 5. Fertility clinics
2	FAN (Fetal Alert Network) historical database	The historical dataset from one of BORN's founding members.
3	Prenatal Screening Ontario (PSO)	The historical dataset from one of BORN's founding members.
4	Niday Perinatal and NICU/ICU Database	The historical dataset from one of BORN's founding members.
5	Ontario Midwifery historical database	The historical dataset from one of BORN's founding members.
6	CARTR (Canadian Assisted Reproductive Technology) historical database	Historical fertility data.

1.6 Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information

See section 1.4 above; BORN has in place a combined policy **P-04: Collection of Personal Health Information and P-06: Statements of Purpose for Data Holdings Containing Personal Health Information**.

1.7 Statements of Purpose for Data Holdings Containing Personal Health Information

BORN has in place policy **P-07 Evidence: Statements of Purpose for Data Holdings Containing Personal Health Information** that identifies six statements of purpose for which BORN may collect personal health information as a prescribed registry. The policy indicates that the BORN Data Dictionary maps data collected by BORN to one or more of these statements of purpose. The six approved statements of purpose are:

1. Identifying where appropriate care has not been received and facilitating access to care and treatment for mothers, infants and children. For example, identifying missed screens and informing the relevant health care provider in order to enable them to offer parents appropriate care for their baby
2. Facilitating continuous improvement of healthcare delivery tools to minimize adverse outcomes. For example, improvement of screening algorithm and cut-offs to minimize missed screens.
3. Raising alerts where maternal and/or newborn outcomes are statistically discrepant with accepted norms. For example, an increase in congenital anomalies associated with a specific geographic region suggesting a toxic exposure or a provider being identified as performing too many episiotomies as compared to peers, leading to poor maternal outcomes.
4. Enabling health care providers to improve care by providing them the information and tools to compare themselves with peers and/or benchmarks.
5. Knowledge translation to improve the quality and efficiency of care for mothers, infants and children. For example, identifying strategies for health information custodians for continuous quality improvement.
6. Creating reports that can be used to provide the Ministry of Health and Long-Term Care, LHINs and Public Heath Units with comprehensive and timely information to support effective

planning and management of health care delivery for mothers, babies and children in the province.

1.8 Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information

BORN has in place policy **P-08: Limiting Agent Access to and Use of Personal Health Information**. The policy defines a BORN agent, and states that access to personal health information by BORN agents is based on the "need to know" principle that is controlled via role-based access.

The policy prohibits access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose and the policy requires agents to access and use the minimum amount of identifiable information reasonably necessary for carrying out their day-to-day employment, contractual or other responsibilities with BORN.

The policy defines seven levels of access to personal health information, where the purpose of each level of access and use is explained as follows:

1. Authorization to read
2. Authorization to enter
3. Authorization to create new users
4. Authorization to use personal health information, where the term use:
    - Includes handling the personal health information, analyzing the information for the purposes of the prescribed registry, disposing of the information, modifying the information in order to conceal identities, and includes the provision of personal health information to an agent of BORN
5. Authorization to edit
6. Authorization to delete personal health information
7. Authorization to access application code

The policy prohibits agents from using de-identified and/or aggregate information, either alone or with other information to identify an individual, including attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

Review and Approval Process

As per the policy, the immediate supervisor of an agent completes an Agent Data Access Form, recommending a particular level of access as per the seven levels outlined above, and why, and submits it to the Privacy Officer along with a copy of the job specification or contract. The policy states that the supervisor must consider the following criteria in making a recommendation:

- The agent routinely requires access to and use of personal health information on an ongoing basis or for a specified period for his or her employment, contractual or other responsibilities
- De-identified and/or aggregate information will not serve the identified purpose
- No more personal health information will be accessed and used than is reasonably necessary to meet the identified needs of the role
- The access and use recommendations meet and do not exceed the functions to be performed as per the BORN job specification or contract
- The data will be used in a manner that is consistent with the purposes for which it was originally collected
- Any conditions or restrictions to be imposed on access and use (i.e. no access to specified data elements)

- Rationale for the recommendations

The Agent Data Access Form identifies:

- The purpose for which access is required
- The data holdings to which access is required
- The level of access required
- The time frame for access and use

The policy sets out that the Privacy Officer reviews the application form and supporting documentation and recommendation and considers all criteria, including:

- The identified purpose for which access to and use of personal health information is requested is permitted by the *Personal Health Information Protection Act, 2004* and its regulation, and cannot be reasonably accomplished without Personal Health Information
- Functions to be performed as per BORN job specification or contract
- Where permission is requested to disclose personal health information, such disclosures are permitted by the *Personal Health Information Protection Act, 2004* and its regulation

Conditions or Restriction on the Approval

The BORN policy on **Limiting Agent Access to and Use of Personal Health Information** sets out two methods for imposing conditions:

1. The Agent Data Access Form that is completed for each agent granted access to and use of personal health information defines seven levels of access including read, write, create, update and delete, where the supervisor selects only those levels that are needed for the agent to perform his or her role;
2. The Agent Data Access Form includes an entry for additional conditions that may be stipulated by the supervisor and which are tracked on BORN Log of Agents Granted Approval to Access/Use/Disclose personal health information.

The BORN policy sets out that the Agent Data Access Form defines the time frame for which the access is approved. The BORN System Administrator enters this information into the BORN Information System which automates the end date (removes access automatically on the end date).

As per the policy, all approved accesses and uses of personal health information are subject to an automatic expiry after one year or sooner based on the Agent Data Access Form. Agents and their supervisors request approval on an annual basis one year from the date the approval is granted.

The policy does not cover disclosure of personal health information as BORN agents do not need to disclose personal health information in their day-to-day work. The Scientific Manager or designate (BORN Research Coordinator) are the only two BORN agents who are authorized to disclose personal health information, as detailed in the BORN policies on **Disclosure of Personal Health Information for Purposes Other Than Research** and **Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements**.

Notification and Termination of Access and Use

The policy sets out that The BORN agent and the supervisor of an agent granted approval to access and use personal health information must notify the Privacy Officer and the System Administrator via e-mail as soon as a decision is taken to terminate or to make any changes that would impact the level and type of access and use required by that agent in compliance with BORN policy **HR-10: Termination or Cessation of the Employment or Contractual Relationship** which states:

1. Agents and their supervisors are required to notify the BORN Director and the Privacy Officer of the termination of an employment or contractual relationship two weeks in advance, if possible. The notification must be via e-mail and contain the following information:
    a. Name of Agent
    b. Termination date
    c. Reasons for termination
2. Within three days, the BORN Director, or designate forwards the name of the agent and the termination date to the Manager of Health Informatics who arranges for the withdrawal of access to personal health information on termination date and updates BORN log **P-09: Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information**

Secure Retention
The BORN policy states that an agent who is granted approval to access and use personal health information by BORN must securely retain the records of personal health information in compliance with BORN policy **S-05: Secure Retention of Records of Personal Health Information**.

Secure Disposal
The BORN policy states that an agent granted approval to access and use personal health information must securely dispose of the records of personal health information in compliance with BORN policy **S-08: Secure Disposal of Records of Personal Health Information**.

Tracking Approved Access to and Use of Personal Health Information
The BORN policy states that the BORN System Administrator maintains a log of agents granted approval to access, use and disclose personal health information by BORN. The log is BORN **P-09: Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information** and is supported by BORN policy **S-10: System Control and Audit Logs**.

Compliance, Audit and Enforcement
The policy is clear that BORN agents must comply with the policy and procedures and that compliance is audited on an ongoing basis by the Privacy Officer in accordance with **P-27: Privacy Audits**. The policy further states that agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per **S-17: Security Breach Management** as appropriate and that consequences of breach are detailed in each respective breach policy.

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

BORN maintains a log of agents granted approval to access and use personal health information. The log includes the following fields:

- Name of Agent
- Data Holding
- Level and type of access
- Any conditions imposed on access
- Data access granted
- Level and type of use
- Data use granted
- Any condition imposed on use
- Level and type of disclosure
- Any conditions imposed on disclosure

- Timeframe that applies to the authorization (if less than one year)
- Date access terminated
- Reason access terminated

1.10 Policy and Procedures for the Use of Personal Health Information for Research

BORN has in place policy **P-10: Use of Personal Health Information for Research** to identify the circumstances under which agents are permitted to use personal health information for research.

The policy prohibits the use of personal health information for research if other information will serve the research purpose and states that no more personal health information will be used than is reasonably necessary to meet the research purpose.

The policy states that agents must comply with the policy and that compliance is audited on an ongoing basis by the Privacy Officer in accordance with policy **P-27: Privacy Audits**. Where an agent is found to be non-compliant with the policy, it is clear that the provisions in the BORN policy **HR-11: Discipline and Corrective Action** will apply, up to and including termination of employment.

The policy requires agents to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management** as appropriate.

Where the Use of Personal Health Information is Permitted for Research

The policy sets out that BORN permits use of personal health information for research purposes as authorized under *Personal Health Information Protection Act, 2004* where:

- BORN agents meet the requirements for research provided in *Personal Health Information Protection Act, 2004* section 44 and associated regulations.
- The purpose for the use is in accordance with the stated purpose for the Registry

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

As per the policy, when the Scientific Manager is reviewing the request by an agent to use personal health information for research, there is a requirement to confirm that the request constitutes a research use, where a request is NOT research if it:

- Does not test a specified hypothesis
- Is intended to provide data for quality improvement or resource allocation analysis
  Relates to improving care for a specific individual

Review and Approval Process

The BORN policy identifies that BORN agents may request the use of personal health information for research by submitting to the Scientific Manager a BORN data request form, a written research plan and a copy of the decision of a research ethics board approving the research.

The BORN policy further identifies the following review steps undertaken by the Scientific Manager in determining whether to approve the request to use personal health information for research:

- Determine that the research plan complies with the requirements of *Personal Health Information Protection Act, 2004*
- Confirm that the research plan has been approved by a Research Ethics Board
- Determine that the purpose for the use is in accordance with the stated purpose for the prescribed Registry

- Determine that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the Research Ethics Board
- Determine whether aggregate data or de-identified information could meet the identified research need where personal health information is being requested
- Where personal health information is being requested, the Scientific Manager or designate works with the researcher to compile a list of data elements in support of the research request. The purpose of this process is to ensure that the minimum number of data elements and the least identifiable information are used while maintaining the feasibility of the research project

The Scientific Manager submits the reviewed request to the BORN Privacy and Security Review Committee for ultimate approval. The Scientific Manager provides to the committee the following:

- Data Request Form
- Research plan
- A copy of the decision of a Research Ethics Board that approved the research plan
- Any relevant electronic correspondence with the agent regarding the research request
- List of agreed-upon data elements

The policy defines that where the Privacy and Security Review Committee approves a request, the Scientific Manager prepares a letter of approval and communicates this electronically to the agent making the request. The content of the approval letter is outlined in the policy.

Conditions or Restrictions on the Approval

As per the policy, approved requests are conditional on the execution of a BORN Confidentiality Agreement, which is done by the Privacy Officer. The Confidentiality Agreement contains a clause reminding an agent that he/she is responsible and accountable for ensuring they act in accordance with the provisions of the Act and its regulation.

The policy identifies the Privacy Officer as the agent responsible for monitoring the BORN agent's compliance with any conditions or restriction on the use of the personal health information.

Secure Retention

BORN agents granted approval to use personal health information for research purposes may only access the data on a secure, encrypted drive equipped with appropriate access controls, as per BORN policy **S-05: Secure Retention of Records of Personal Health Information** and ensures that secure retention is compliant to the Research Ethics Board approved written research plan.

Secure Return or Disposal

The policy states that agents granted approval to use personal health information for research purposes are required to securely dispose of the records of personal health information and provide the BORN Privacy Officer with a certificate of destruction (BORN's official Certificate of Destruction, which is compliant to the BORN policy on **Secure Disposal of Records of PHI**) that includes the following information:

- List of the records of personal health information to be securely destroyed
- The date, time and method of secure disposal employed
- The name and signature of the agent(s) who performed the secure disposal and a person who witnessed the destruction

Certificates of destruction must be received within one week of the date of destruction set out in the written research plan. If the certificate of destruction is not received by the Privacy Officer in stated time period, the policy indicates that the agent is in breach of the policy and BORN may take measures as per

the BORN policy on Discipline and Corrective Action and BORN may also notify the agent's professional body, the Information and Privacy Commissioner and any other suitable oversight body that the agent is in breach.

Tracking Approved Uses of Personal Health Information for Research
As per the policy, the Scientific Manager or designate is responsible for maintaining the BORN **Log of Approved Uses of Personal Health Information for Research.**

The policy also states that the Scientific Manager or designate is responsible for securely retaining the following documentation:

- Data Request form
- Written research plan
- A copy of the decision of a Research Ethics Board that approved the research plan
- List of agreed-upon data elements
- Scientific Manager's letter of approval
- Approval from the Privacy and Security Review Committee, where applicable
- Log of Approved Uses of Personal Health Information for Research

The policy establishes that the Privacy Officer is responsible for securely retaining:

- Signed Confidentiality Agreements for all agents
- Certificates of Destruction

Use of De-identified Information for Research
The BORN policy on **Use of Personal Health Information for Research** includes procedures for using de-identified Information for research and using aggregate information for research.

As per policy directions, due to the sensitive nature of de-identified information, it is to be treated as personal health information and follows the same procedure as Use of Personal Health Information for Research with the following two differences:

- There is no need for approval by the BORN Privacy and Security Review Committee
- The BORN definitions of de-identified information and aggregate information are contained in policy **P-24: De-Identification and Aggregation**. As per this policy, BORN uses the Privacy Analytics Re-Identification Risk Assessment and De-Identification Tool (PARAT) for empirical assessment regarding risk of re-identification.

As per policy directions, use of aggregate information for research also follows the same review and approval process, with no need for approval by the BORN Privacy and Security Review Committee.

The policy states that agents are prohibited from using the de-identified information or aggregate information, either alone or with other information, to identify an individual, including attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. This is done via the Confidentiality Agreement.

1.11 Log of Approved Uses of Personal Health Information for Research

BORN maintains **P-11: Log of Approved Uses of Personal Health Information for Research** that includes:

- Name and identification number of research study
- Agent last name/Agent first name
- Date of Research Ethics Board approval
- Date of BORN approval
- Date Personal Health Information provided to Agent

- Nature of Personal Health Information
- Retention period as per Research Ethics Board plan
- Date of secure disposal of personal health information/certificate of destruction received

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

BORN has in place a policy on disclosure of personal health information for purposes other than research stating that BORN only discloses personal health information for those purposes authorized by the *Personal Health Information Protection Act, 2004* and its regulation.

The policy is clear that BORN will not disclose personal health information if other information will serve the purpose and will not disclose more personal health information than is reasonably necessary to meet the purpose.

Compliance, audit and enforcement are defined as follows in the policy:
BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with **P-27: Privacy Audits**.
Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

Where the Disclosure of Personal Health Information is Permitted
As per the BORN policy, BORN permits the disclosure of personal health information for purposes other than research only in the following circumstances in accordance with *the Personal Health Information Protection Act, 2004* and its regulation:

1. For the purpose of carrying out a statutory or legal duty as per section 49(1) (b) of the *Personal Health Information Protection Act, 2004*
2. For the purpose for which the health information custodian was authorized to disclose the information under the *Personal Health Information Protection Act, 2004* section 49(1)(a)
3. To a prescribed planning entity under regulation section13(5) of the *Personal Health Information Protection Act, 2004*
4. To a health data institute under section 13(5) and section 47 of the *Personal Health Information Protection Act, 2004*

Review and Approval Process
The policy clearly defines the agent(s) responsible for receiving and reviewing requests for the disclosure of personal health information. The Scientific Manager receives all requests and reviews them with the Manager of Health Informatics and the Privacy Officer. The policy further defines that approvals are the responsibility of the Disclosure of Personal Health Information Review Committee. The documentation requirements with respect to review and approval are also stated (what must be completed and by whom), including:

- Requestor submits a Data Request Form
- Scientific Manager submits to the Disclosure of Personal Health Information Review Committee for their review and approval the following:
    - Background of the project including how it aligns with BORN purposes
    - Rationale for the recommendation to approve the disclosure
    - List of agreed-upon data elements

- Method of disclosure
- Results of the review by the Scientific Manager, Manager of Health Informatics and Privacy Officer
- Any relevant electronic correspondence

As per the policy, the following criteria are considered in the review phase of a request for disclosure of personal health information for purposes other than research:

- Determine if the disclosure is permitted or required under the *Personal Health Information Protection Act, 2004* and its regulation
- Determine if the purpose for the disclosure is in accordance with the stated purpose for the BORN Registry
- Confirm that the personal health information is indeed reasonably required for the purpose and that no other information, such as de-identified or aggregate information would suffice for the purpose
- Confirm that the amount of information that is requested is limited to the minimum amount reasonably required to meet the purpose

Where the Disclosure of Personal Health Information Review Committee approves the disclosure, each member sends their approval via e-mail to the Scientific Manager who prepares an official letter of approval which sets out:

- Purpose of the project
- Rationale for the approval of the use for non-research purposes
- Any conditions or restrictions that will be imposed
- List of agreed-upon data elements

Approvals are conditional on the execution of a data sharing agreement.
The Scientific Manager or designate:

- Communicates the approval to the health information custodian
- Forwards to the Privacy Officer and the Scientific Manager letter or approval, along with a link to the secure BORN drive containing the supporting project documentation.

The Scientific Manager updates the Data Tracking Log.

Conditions or Restrictions on the Approval
The BORN policy sets out that a data sharing agreement must be executed with the data recipient as per BORN policy **P-16: Data Sharing Agreements** and as per **P-17: Template Data Sharing Agreement: Disclosure of Personal Health Information.** The Privacy Officer executes the agreement and informs the Scientific Manager.

When the data set has been prepared, the policy identifies that the Scientific Manager:

- Cross checks the data generated or built as per the method of disclosure approved by the Disclosure of Personal Health Information Committee against the list of agreed-upon data elements in the data sharing agreement
- Ensures that any conditions or restrictions have been satisfied
- Ensures the data set is password protected or equivalent

Secure Transfer
The policy requires that records of personal health information are securely transferred, compliant to policy **S-07: Secure Transfer of Records of Personal Health Information**. The specific method of transfer is documented in the data sharing agreement. The health information custodian confirms receipt of the data to the Scientific Manager or designate, who updates the Data Tracking Log.

The policy also states that disclosures to a prescribed entity or data institute are done using the secure network provided by the prescribed entity or data institute. The prescribed entity or data institute e-mails the Scientific Manager or designate confirming arrival. The Scientific Manager or designate records the date of disclosure and receipt of the data set information in the Data Tracking Log.

Secure Return or Disposal
The data sharing agreement specifies data retention dates and method, notification and verification of the disposal of personal health information. The recipient must comply with the requirements set out in the data sharing agreement, and provide a certificate of disposal to the Privacy Officer within the timeframes set out in the data sharing agreement.

The Document Management System flags the disposal date for the Privacy Officer for follow-up. The Privacy Officer ensures that the recipient is contacted regarding the disposal date if the Privacy Officer has not received the certificate of destruction on the date set out in the data sharing agreement, as applicable.

As per policy guidelines, If action is not taken by the recipient within seven days of the disposal date in the data sharing agreement, the recipient is in breach of the Agreement and BORN may take all measures authorized by the Agreement. BORN may also notify the Information and Privacy Commissioner that the recipient is in breach and lodge a complaint.

Documentation Related to Approved Disclosures of Personal Health Information
The Scientific Manager has responsibility for the secure retention of:

- Data Request Form
- Data Tracking Log
- Correspondence between the requestor and BORN
- Relevant documentation from the Privacy Analytics Re-Identification Risk Assessment and De-Identification Tool (PARAT) regarding empirical assessment regarding risk of re-identification

The Privacy Officer has responsibility for the secure retention of all data sharing agreements.

Disclosure of De-identified or Aggregate Information
BORN limits the disclosure of personal health information to those purposes permitted under the *Personal Health Information Protection Act, 2004* and its regulation. The policy contains a complete procedure for the disclosure of de-identified information for purposes other than research, as well as a complete procedure for the disclosure of aggregate data for purposes other than research.

Review and Approval Process for De-identified Information and Aggregate Information
The policy states that the Scientific Manager or designate reviews a submitted Data Request Form to:

- Determine if the disclosure is permitted or required under the *Personal Health Information Protection Act, 2004* and its regulation
- Determine that the purpose for the disclosure is in accordance with the stated purpose for the prescribed Registry as defined in policy **P-07: Evidence: Statements of Purpose for Data Holdings Containing Personal Health Information** (where purposes are listed under A – F).
- Confirm that the amount of information that is requested is limited to the minimum amount reasonably required to meet the purpose. The Scientific Manager works with the requestor to compile a list of data elements in support of the request. The purpose of this process is to ensure that the minimum number of data elements and the least identifiable information are used while maintaining the feasibility of the project. This process generally requires at least one and sometimes two or more meetings to discuss the project and data.

The policy sets out that, prior to the provision of the de-identified data, the Scientific Manager undertakes a final review of the data to identify any residual risk of re-identification (ensures the data set does not identify an individual and that is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual).

Approved requests are communicated electronically by the Scientific Manager or designate to the requestor.

The Scientific Manager or designate prepares an official letter of approval which sets out:

- Purpose of the project
- Rationale for the approval of the use for non-research purposes
- Any conditions or restrictions that will be imposed
- List of agreed-upon data elements

Approvals of the disclosure of de-identified information are conditional on the execution of a data sharing agreement.

The Scientific Manager or designate forwards to the Privacy Officer the letter of approval, along with a link to the secure BORN drive containing the supporting project documentation.

Approved requests for aggregate information are communicated electronically by the Scientific Manager or designate to the requestor.

The Scientific Manager updates the Data Tracking Log.

Conditions or Restrictions on the Approval
Data Sharing Agreement
The policy states that approvals are conditional on the Privacy Officer executing a data sharing agreement with the individual or organization as per policy **P-16: Data Sharing Agreements** and as per **P-17: Template Data Sharing Agreement: Disclosure of Personal Health Information** after which the Privacy Officer:

- Informs the Scientific Manager that the data sharing agreement has been fully executed
- Enters the disposal date into the BORN Document Management System and updates policy **P-18 Log of Data Sharing Agreements**. The monitoring capabilities of the Document Management System flag the disposal date for the Privacy Officer for follow-up.
- Sends a copy of the executed data sharing agreement to the recipient

The Scientific Manager or designate updates the Data Tracking Log.

The signed data sharing agreement requires the recipient to acknowledge that they will not use the de-identified information, either alone or with other information, to identify an individual.

Where aggregate information is being disclosed, the recipient is required to acknowledge by e-mail:

- Receipt of the information
- Confirmation that no attempt will be made to identify an individual using this information either alone or with other information

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

BORN has in place a policy to ensure that it only discloses personal health information for research purposes in accordance with the *Personal Health Information Protection Act, 2004* and its regulation. Researchers must meet the requirements for research disclosure provided in section 44 of the Act and associated regulations.

The policy states clearly that BORN will not disclose personal health information for research purposes if other information will serve the research purpose and BORN will not disclose more personal health information than is reasonably necessary to meet the identified research purpose.

Compliance, audit and enforcement are defined as follows in the policy:

- BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with **P-27: Privacy Audits**.
- Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

Where the Disclosure of Personal Health Information is Permitted for Research
The BORN policy sets out that BORN permits personal health information to be disclosed for research purposes in accordance with the Act and its regulation and where researchers meet the requirements for research disclosure in section 44 of the Act and where the following review and approval steps are met.

Review and Approval Process
The BORN policy defines the following process to receive and review a request for personal health information for research:
Researchers requesting disclosure of personal health information must submit to the Scientific Manager:

- A completed Data Request Form (available on the BORN website)
- A research plan, where the research plan must be in writing and must fulfill the requirements set out in section 44(2) of the *Personal Health Information Protection Act, 2004* and section 16 of the regulation
- A copy of the decision of a Research Ethics Board that approved the research plan

The policy sets out that the Scientific Manager conducts a further review to:

- Determine that personal health information disclosure is authorized by *Personal Health Information Protection Act, 2004*
- Confirm that the research plan has been approved by a Research Ethics Board
- Determines that the purpose for the disclosure is in accordance with the stated purpose of BORN
- Determine that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the Research Ethics Board
- Determines if the data are available to answer the research question
- Considers the scientific merit (whether the data and approach are appropriate to answer the question) and whether there is opportunity for collaboration with others working on a similar question
- Determines whether aggregate data or de-identified record-level data would meet the identified research need
- Assesses potential risk of harm to a group or individual as a result of releasing the data

Where personal health information is being requested, the Scientific Manager or designate works with the researcher to compile a list of data elements in support of the research request. The purpose of this process is to ensure that the minimum number of data elements and the least identifiable information

are used while maintaining the feasibility of the research project. This process generally requires at least one and sometimes two or more meetings to discuss the project and data.

Once the Scientific Manager has completed a thorough review, the Scientific Manager forwards the request to the Disclosure of Personal Health Information Review Committee for their review and approval and provides the following:

- Data Request Form
- Research plan
- A copy of the decision of a Research Ethics Board that approved the research plan
- Any relevant electronic correspondence with the agent regarding the research request
- List of agreed-upon data elements
- Any relevant correspondence with the researcher

Where the Disclosure of Personal Health Information Review Committee approves the disclosure, the policy identifies that each member sends their approval via e-mail to the Scientific Manager.
The Scientific Manager prepares an official letter of approval which sets out:

- Purpose of the research
- Rationale for the approval of the use for research purposes
- Any conditions or restrictions that will be imposed
- List of agreed-upon data

Approved requests are communicated electronically by the Scientific Manager to the researcher. Approvals are conditional on the execution of a BORN research agreement.

The Scientific Manager or designate forwards to the Privacy Officer:

- Data Request Form
- Research plan
- A copy of the decision of a Research Ethics Board that approved the research plan
- List of agreed-upon data elements
- Approval from the Disclosure of Personal Health Information Review Committee
- Scientific Manager's letter of approval

Conditions or Restrictions on the Approval
The BORN policy sets out that the Privacy Officer or designate executes a research agreement as using the BORN Template Research Agreement with the researcher and:

- Informs the Scientific Manager or designate that the research agreement has been fully executed
- Enters the disposal date into the BORN Document Management System. The monitoring capabilities of the Document Management System flag the disposal date for the Privacy Officer for follow-up.
- Updates the **Log of Research Agreements**
- Sends a copy of the executed Research Agreement to the researcher

The policy includes the following list of check points for the Scientific Manager or designated to verify prior to the release of data:

- Cross checks the information on the specification list against the data element list on the research agreement
- Ensures that any conditions or restrictions have been satisfied
- Ensures the data set is password protected

Secure Transfer

The Scientific Manager or designate transfers the data set as per policy **S-07: Secure Transfer of Records of Personal Health Information**. The health information custodian must call the BORN Scientific Manager or designate to confirm receipt of the data and to obtain the password.
The Scientific Manager of designate updates the Data Tracking Log and the Log of Research Agreements as applicable.

Secure Return or Disposal
In accordance with the Research Agreement which specifies data retention dates and method, notification and verification of the disposal of personal health information, the researcher must destroy the personal health information and provide confirmation of disposal as per the applicable Research Agreement.

The Document Management System flags the disposal date for the Privacy Officer for follow-up. The Privacy Officer ensures that the researcher is contacted regarding the disposal date if the researcher has not provided BORN with written confirmation of disposal as per the requirements of the Research Agreement within seven days of the disposal date.

All certificates of destruction provided by researchers must include the following information:

- List of the records of personal health information to be securely destroyed
- Description of the secure disposal of the records
- The date, time and method of secure disposal employed
- The name and signature of the agent(s) who performed the secure disposal, and a person who witnessed the destruction

The Privacy Officer must receive certificates of destruction within one week of the date of destruction set out in Research Agreement.

If the certificate of destruction is not received within this time period, the researcher is in breach of the Agreement and BORN may take all measures authorized by the Research Agreement. BORN may also notify the researcher's professional body, the Information and Privacy Commissioner and any other suitable oversight body that the researcher is in breach and, where appropriate, lodge a complaint against the researcher.

Documentation Related to Approved Disclosures of Personal Health Information for Research
As per the policy, the following documents are maintained and securely stored:
The Privacy Officer is responsible for the secure retention of:

- Signed Research Agreement
- Certificate of destruction
- Results of any audits performed by BORN

The Scientific Manager or designate is responsible for the secure retention of:

- Correspondence between the researcher and BORN
- Data Request Form
- Research plan
- Decision of the Research Ethics Board that approved the research plan
- Approval of the Disclosure of Personal Health Information Review Committee
- Data Tracking Log
- Log of Research Agreements

Disclosure of De-identified or Aggregate Information for Research
BORN limits the disclosure of personal health information to those purposes permitted under the *Personal Health Information Protection Act, 2004* and its regulation. The policy contains a complete

procedure for the disclosure of de-identified information for research, as well as a complete procedure for the disclosure of aggregate data for research.

Review and Approval Process
The BORN policy on Disclosure of Personal Health Information for Research includes a complete procedure on disclosing de-identified Information for research and disclosing aggregate information for research. As per policy directions, due to the sensitive nature of de-identified information, it is to be treated as personal health information and follows the same procedure as Disclosure of Personal Health Information for Research with the following two differences:

- There is no need for approval by the BORN Disclosure of Personal Health Information Review Committee
- The BORN definitions of de-identified information and aggregate information are contained in policy **P-24: De-Identification and Aggregation**. As per this policy, BORN uses the Privacy Analytics Re-Identification Risk Assessment and De-Identification Tool (PARAT) for empirical assessment regarding risk of re-identification.

Agents are prohibited from using the de-identified information or aggregate information, either alone or with other information, to identify an individual, including attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. This is done via the Confidentiality Agreement.

The Scientific Manager undertakes a final review of the data to ensure that it does not identify an individual and that is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual

1.14 Template Research Agreement

BORN has in place a **Template Research Agreement** that is required to be executed by a researcher to whom personal health information will be disclosed prior to the disclosure occurring. The agreement addresses the matters set out below.

General Provisions
The research agreement includes a description of the status of the Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network (BORN) under the Act, as well as associated responsibilities arising from the Act. In addition the template agreement contains a provision that specifies the precise nature of the personal health information being disclosed by BORN for research purposes, and it provides a definition of personal health information that is consistent with the Act and its regulation.

Purposes of Collection, Use and Disclosure
The research purpose for which the personal health information is being disclosed by BORN and the purposes for which the personal health information may be used or disclosed by the researcher are identified in the Research Agreement template. In addition it includes the statutory authority for each collection, use and disclosure identified.

The BORN **Template Research Agreement** only permits the researcher to use the personal health information for the purposes set out in the written research plan approved by the research ethics board, and further it prohibits the use of the personal health information for any other purpose. The Research Agreement also prohibits the researcher from permitting persons to access and use the personal health

information except those persons described in the written research plan approved by the research ethics board.

The BORN **Template Research Agreement** contains a provision to limit linking of data as follows: *The recipient shall not link the data with any other administrative, clinical or other external public or privacy data sources except as set out in the approved Research Agreement*. As per the BORN policy on Disclosure of Personal Health Information for Research Purposes, a research agreement is dependent on a written research plan and research ethics board approval.

The BORN **Template Research Agreement** reflects that the researcher acknowledges the personal health information being disclosed pursuant to the Research Agreement is necessary for the identified research purpose and that other information, namely de-identified and/or aggregate information, will not serve the research purpose. The researcher must also acknowledge, via the agreement, that no more personal health information is being collected and will be used than is reasonably necessary to meet the research purpose.

The agreement imposes restrictions on the disclosure of personal health information, including:

- The researcher acknowledges and agrees not to disclose the personal health information except as required by law and subject to the exceptions and additional requirements prescribed in the regulation to the Act
- The researcher acknowledges and agrees not to publish the personal health information in a form that could reasonably enable a person to ascertain the identity of the individual; and not to make contact or attempt to make contact with the individual to whom the personal health information relates, directly or indirectly, unless the consent of the individual being contacted is first obtained in accordance with subsection 44(6) of the Act.

Compliance with the Statutory Requirements for the Disclosure for Research Purposes
The agreement sets out that the researcher and BORN acknowledge and agree that the researcher has submitted an application in writing, a written research plan that meets the requirements of the Act and its regulation, and a copy of the decision of the research ethics board approving the written research plan.

The agreement also indicates that the researcher must also be required to acknowledge and agree that they will comply with the Research Agreement with the written research plan approved by the research ethics board and with the conditions, if any, specified by the research ethics board in respect of the research plan.

Secure Transfer
The BORN **Template Research Agreement** sets out the secure manner in which records of personal health information will be transferred. The template agreement states that BORN transfers personal health information to the researcher as determined in BORN's sole discretion by using a secure FTP server and password protection process, where the secure FTP is an application which can be accessed via industry standard, encrypted, secure socket layer sessions, and that this method is compliant with the BORN policy on secure transfer of records of personal health information. In addition the BORN **Template Research Agreement** contains a provision stipulating that the researcher shall ensure that no transfer of personal health information outside of Canada occurs, and that no personal health information is accessed from a location outside of Canada without the express prior and written authorization of BORN**.**

Secure Retention
The agreement identifies the retention period for the records of personal health information including the length of time that the records of personal health information will be retained in the identifiable form which must be consistent with the written research plan approved by the research ethics board.

The template requires the researcher to ensure that the records of personal health information are retained in a secure manner and states that the researcher shall at all times maintain reasonable physical, procedural, technical and general security measures so as to protect personal health information against any loss, theft, accidental or unlawful modification or destruction or unauthorized use, disclosure, access, copying or transfer. In addition the agreement states that the researcher shall include all measures described in the Research Plan and in the Data Request Form and be reasonable in the circumstances.

Secure Return or Disposal
The BORN **Template Research Agreement** requires records of personal health information be disposed of in a secure manner and provides the following definition of secure disposal:

- Undertake and ensure the secure destruction of personal health information in the Recipient's custody or control within 30 days after the first of the following to occur:
  - The termination of this Agreement for any reason
  - The provision of a written request by BORN to the Recipient to undertake the secure destruction of the personal health information
  - The date expressly specified for secure destruction of the personal health information by BORN in the Research Agreement.
- When performing the secure destruction of personal health information, the Recipient will employ the methods prescribed in the Secure Destruction Information Package attached in Schedule D - Certificate of Destruction. Schedule D includes specific instructions and technical guidelines for the destruction of the personal health records subject to the research agreement where the methods of destruction are consistent with:
  - The *Personal Health Information Protection Act*, 2004 and its regulation
  - Orders issued by the Information and Privacy Commissioner of Ontario including Order HO-001 and Order HO-006
  - Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario including Fact Sheet 10).

  In addition, as set out in the research agreement, researchers are obligated to complete and return to the BORN Privacy Officer the Schedule D Certificate of Destruction which indicates that the personal health information was destroyed in the normal course of business pursuant to the organizational retention schedule and destruction policies and procedures. The certificate of destruction also includes the names of the individuals who were responsible for the destruction of the personal health information.

Notification
Section 7 of the BORN Template Research Agreement includes provisions for breaches. This section states that the researcher must provide BORN's Privacy Officer with written notice immediately after the researcher becomes aware of any security or privacy incident under Section 44(6) of PHIPA, or any likely breach of a term or condition of research agreement which includes all appendices to the Agreement, any breach or any likely breach of the researcher's duties under PHIPA. Further the agreement states that the researcher shall take steps that are reasonable in the circumstance to

contain, mitigate and remedy any security or privacy Incident or breach as the case may be and obtain express written authorization from BORN before providing information to any party regarding the events subject to notification.

Consequences of Breach and Monitoring Compliance
As per the template, if the recipient becomes aware of a breach of the agreement, they shall notify the BORN Privacy Officer in writing, take steps that are reasonable in the circumstances to contain, mitigate and remedy a breach, and obtain written authorization from BORN before providing information to any party regarding the event subject to notification.

Where there is a data breach, the agreement stipulates that BORN may terminate the agreement via written notice of termination, provide the recipient with the opportunity to remediate the incident within 30 days, cease to provide data and the recipient must, upon termination, immediately destroy any BORN data in their possession.

At any time during the terms of this agreement, BORN may, in its sole discretion and upon notice of not less than seven days, conduct an audit to ensure the Recipient's compliance with any provision in the agreement. A copy of the audit report will be provided to the recipient as well as a copy of the remediation plan developed by BORN to address any deficiencies identified in the audit report.
Section 3 of the agreement states that the researcher, and individuals employed by the researcher, who have been clearly identified in the BORN Data Request Form and Research Plan, are subject to the terms of the entire agreement. In addition the agreement requires the researcher to ensure all persons who will have access to the data must sign the Confidentiality Agreement. A sample the confidentiality agreement is provided as a schedule to the agreement, or they must provide proof that an institutional-specific agreement with the same requirements has been completed prior to any person accessing the data.

1.15 Log of Research Agreements

BORN maintains a log of research agreements that contains the following information:

- Name of research study
- Principal researcher last name, first name
- Date of receipt of the written application
- Date of receipt of the written research plan
- Date of Research Ethics Board approving the research plan
- Date approval to disclose personal health information for research was granted
- Date research agreement executed
- Date personal health information was disclosed
- Nature of personal health information
- Retention period
- Securely disposed (date)
- Date certificate of destruction was received

1.16 Policy and Procedures for the Execution of Data Sharing Agreements

BORN has in place a policy to ensure that data sharing agreements are executed effectively.

The 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.

BORN's policy on execution of data sharing agreements identifies that data sharing agreements are managed and executed by the Privacy Officer or the Privacy Advisor, where the Privacy Officer or Privacy Advisor ensures:

- Disclosures are approved in accordance with the BORN privacy policy **P-12: Disclosure of Personal Health Information for Purposes Other Than Research**
- Collections are approved in accordance with BORN privacy policy **P-04: Collection of Personal Health Information and P-06: Statements of Purpose for Data Holdings Containing Personal Health Information**
- The agreement is executed with the other party
- The log of data sharing agreements is updated
- The System Administrator is informed in order for any necessary access to the BORN database, or the Scientific Manager is informed upon execution of the agreement in order for the data tracking log to be updated (for disclosure of personal health information).

The policy mandates that the Privacy Officer or Privacy Advisor is responsible for storing the data sharing agreement (hard copy) in a locked storage unit in an area with controlled access, as well as electronic copies of all agreements and the log of data sharing agreements on the BORN privacy drive.

The policy mandates compliance to this policy and procedure by all BORN agents and states that compliance will be audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **P-27: Privacy Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management**, which each outline consequences of breach.

1.17 Template Data Sharing Agreement

BORN's policy for the **Execution of Data Sharing Agreements** mandates use of the BORN Template Data Sharing Agreement, the contents of which include:

General Provisions
The data sharing agreement template includes a description of the status of the Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network (BORN) under PHIPA, as well as associated responsibilities arising from the Act. It also sets out the precise nature of the personal health information subject to the agreement, as well as a definition of personal health information in accordance with section 4 of PHIPA.

The agreement clearly recognized the person or organization collecting or disclosing personal health information pursuant to the agreement.

Purposes of Collection, Use and Disclosure

The BORN data sharing agreement identifies the purpose and use for which the personal health information is being collected. In identifying the approved use of the personal health information being collected, the BORN data sharing agreement template states that the personal health information collected pursuant to the agreement may be linked with the personal health information in the BORN system for the purposes of BORN as defined in the agreement, pursuant to the registry purpose of facilitating or improving the provision of health care to mothers, infants and children. The agreement also mandates that any data linkage is subject to the BORN **Policy and Procedures for the Linkage of Records of Personal Health Information**.

In identifying the approved use of personal health information being disclosed by BORN, the BORN data sharing agreement template states that the recipient will link the BORN personal health information to personal health information defined in the agreement only for the purposes identified in the agreement.

The BORN data sharing agreement template states that the personal health information disclosed or collected pursuant to the agreement is necessary for the purpose for which is disclosed/collected and other information, de-identified and/or aggregate information, will not serve the purpose. This same agreement clause states that no more personal health information is being collected/disclosed than is reasonably necessary to meet the purpose.

Section 6 of the BORN data sharing agreement template for *collection* of personal health information identifies the purposes for which personal health information collected pursuant to the agreement may be disclosed as well as conditions and restrictions of disclosure.

Section 6 of the BORN data sharing agreement template for disclosure of personal health information identifies limitations, conditions and restrictions on disclosure of personal health information subject to the agreement.

The BORN data sharing agreement template requires the collection, use and disclosure of personal health information subject to the agreement to comply with the provisions of the Act and its regulation, as well as the statutory authority for the collection, disclosure.

The BORN data sharing agreement template includes a provision to set out the specific statutory authority for each collection, use and disclosure contemplated in the agreement. For example, the Data Sharing Agreement used by BORN to collect personal health information from hospitals contains the following provision:
Section 13(5) of the regulation to the personal health information Act, 2004 permits BORN ONTARIO to disclose personal health information without the patient's consent to an entity prescribed under section 45 of the personal health information Protection Act.

Secure Transfer
The BORN data sharing agreement template states the following with respect to the secure transfer of records of personal health information:

> The Parties will mutually determine agree to the following method, medium, frequency and timetable to be used with respect to the provision of information under this Agreement:
> - <insert specifics here>
>
> Where the secure transfer complies with the BORN policy on Secure Transfer of Records of personal health information

Secure Retention
Section 7 of the BORN data sharing agreement template for collection identifies that BORN will retain the personal health information collected subject to the agreement in electronic format for as long as necessary for long-term analysis and that personal health information no longer required by BORN for the purpose of improving or facilitating the provision of health care will be securely destroyed.

Section 7 of the BORN data sharing agreement template for disclosure states the retention period (specific to each disclosure) at which point as per the agreement the personal health information is to be securely destroyed and recorded in a certificate of destruction that must be forwarded to BORN within seven days of destruction.

Section 4 of the BORN data sharing agreement template for collection states that BORN will retain personal health information in a secure manner and will protect it against any theft, loss and unauthorized use or disclosure, and unauthorized copying, modification or disposal and identifies steps in this regard. The agreement specifies that security of personal health information collected under the agreement will be consistent with the BORN **Policy and Procedures for Secure Retention of Records of Personal Health Information**.

Section 4 of the BORN data sharing agreement template for disclosure states that the recipient will take reasonable steps to protect personal health information by means of industry best practices, including encryption, audit trails, intrusion and alteration alert systems and that the recipient will make available information on specific security practices on request of BORN.

Secure Return or Disposal
With respect to the collection of personal health information, section 7 of the BORN data sharing agreement identifies that personal health information no longer required by BORN will be securely destroyed as set out in BORN **Policy and Procedures for the Secure Disposal of Records of Personal Health Information** and a certificate of destruction will be issued, where acceptable secure destruction methods are defined, the method chosen and used is specified, and the certificate is issued within seven days of the secure destruction.

With respect to the disclosure of personal health information, section 7 of the BORN data sharing agreement mandates the secure destruction of all personal information received from BORN and any copies at the end of the retention period. A certificate of destruction, contained in the agreement, must be returned to the BORN Privacy Officer setting out the records of personal health information, date, time, location and method of secure destruction employed, bearing the name and signature of the person who performed the secure destruction. This will be issued to BORN within seven days of the secure destruction.

When performing destruction, the recipient will employ the methods prescribed in the Secure Destruction Information Package that is Schedule D of the data sharing agreement. Schedule D includes specific instructions and technical guidelines for the destruction of the personal health records subject to the research agreement where the methods of destruction are consistent with:

- The *Personal Health Information Protection Act*, 2004 and its regulation
- Orders issued by the Information and Privacy Commissioner of Ontario including Order HO-001 and Order HO-006
- Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario including Fact Sheet 10).

Notification
The data sharing agreement templates for collection and disclosure of personal health information identify:

- Written notice be provided by/to the BORN privacy officer immediately upon becoming aware of any breach or suspected breach of the agreement or if the personal health information subject to the agreement is stolen, lost or accessed by unauthorized persons.
- All reasonable steps will be taken to contain a breach of the agreement and to contain the theft, loss, or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance
The consequences of breach of the data sharing agreement state that failure of either party to comply with the terms and conditions of the agreement is cause for termination of the agreement and where applicable, a complaint to the Information and Privacy Commissioner.

Audits to ensure compliance with the agreement may be conducted with at least seven days' notice and may include provision of agreements, inspection of premises or computer databases to confirm that security and privacy controls are in place.

With respect to the disclosure of personal health information, the data sharing agreement requires all persons who will have access to the personal health information or de-identified health information to sign the Confidentiality Agreement (schedule B of the agreement) or provide proof that an institutional-specific agreement with the same requirements has been completed prior to the any person accessing the data. The Confidentiality Agreement requires that all persons are aware of and agree to be compliant with the terms and conditions of the data sharing agreement.

With respect to the collection of personal health information, the data sharing agreement requires all persons who will have access to the data to sign confidentiality agreements. Section 5, *Use of Personal Health Information* in the BORN data sharing agreement, requires that personal health information subject to the agreement can be used only in accordance with the agreement.

1.18 Log of Data Sharing Agreements

BORN maintains a log of data sharing agreements that includes:

- The name of the person or agency from whom the personal health information was collected or to whom the personal health information was disclosed
- The date that the collection or disclosure of personal health information was approved
- The date that the data sharing agreement was executed
- The date the personal health information was collected or disclosed
- The nature of the personal health information subject to the data sharing agreement
- Retention period or expiry of agreement
- Date of secure disposal of PHI
- Date secure certificate of destruction was received or provided

1.19 Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information

BORN has developed and implemented a policy and procedure to ensure that BORN executes agreements with third-party service providers prior to permitting access to and use of personal health

information. The written agreement is BORN policy **P-20: Template Agreement for All Third Party Service Providers**.

Agreements are initiated and executed by the appropriate BORN Director and are prepared by the Privacy Officer or the Privacy Advisor. The BORN policy and procedure include step-by-step instructions from initiation through execution and logging of a third-party service provider agreement.

The BORN procedure states that BORN does not provide personal health information to a third party service provider if other information, namely de-identified and/or aggregate data, will serve the purpose and will not province more personal health information than is reasonably necessary to meet the purpose. This determination is made by the appropriate BORN Director and is documented and forwarded to the BORN Privacy Officer as part of the request to prepare a third-party service provider agreement.

With respect to the secure disposal of the records of personal health information, the agreement specifies retention dates which are flagged for follow-up to the Privacy Officer. If the Privacy Officer has not received a Certificate of Destruction from the third-party service provider within seven days of the date of termination of the agreement, the Privacy Officer may take all measures authorized by the agreement and may notify the Information and Privacy Commissioner that the third party is in breach and, where appropriate, lodge a complaint.

The policy requires sets out that the Privacy Officer is responsible for maintaining a log of all agreements executed with third-party service providers. The Privacy Officer is also responsible for securely retaining this log as per the Document Retention section of BORN policy **P-19: Executing Agreements with Third Party Service Providers in Respect of Personal Health Information**.

The policy mandates compliance to this policy and procedure by all BORN agents and states that compliance will be audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **P-27: Privacy Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management**, which each outline consequences of breach

1.20 Template Agreement for All Third Party Service Providers

As per BORN policy **P-19: Executing Agreements with Third Party Service Providers in Respect of Personal Health Information**, third-party service providers that will be permitted to access and use personal health information must enter into a written agreement. The contents of this agreement are discussed in this section.

General Provisions
The BORN third-party service provider agreement clearly states BORN's status under the Act as a prescribed registry as well as the associated responsibilities arising from this status. It also states that the third-party service provider is an agent of BORN in relation to the use and disclosure of personal health information related to BORN.

Where the third-party service provider is an Electronic Service Provider under the Act, BORN is authorized to disclose personal health information to the third-party service provider as an electronic service provider as described in subsection 10(4) of the *Personal Health Information Protection Act*. As such the third-party service provider acknowledges that it is not an agent of BORN and will adhere to the requirement prescribed in Section 6 of Ontario Regulation 329/04-General (Regulation), enacted under the Act.

Where the third-party service provider is an agent of BORN, the agency relationship requires the third-party service provider to comply with the provisions of the Act and its regulation and with BORN privacy policies and procedures in all its dealings with personal health information and BORN data in general.

The agreement provides a definition of personal health information consistent with the Act and its regulation, and each agreement refers to "Schedule B, List of Data Elements" which specifies the nature of the personal health information pursuant to the agreement.

The agreement sets out that the third-party service provider agrees that their services will be performed in a professional manner by agents who are properly trained and will be in accordance with industry standards and practices.

Obligations with Respect to Access and Use and Disclose
The agreement sets out that

- The third-party service provider agrees to use (and/or disclose, where applicable) the personal health information provided through this Agreement only for the purpose of performing the services described in the agreement, and
- The Contractor agrees that this agency relationship requires the Contractor to comply with the provisions of the Act and its regulation and with BORN privacy policies and procedures in all its dealings with personal health information and BORN data in general.

Under section 3.2 of the agreement, entitled “Where Contractor is an Electronic Service Provider”, the Contractor agrees not to use personal health information except as necessary in the course of providing services pursuant to the Agreement and not to disclose personal health information to which it has access in the course of providing services, except as required by law.

The Contractor agrees to only use (and/or disclose) personal health information for these purposes if other information such as de-identified or aggregate information will not suffice, and in all cases, the Contractor must use (and/or disclose where applicable) only the least amount of personal health information that will suffice. Any other use or disclosure of personal health information is strictly prohibited unless required by law.

Secure Transfer
The agreement details the protections required by the third-party service provider with respect to the secure transfer of records of personal health information. The 'Transfer of Data section requires customization each time the agreement is used and mandates that the secure protections be included in the agreement and that the contractor agrees to provide documentation to BORN setting out the date, time and mode of transfer of records of personal health information and confirming receipt of the records. The contractor agrees to maintain a detailed inventory of the records of personal health information transferred. The agreement states that the method of transfer is compliant with the BORN policy on secure transfer of records of personal health information.

Secure Retention
As per the BORN agreement

- The Contractor agrees to maintain a detailed inventory of the records of personal health information being retained on behalf of BORN and must implement a method to track the records being retained.
- The Contractor agrees to retain records of personal health information in a secure manner that includes encryption, audit trails, intrusion and alteration alert systems and that is consistent with the BORN policy on secure retention (**Policy S-05: Secure Retention of Records of Personal Health Information**).
- The Contractor agrees to take steps that are reasonable in the circumstances to ensure that the personal health information accessed and used in the course of providing services pursuant to the agreement is protected against theft, loss, and unauthorized use or disclosure, and to ensure that the records of personal health information subject to the Agreement are protected against unauthorized copying, modification, or disposal.
- The Contractor agrees to:
    - Implement password protections, encryption, role-based access, and audit systems for records of personal health information retained in electronic media
    - Securely lock paper records in locked cabinets in locked premises

Secure Return or Disposal Following Termination of the Agreement
The BORN **template agreement for third-party service providers** requires records of personal health information be disposed of in a secure manner at the end of the retention period or on Termination of the Agreement. BORN does not require the return of records of personal health information.

A certificate of destruction setting out the date, time, location and method of secure destruction employed records of personal health information securely destroyed, and bearing the name and signature of the person who performed the secure destruction will be issued to the BORN Privacy Officer within 7 days of the destruction. Secure destruction means that the records are destroyed in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstance.

The agreements states that that Contractor agrees to:

- Securely dispose of records of personal health information within 30 days of termination of the Agreement
- Securely destroy records of personal health information on electronic storage media by disintegration, incineration, pulverization or melting
- Securely destroy paper records of personal health information using a crosscutting shredding method and incineration to eliminate the possibility of reconstructing the documents
- Any other conditions pursuant to the destruction, as applicable

Implementation of Safeguards
In the BORN template agreement for third party service providers, the Contractor agrees to:

- Take steps that are reasonable in the circumstances to ensure that the personal health information accessed and used in the course of providing services pursuant to the Agreement is protected against theft, loss, and unauthorized use or disclosure, and to ensure that the records of personal health information subject to the Agreement are protected against unauthorized copying, modification, or disposal

- Implement password protections, encryption, role-based access, and audit systems for records of personal health information retained in electronic media
- Securely lock paper records in locked cabinets in locked premises

Training of Agents of the Third Party Service Provider
As per the BORN agreement, the Contractor agrees to train its agents on the importance of protecting the privacy and security of the records of personal health information and the consequences of a breach of privacy or security. Under the agreement section 3.1, the Contractor agrees to require its agents to sign the Confidentiality Agreement in Schedule II (of the BORN template agreement) before giving agents access to the records of personal health information. The confidentiality agreement stipulates:

- I am aware of and agree to comply with the terms and conditions of this Agreement.

Subcontracting of the Services
The template agreement requires that the Contractor acknowledges and agrees to provide BORN with 7 days advance notice of its intention to subcontract services and to enter into a written agreement with the subcontractor that includes the obligations set out in this Agreement and to provide a copy of that written agreement with the subcontractor to the BORN Privacy Officer within 7 days of the execution of the document.

Notification
The BORN template agreement includes the provision that the Contractor agrees to provide written notice to the BORN Privacy Officer, at the first reasonable opportunity, upon becoming aware of any breach or suspected breach of this agreement or if the personal health information has been accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. The Contractor agrees to advise BORN of the reasonable steps taken in the circumstances to contain the breach and to contain the theft, loss or access by authorized persons to correct any such default and to prevent recurrence.

Consequences of Breach and Monitoring Compliance
As per the agreement template, compliance with terms of this Agreement will be monitored by the Privacy Officer of BORN. The Contractor agrees that BORN representatives will be permitted to carry out on-site visits and such other inspections or investigations on reasonable notice during normal working hours or at mutually agreed times to ensure compliance with the conditions of this Agreement. Such measures may include, but are not limited to, provision of agreements and inspection of premises or computer databases to confirm that security and confidentiality controls that are set out in this Agreement are in effect. The agreement contains the following provision:
Failure to comply with the terms or conditions of this Agreement is cause for Termination of this Agreement.

1.21 Log of Agreements with Third Privacy Service Providers

BORN maintains a log of third-party service provider agreements which includes:

- Name of the third party service provider
- Nature of the services provided
- Date agreement executed
- Date that personal health information or access to records provided
- Nature of the personal health information
- Date of termination of agreement

- Date Certificate of Destruction received or Date access to PHI terminated

1.22 Policy and Procedures for the Linkage of Records of Personal Health Information

BORN has in place a policy for the appropriate linkage of records of personal health information. This policy sets out that BORN permits linkage of personal health information for the following purposes:

- 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 (pregnancy to birth to young childhood) to improve the quality and efficiency of care for mothers, infants and children. For example, linking health outcome information to interventions allows for the analysis of the quality of the care being provided
- 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.

The BORN policy states that BORN permits the following types of record linkages:

- Linkage of records of personal health information solely in the custody of BORN for the exclusive purposes of BORN
- Linkage of 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
- Linkage of records of personal health information solely in the custody of BORN for the purposes of disclosure to another person or organization
- Linkage of 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 that other person or organization

Review and Approval Process and Conditions and Restrictions on Approval

As per the BORN policy, where the linked records of personal health information are disclosed by BORN to another person or organization:

- The disclosure is approved as per BORN policy **P-13: Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements** or **P-12: Disclosure of Personal Health Information for Purposes Other Than Research**, as applicable

Where the linked records of personal health information are used by BORN for research:

- The use is approved as per BORN policy **P-10: Use of Personal Health Information for Research**

Where the linkage of records of personal health information solely in the custody of BORN is exclusively for the purposes of BORN as a prescribed registry:

- The linked records of personal health information are de-identified and/or aggregated as per BORN policy **P-24: De-Identification and Aggregation**. Data are kept in identifiable, but secure, format to allow for ongoing linking as new data are entered into the system. To the extent possible, only de-identified and/or aggregate information will be used by Agents of BORN for project-specific analyses.

Process for the Linkage of Records of Personal Health Information
The policy states that a linking and matching algorithm has been developed to automate the process of linking information where sufficient information exists within the BORN Information System. The algorithm uses ten (10) and twelve (12) baby personal identifiers to determine if records should be linked automatically. Where a 'potential' link is found – likely a match but not sufficient information to be certain – human interaction is required to complete the work. A designated BORN Agent (linking and matching resource) has responsibility for managing the queue of potential linked records.

Retention
As per the policy, linked records of personal health information are retained in compliance with BORN policy **S-05: Secure Retention of Records of Personal Health Information** until they are de-identified and/or aggregated as per BORN policy **P-24: De-Identification and Aggregation**.

Secure Disposal
As per the policy, records of personal health information linked by BORN are securely disposed of in compliance with BORN policy **S-08: Secure Disposal of Records of Personal Health Information**.

Compliance, Audit and Enforcement
The policy mandates compliance to this policy and procedure by all BORN agents and states that compliance will be audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **P-27: Privacy Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management**, which each outline consequences of breach

Tracking Approved Linkages of Records of Personal Health Information
The Manager of Health Informatics maintains the **Log of Approved Linkages of Records of Personal Health Information**.

1.23 Log of Approved Linkages of Records of Personal Health Information

The BORN log of approved linkages of records of personal health information includes the following:

- Name of organization
- Individual last name
- Individual first name
- Date linkage approved
- Nature of personal health information
- Fields used for linking of personal health information

1.24 Policy and Procedures with Respect to De-Identification and Aggregation

BORN has in place a policy to ensure appropriate implementation of data de-identification and aggregation practices. The policy states that BORN prohibits the use or disclosure of personal health information if other information, namely de-identified and/or aggregate information, will serve the identified purpose.

The policy sets out that where information is aggregated, but includes information about individuals in groups of five (5) or less, the information will not be released. This restriction is contained in all Research Agreements and data sharing agreements.
The BORN policy provides the following definition of de-identified information and aggregate information:

- **De-identified information** refers to records that have had enough personal information removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information alone can be used to identify an individual.
- **Aggregate information** refers to summed and/or categorized data that is analyzed and placed in a format that precludes further analysis (e.g. tables or graphs) to prevent the chance of revealing an individual's identity. Individual records cannot be reconstructed.

The policy further states that identifying information refers to information that identifies an individual or that it is reasonably foreseeable in the circumstances could be used either alone or with other information to identify an individual.

As stated in the policy, BORN uses the Privacy Analytics Re-Identification Risk Assessment and De-identification Tool (PARAT) for all uses and disclosures of de-identified/aggregate data. De-identification occurs in consultation with the CHEO Electronic Health Information Laboratory. The BORN Scientific Manager or designate forwards a request to a BORN data analyst to assess the level of re-identification risk of a particular data set using the empirical analysis Privacy Analytics Re-Identification Risk Assessment and De-identification Tool (PARAT) for all uses and disclosures of de-identified/aggregate data. A pre-determined low level of risk (0.1) is considered an acceptable level of risk. PARAT uses several de-identification techniques including suppression (removing high risk records) and generalization (reducing the resolution of a given field.) PARAT will automatically de-identify the data to reduce the re-identification risk to an acceptable level.

In addition, de-identified and/or aggregate data including information of cell-sizes of five (5) or less is reviewed by the Scientific Manager or designate prior to every use or disclosure in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized to identify an individual.

The policy states that BORN agents are prohibited from using de-identified and/or aggregate information, alone or in combination with other information, to identify an individual. This requirement is contained in all research agreements and data sharing agreements.

As per the policy, where de-identified information or aggregate information is disclosed outside of BORN, the disclosure is made only under one of the following policies which contain provisions prohibiting recipients from using the de-identified information or aggregate information either alone or with other information to identify an individual:

- BORN policy **P-12: Disclosure of Personal Health Information for Purposes Other Than Research**
- BORN policy **P-13: Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements**

The policy mandates compliance to this policy and procedure by all BORN agents and states that compliance will be audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **P-27: Privacy Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management**, which each outline consequences of breach.

1.25 Privacy Impact Assessment Policy and Procedures

BORN has in place effective policies to assess the impact of new or modified activities that involve the collection, use or disclosure of personal health information. It sets out that BORN undertakes privacy impact assessments:

- On existing programs, processes and systems when there are significant changes relating to the collection, access, use or disclosure of personal health information
- In the design of new programs, processes and systems involving personal health information
- On any other programs, processes and systems with privacy implications, as recommended by the Privacy Officer

The policy states that privacy impact assessments are not required where existing programs, processes and systems are changed or new programs, processes, and systems are implemented, if no personal information or personal health information is involved.

As per the policy, the following occurs:
The BORN Director is required to provide the Privacy Officer with a written description of proposed new programs and/or changes to existing information systems, technologies or programs involving personal health information at the design stage and the Privacy Officer evaluates the need for a privacy impact assessment. In respect of new programs or changes to existing information systems, technologies or programs involving personal health information, the Privacy Officer conducts a privacy impact assessment at the design stage to ensure that privacy protections can be designed into the new system. Following this:

- For new programs: the Privacy Officer ensures that a second privacy impact assessment is undertaken once the program is implemented to ensure that all recommendations have been fully implemented
- For changes to existing information systems, technologies or programs, the Privacy Officer reviews the systems, technologies or programs on completion of implementation of changes to ensure that all recommendations contained in the privacy impact assessment have been implemented and will make a note of this in the BORN Log of Privacy Impact Assessments Initiated/Completed

The Privacy Officer, in conjunction with the Manager of Health Informatics, develops a timetable for the conduct of privacy impact assessments related to existing holdings to ensure privacy impact assessments are reviewed and refreshed on an on-going basis, and are repeated every three years at a minimum.

The Privacy Officer defines the scope and requirements and then works with the Manager of Health Informatics in all aspects of completing the privacy impact assessment. Where outsourced, the Privacy

Officer completes the request for proposals, executes the contract, monitors the process and receives the completed report and recommendations.

The contents of the privacy impact assessment, as per the policy, include:

- Data holding, information system, technology or program at issue
- Nature and type of personal health information collected, used or disclosed or that is proposed to be collected, used or disclosed
- Sources of the personal health information
- Purposes for which the personal health information is collected, used or disclosed or is proposed to be collected, used or disclosed
- Reason that the personal health information is required for the purposes identified
- The flows of the personal health information
- Statutory authority for each collection, use and disclosure of personal health information identified
- Limitations imposed on the collection, use and disclosure of the personal health information;
- Whether or not the personal health information is or will be linked to other information
- Retention period for the records of personal health information
- Secure manner in which the records of personal health information are or will be retained, transferred and disposed of
- Functionality for logging access, use, modification and disclosure of the personal health information and the functionality for auditing logs for unauthorized use or disclosure
- Risks to the privacy of individuals whose personal health information is or will be part of the data holding, information system, technology or program and an assessment of the risks
- Recommendations to address and eliminate or reduce the privacy risks identified
- Administrative, technical and physical safeguards implemented or proposed to be implemented to protect the personal health information

The Privacy Officer, working with the Manager of Health Informatics, develops and implements a process for addressing the recommendations arising from the privacy impact assessment, including:

- Assigning responsibilities to BORN Agent(s)
- Setting timelines
- Monitoring timelines
- Monitoring implementation of recommendations

As per the policy, where a privacy impact assessment is required, the Privacy Officer defines the scope and requirements of the privacy impact assessment based on the Privacy Impact Assessment Guidelines for the *Ontario Personal Health Information Protection Act, 2004* published by the Information and Privacy Commissioner of Ontario.

The Privacy Officer develops and maintains the **Log of Privacy Impact Assessments Initiated/Completed** and the **Log of Privacy Impact Assessments Not Undertaken**.

The policy mandates compliance to this policy and procedure by all BORN agents and states that compliance will be audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **P-27: Privacy Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management**, which each outline consequences of breach

1.26 Log of Privacy Impact Assessments

BORN has a log of privacy impact assessments that have been completed and privacy impact assessments that have been undertaken but not yet completed that includes:

- Data Holding/Information System/Technology/Program of Personal Health Information
- Date, PIA completed or expected to be completed
- Agent(s) responsible
- PIA recommendations
- Agent responsible for addressing each recommendation
- Date recommendations to be implemented
- Manner in which each recommendation was or is to be addressed
- Date recommendations implemented

BORN has a log of privacy impact assessments not undertaken that describes:

- Data Holding/Information System/Technology/Program of Personal Health Information
- Reason the PIA not undertaken
- Agent responsible for decision
- Date PIA expected to be completed
- Agent responsible for completing or ensuring completion

1.27 Policy and Procedures in Respect of Privacy Audits

BORN has in place a privacy audit policy to ensure that privacy audits are regularly conducted, and appropriately manages findings and recommendations resulting from these audits. As per the policy, 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
- On external parties to assess compliance with Research, Data Sharing and Third-party agreements
- Assess compliance of agents permitted to access and use personal health information as per BORN policy **P-08: Limiting Agent Access to and Use of Personal Health Information**

As per the BORN policy, the Privacy Officer is responsible for developing and implementing an annual plan and schedule for the audit of privacy policies and procedures and agent compliance. The Privacy Officer develops the annual privacy auditing plan which includes:

- Specific Area(s) to be audited
- Purposes of the privacy audits
- Frequency of the audits
- Timeframes for the privacy audits
- Nature and scope of the privacy audits (e.g. document reviews, interviews, group discussions, questionnaires, file reviews, site visits, inspections)
- Agent(s) responsible for conducting the privacy audits

- Framework for the review, including questions or areas of concern

The Privacy Officer schedules the audit and provides notification to agents and/or third parties as applicable. The notification includes:

- Statement that BORN is undertaking an audit
- Purpose of the audit
- Scope of the audit (site visit, inspection, interview, document review)
- List of documentation required for review, if applicable
- Date and time that BORN Privacy Officer will be contacting the Agent/third party

The Privacy Officer documents the results of the site visits, inspections, interviews, and document reviews, and based on these findings prepares a report which includes background, findings, recommendations and action plans in an annual privacy audit report that is provided to the Director, Privacy and Security Review Committee and the Leadership Team within a month of the report being completed.

The Privacy Officer further:

- Implements the action plan(s) from the audit report, assigning responsibilities and establishing timelines
- Monitors implementation, and
- Provides quarterly status updates to the Director, the Privacy and Security Review Committee, and the Leadership Team in the quarterly report and annual report on privacy that includes:
    - Results of each privacy audit
    - Recommendations of each privacy audit
    - Status of implementation of the recommendations of each privacy audit

The Privacy Officer maintains the BORN Log of Privacy Audits and also enters the recommendations of each privacy audit into the BORN Consolidated Log of Recommendations.

The Privacy Officer is responsible for maintaining and securely retaining:

- Annual audit plan
- All audit reports and action plans and related materials
- All quarterly status updates (in the quarterly report on privacy)
- Log of Privacy Audits

Agents responsible for conducting privacy audits are required to notify the Privacy Officer, at the first reasonable opportunity, of a privacy breach or suspected privacy breach as per BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and Manager of Health Informatics of security breach or suspected security breach as per BORN policy **S-17: Security Breach Management**.

1.28 Log of Privacy Audits

BORN maintains a log of privacy audits that includes:

- Nature and type of privacy audit
- Expected/actual date completed
- Agent(s) responsible for completing
- Findings and recommendations
- Agent(s) responsible for addressing each recommendation

- Date recommendation to be addressed
- Manner recommendation to be addressed
- Date recommendation addressed

1.29 Policy and Procedures for Privacy Breach Management

BORN has in place a policy and procedures for privacy breach management to address the identification, reporting, containment, notification, investigation and remediation of privacy breaches.
The policy contains a definition of a privacy breach as follows:

- The collection, use and disclosure of personal health information that is not in compliance with the Act, 2004 and its regulation
- A contravention of BORN privacy policies, procedures or protocols
- A contravention of a BORN Confidentiality Agreement or the terms and conditions in data sharing agreements, Research Agreements, and Agreements with Third Party Service Providers retained by BORN
- Circumstances where personal health information is stolen, lost or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification or disposal

The policy states that agents must notify the Privacy Officer as soon as reasonably possible of a breach or suspected breach and the contact information for the privacy officer is indicated in the policy.
As per the policy, the breach notification may be made verbally to the Privacy Officer and must include:

- Type of suspected breach
- Location of suspected breach
- Any actions taken by the reporting Agent to contain the breach

An agent who discovers a breach or suspected breach is required to initiate the process of containment.

The verbal notification must be followed up as soon as possible by completion of a Breach Reporting Form to be forwarded by the agent to the Privacy Officer. The completed Breach Reporting Form includes:

- Name and position of the individual who discovered the incident
- Date and time of discovery of the incident
- Estimated time and date the breach occurred, if known
- Type of breach (loss, theft, inadvertent disclosure)
- Cause of breach, if known
- Description of information involved in the breach
- Actions taken by Agent reporting the breach to contain the breach
- Any other individuals or organizations involved in the breach

The policy states that the Privacy Officer confirms the breach and determines what (if any) personal health information has been stolen, lost or accessed, used, disclosed, copied, modified or disposed of in an unauthorized manner.

Further notification including senior management is defines in the policy as follows:

The Privacy Officer notifies the Director immediately by e-mail indicating that:

- A privacy breach has occurred and whether it is internal or external

- A brief description of the nature and extent of the breach, including what information has been breached
- Actions taken by the Agent reporting the breach and by the Privacy Officer to contain the breach
- Whether hard copies of the information have been successfully retrieved or the breached information has been destroyed
- The police have been notified and why, if applicable.

As soon as reasonably possible, the BORN Director forwards the Privacy Officer's notification and a description of any further efforts at containment to the Leadership Team.

Within 24 hours of a privacy breach, the Privacy Officer completes a CHEO Incident Report using the AEMS System as per CHEO Incident Reporting Policy No. 008. 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.

If the Privacy Officer determines that the breach involves theft or impacts personal safety, the Privacy Officer:

- Alerts the Director of BORN and the CEO of CHEO and informs them that the police will be notified
- Notifies the police

The Privacy Officer, together with the appropriate Agent(s), works immediately to further contain the breach. The Privacy Officer:

- Determines whether the breach or potential breach would allow unauthorized access to any other data and takes whatever action is required to ensure that no further breaches can occur through the same means (e.g. change password, shut down the system) and that the breach is contained
- Determines what (if any) personal health information has been stolen, lost or accessed, used, disclosed, copied, modified or disposed of in an unauthorized manner
- Securely retrieves hard copies of any personal health information that has been disclosed or ensures as much as possible of the breached information has been disposed of in a secure manner
- Where the breached information has been securely destroyed by the organization to which the information was disclosed, the Privacy Officer obtains written confirmation related to the date, time and method of secure disposal and records this confirmation in the Log of Privacy Breaches
- Ensures no copies of the personal health information have been made or retained by the individual who was not authorized to retrieve or receive the information

The BORN Director, along with the Privacy Officer, reviews the containment measures implemented to determine that the privacy breach has been effectively contained. Where further measures are required, the BORN Director works with the Privacy Officer to ensure secure containment.

The Privacy Officer enters the information into the BORN Log of Privacy Breaches.

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 organization, the Privacy Officer sends written notification to the heath information custodians or organization who provided the information at the first reasonable opportunity in order that they may

notify individuals whose privacy was breached as per section 12(2) of the *Personal Health Information Protection Act, 2004*. As a prescribed registry, BORN does not directly notify individuals whose information has been breached.

This notification from BORN to the health information custodian includes:

- Date of the privacy breach
- A general description of the extent of the breach
- Nature of the personal health information that was the subject of the privacy breach
- Date that the privacy breach was contained and the nature of the containment measures
- Steps that have been taken to reduce the possibility of future breaches
- Steps the individual can take to further mitigate the risk of harm (where applicable)
- Notice that the Information and Privacy Commissioner has been contacted
- Name and phone number of contact person within BORN who can answer questions
- That individuals have a right to complain to the Information and Privacy Commissioner and the contact information for the Commissioner.

The policy sets out that after consultation with the BORN Director, the Privacy Officer may send a written notification to the Ministry of Health and Long-Term Care setting out:

- Date of the privacy breach
- A general description of the extent of the breach
- Nature of the personal health information that was the subject of the privacy breach
- Date that the privacy breach was contained and the nature of the containment measures
- Steps that have been taken to reduce the possibility of future breaches
- Steps the individual can take to further mitigate the risk of harm (where applicable)
- Notice that the Information and Privacy Commissioner has been contacted
- Name and phone number of BORN Privacy Officer

The Privacy Officer together with the appropriate BORN agents initiates a comprehensive investigation, including interviews, document reviews, site visits and inspections. The review will determine:

- Organizations involved in the breach
- Cause of the breach
- Data elements involved
- Number of individuals affected by the breach
- Identification of the individuals affected by the breach
- Any harm that may result from the breach, including:
    - Security risk
    - Identity theft or fraud
    - Hurt, humiliation, damage to reputation
    - Actions required to prevent future breaches

The Privacy Officer completes the comprehensive investigation within four weeks from the time the breach was reported and prepares a comprehensive report for the Director, including:

- Date of the privacy breach
- Date that the privacy breach was identified or suspected
- Nature of the breach, that is, whether it was determined to be a privacy breach and whether it was internal or external
- Nature of the personal health information that was the subject matter of the privacy breach

- Facts or events relevant to the breach
- Date that the privacy breach was contained and the nature of the containment measures
- Date that the health information custodian or other organization that disclosed the personal health information to BORN was notified
- Date that the investigation of the privacy breach was completed
- Agent(s) responsible for conducting the investigation
- Recommendations for corrective measures arising from the investigation
- Agent(s) assigned to address each recommendation; the date each recommendation is expected to be addressed

The BORN Director reviews the report and forwards it to the Privacy and Security Review Committee for approval to proceed with implementation of the recommendation.

The policy identifies the Privacy Officer as the agent responsible for maintaining a log of privacy breaches and for tracking that recommendations arising from the investigation are addressed within the identified timelines.

The policy clearly sets out that the privacy officer is responsible for the secure retention of:

- All correspondence related to the privacy breach
- Investigative notes and final report on the breach
- The Log of Privacy Breaches

The policy mandates compliance to this policy and procedure by all BORN agents and states that compliance will be audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **P-27: Privacy Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management**, which each outline consequences of breach

1.30 Log of Privacy Breaches

The BORN Privacy Officer maintains a log of privacy breaches that includes:

- Date of privacy breach
- Date privacy breach was identified or suspected
- Internal/external
- Nature of the personal health information involved
- Nature and extent of privacy breach
- Date privacy breach contained
- Nature of containment measures
- Date personal health information custodian notified
- Date investigation completed
- Agents conducting investigation
- Recommendations Arising from Investigation
- Agent responsible for addressing each recommendation
- Date each recommendation will be/was addressed
- Manner in which each recommendation will be/was addressed

1.31 Policy and Procedures for Privacy Complaints

BORN has developed and implemented a policy to effectively manage all privacy complaints including:

- Complaints related to the privacy policies and procedures implemented by BORN
- Complaints related to the compliance of BORN to the Act and its regulation

The policy and procedure identifies that individuals may obtain further information about BORN policies and procedures or direct complaints and concerns to the Privacy Officer by calling, e-mailing or writing, and full contact details are supplied in support of this. The procedure further states that individuals may make a complaint regarding compliance to the Act and its regulation to the Information and Privacy Commissioner of Ontario and provides the mailing address and contact information to this end.

The procedure establishes the process to be followed in receiving complaints (in written format or by phone) including entering complaints in the log of privacy complaints and privacy inquiries, sending a follow-up letter to the complainant, and, where quick resolution is not achieved, completion of a complaint form by the complainant. For all complaints received, the Privacy Officer is responsible for assessing the complaint and determining whether the complaint relates to a privacy breach and should be addressed as per the BORN policy on privacy breach management. ***Error! Reference source not found.***

The Privacy Officer is responsible for determining, within seven days, whether the complaint should be investigated according to criteria defined in the procedure. The complaint is documented, as is the determination of whether or not an investigation is needed, and the reason(s) for this decision.

Where the privacy complaint will not be investigated, the policy and procedures set out that the Privacy Officer sends a letter to the complainant within 14 days of receipt of the complaint form. The letter includes:

- Acknowledges receipt of the privacy complaint
- Provides a response of the privacy complaint
- Advises that an investigation will not be undertaken
- Advises that the complainant may make a complaint to the Information and Privacy Commissioner if there are reasonable grounds to believe that BORN has contravened or is about to contravene the Act or its regulation, and providing contact information for the Information and Privacy Commissioner

Where the privacy complaint results in an investigation, the policy and procedures sets out that the Privacy Officer sends a letter to the complainant within 14 days of receipt of the complaint form. The letter includes:

- Acknowledges receipt of the privacy complaint
- Advises that an investigation will be undertaken
- Provides an explanation of the BORN privacy complaint procedure
- Indicates that if additional information if required, the complainant will be contacted
- Sets out the timeframe for completion of the investigation
- Sets out the nature of the documentation that will be provided upon completion of the investigation

The BORN Privacy Officer is responsible for conducting privacy complaint investigation as per the procedure, which also sets out that the Privacy Officer seeks to substantiate the facts surrounding the

complaint by undertaking reviews of relevant documents, conducting interviews with the complainant, BORN agents and third parties, health information custodians, and researchers, as appropriate, and carrying out site visits and inspections, as appropriate.

The investigation and documentation of the findings are completed by the Privacy Officer within 30 days of receipt of the complaint form. The report is forwarded to the BORN Director, who in turn forwards it to the Leadership Team. The documentation includes:

- Findings from the investigation
- Where BORN agents, third parties and/or researchers have deviated from BORN policies and procedures and/or have been non-compliant with the Act and its regulation
- Any related considerations
- Recommendations to address the concern identified in the complaint and timelines
- A draft response to the complainant

The Leadership Team approves the recommendations in the report and the Privacy Officer is responsible for implementing these recommendations, including assigning Agent(s) to recommendations, establishing timelines and monitoring and tracking implementation and ensuring timelines are met.

The Privacy Officer provides a written status report to the BORN Director, Communications Lead, Leadership Team and BORN staff upon completion of the implementation of the recommendations.

The Privacy Officer includes a description of the complaints received and actions taken by BORN in the quarterly reports to the Privacy and Security Review Committee and the Leadership Team and the Annual Report on Privacy and Security.

Within 45 days of receiving the complaint form, the Privacy Officer notifies the complainant in writing of the nature of the findings of the investigation, any measures that have been/will be taken in response to the privacy complaint, the complainant's right to make a complaint to the Information and Privacy Commissioner of Ontario, and contact information for the Information and Privacy Commissioner.

The procedure mandates that the Privacy Officer is responsible for the secure retention of:

- The log of privacy complaints, including those for which an investigation was not undertaken.
- Comprehensive files for each privacy complaint including all correspondence (both external and internal), complaint form and any notes made by the Privacy Officer

The policy mandates compliance to this policy and procedure by all BORN agents and states that compliance will be audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **P-27: Privacy Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management**, which each outline consequences of breach

1.32 Log of Privacy Complaints

The BORN Privacy Officer maintains a log of privacy complaints and inquiries that includes:

- Date of complaint or enquiry and nature of the privacy complaint

- Will Complaint be Investigated? Y/N
- Date Determination Made
- Date Complainant was advised Complaint would NOT be investigated and response provided
- Date Complainant was advised Complaint would be investigated
- Agents Responsible for Conducting the Investigation
- Date the investigation commenced
- Date the investigation completed
- Recommendations Arising from Investigation
- Agents Responsible for Addressing each Recommendation
- Date each recommendation is expected to be addressed
- Date each recommendation was addressed
- Manner each recommendation was addressed
- Date Complainant was Advised of Findings and Measures Taken

1.33 Policy and Procedures for Privacy Inquiries

BORN has developed and implemented a policy and procedures to ensure that privacy inquiries are effectively managed. The policy includes a definition of privacy inquiries as follows:

- Inquiries relating to the privacy policies and procedures implemented by BORN
- Inquiries relating to compliance of BORN with the *Personal Health Information Protection Act, 2004* and its regulation

The policy and procedures identify that individuals may direct privacy-related inquiries and may obtain information about BORN privacy policies and procedures by calling, e-mailing or writing to the Privacy Officer, and full contact details are supplied in support of this.

The BORN policy and procedures for privacy inquiries sets out that the BORN Privacy Officer receives and reviews all inquiries, records all inquiries in the log of privacy complaints and privacy inquiries, including the date and nature of the inquiry, date the inquiry was responded to by the Privacy Officer, any further queries resulting from the initial inquiry and the date the inquiry was completed. A copy of this log is forwarded by the Privacy Officer to the BORN Director and the Privacy and Security Review Committee as necessary, and at a minimum, quarterly.

With respect to the review of an inquiry, the policy sets out that:
The Privacy Officer receives and reviews all inquiries to determine if the inquiry:

- Relates to a privacy breach and should be addressed as per **Error! Reference source not found.**
- Relates to a privacy complaint and should be addressed as per **Error! Reference source not found.**

Responses to all inquiries are provided in writing either by e-mail or by mail, as requested by the individual or organization making the inquiry.

The policy mandates compliance to this policy and procedure by all BORN agents and states that compliance will be audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **P-27: Privacy Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** and to notify the

Privacy Officer and the Manager of Health Informatics of a security breach or suspected breach as per BORN policy **S-17: Security Breach Management**, which each outline consequences of breach

BORN Compliance to IPC Manual Part 2 – Security Documentation

2.1 Information Security Policy

BORN has developed an information security policy to ensure that a security framework is in place to protect the personal health information it receives. As per the policy, BORN securely maintains the personal health information in its custody and protects the information against theft, loss and unauthorized use or disclosure, and unauthorized copying, modification and disposal.

BORN undertakes threat and risk assessments to cover security assets, personal health information and project specific threats and risks. The methodology for these assessments is included in the BORN policy **S-15: Security Audits** which sets out the following:

- Threat and risk assessments are a mandatory element of BORN security audits and defined as:
    - Comprehensive and organization-wide including all information security assets, including personal health information, as well as appropriate project specific threat and risk assessments to identify both internal and external risks; may be performed by a third party.
- Each security audit, including a threat and risk assessment, is recorded in a written report that contains:
    - Audit as identified in the annual plan
    - Scope of the audit
    - Methodology employed
    - Findings/risk scores (where applicable, for prioritization of remedial action)
    - Recommendations

  This written report is the BORN methodology for identifying and assessing risks.
- Each recommendation resulting from a threat and risk assessment is recorded in the BORN Consolidated Log of Recommendations by the Privacy Officer, who also assigns and records the agent responsible for addressing the recommendation (remediation) and the timelines for completion. Completion dates are tracked by the Privacy Officer.

The information security policy indicates that:

- The Manager of Health Informatics has responsibility for the implementation of a comprehensive information security program that includes administrative, physical and technical safeguards consistent with industry standards.
- 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 as per BORN policies **S-15: Security Audits** and **O-04: Corporate Risk Management Framework**.

The BORN information security policy includes references to the following policies and procedures:

- A security governance framework as per BORN policy **O-01 and O-02: Privacy and Security Governance and Accountability Framework** and BORN policy **HR-01 and HR-03: Privacy and Security Training and Awareness**
- Policies and procedures for the ongoing review of the security policies, procedures and practices implemented as per BORN policy **S-02: Ongoing Review of Security Policies and Procedures**
- Policies and procedures for ensuring physical security of the premises as per BORN policy **S-03: Ensuring Physical Security of Personal Health Information**

- Policies and procedures for the secure retention, transfer and disposal of records of personal health information which address among other things remote access and data at rest, as per BORN policy **S-05: Secure Retention of Records of Personal Health Information**, BORN policy **S-06: Secure Retention of Records of Personal Health Information on Mobile Devices**, BORN policy **S-07: Secure Transfer of Records of Personal Health Information** and, BORN policy **S-08: Secure Disposal of Records of Personal Health Information**
- Policies and procedures to establish access control and authorization, including business requirements, user access management, user responsibilities, network access control, operating system access control and application and information access control as per BORN policy **S-09: Passwords,** BORN policy **S-14: Acceptable Use of Technology,** BORN policy **P-08: Agent Data Access,** BORN policy **S-03: Ensuring Physical Security of Personal Health Information,** BORN policy **HR-06: Template Confidentiality Agreement with Agents**
- Policies and procedures for information systems acquisition, development and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management as per the following BORN policies: **S-10: System Control and Audit Logs**, **P-19: Executing Agreements with Third Party Service Providers in Respect of Personal Health Information**, **S-05: Secure Retention of Records of Personal Health Information**, **S-15: Security Audits**, **S-11: Patch Management**, **S-12: Change Management** and **S-03: Ensuring Physical Security of Personal Health Information**
- Policies and procedures for monitoring as per BORN policy **S-10: System Control and Audit Logs** and BORN policy **S-15: Security Audits**
- Policies and procedures for network security management as per BORN policy **S-11: Patch Management** and BORN policy **S-12: Change Management**
- Policies and procedures related to the acceptable use of information technology as per BORN policy **S-14: Acceptable Use of Technology**
- Policies and procedures for back-up and recovery as per BORN policy **S-13: Back-up and Recovery of Records of Personal Health Information**
- Policies and procedures for information security breach management as per BORN policy **S-17: Security Breach Management**
- Policies and procedures to establish protection against malicious and mobile code as per BORN policy **S-15: Security Audits** and BORN policy **O-04: Corporate Risk Management Framework** and BORN policy **S-14: Acceptable Use of Technology**

The BORN Information Security Policy outlines technical safeguards that are implemented, which include:

- User system access protected by secure socket layer encryption
- Transmission of personal health information over authenticated, encrypted and secure connections
- Hardened servers
- Firewall (with demilitarized zone)
- Anti-virus, anti-spam and anti-spyware measures
- Penetration testing, vulnerability assessments and threat-risk assessments for internal and external systems when required
- Daily backup of necessary information
- Mandatory password-protected screen savers after a 15-minute timeout period on user devices and mandatory idle timeout on BORN portal pages

The Manager of Health Informatics implements a program for continuous assessment and verification of the effectiveness of the security program as per BORN policy **S-15: Security Audits** and BORN policy **O-04: Corporate Risk Management Framework**. The Manager of Health Informatics is supported by the Privacy Officer in both the implementation and review of the security program.

As per policy directions, BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and/or the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**. The policy also states that agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics in accordance with BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

2.2 Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices

BORN has developed and implemented a joint policy for the ongoing review of privacy and security policies and procedures to ensure appropriate review. Compliance to all requirements for the policy and procedures for ongoing review of security policies, as per the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities, is included in the BORN triennial review document **BORN IPC Part 1 – Privacy Policies 1 – 13 Compliance**.

2.3 Policy and Procedures for Ensuring Physical Security of Personal Health Information

BORN has in place a policy to ensure appropriate physical security in order to protect personal health information against theft, loss and unauthorized use, disclosure copying, modification or disposal.

The physical safeguards implemented by BORN to protect records of personal health information include locked doors, locked filing cabinets, alarms and controlled access to premises where BORN agents work and to secure locations within the premises where records of personal health information are retained.

BORN defines two types (levels) of access:

1. The BORN premises where BORN employees work
    - A secure research building located on the premises of the Ottawa Hospital protected by two levels of secure access
    - When not in use, portable computers must be stored in locked cabinets or locked offices
    - No personal health information is retained on these premises
2. The Data Centre where records of personal health information in BORN's custody are retained (all personal health information is stored in this secure location; there is no personal health information stored anywhere else)
    - The Data Centre is managed by the BORN System Hosting Provider (a BORN agent) and is protected by four levels of secure access (in a protected area with perimeters secured by entry controls that include tracked badge swipe cards or key locks to ensure that only authorized personnel are allowed access).

As per the policy, BORN Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **S-15: Security Audits**.

Agents are required to notify the Privacy Officer or the Manager of Health Informatics at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

Policy, Procedures and Practices with Respect to Access by Agents
All personal health information in the custody of BORN is stored on secure servers in a Data Centre that is managed by the BORN System Hosting Provider (a BORN agent). There are four levels of secure access to ensure only authorized personnel are allowed access, including three card accesses equipped with security system logs to track date, time and card ID of each swiped access card.

- The System Hosting Provider Director (CHEO Director of IT Shared Services) authorizes access to the Data Centre through CHEO security. The request outlines the name of the agent and the purpose for which access is required. Access is only requested where it is required to carry out employment/contractual responsibilities
- CHEO security manages the list of users with access to the Data Centre as well as the logs that capture each badge swipe
- CHEO security provides a list of agents with authorized access (audit list) and a list of all associated badge activity (log) to the System Hosting Provider Director annually

With respect to the Data Centre, the System Hosting Provider Director authorizes access via CHEO security for only those employees/agents who need access to the servers to complete their employment tasks.

Access to BORN premises where BORN employees work: provision of identification/access cards and office keys
The BORN premises are located in a secure research institute on the premises of the Ottawa Hospital and are protected by two levels of secure access:

- Building is protected by access cards (swipe)
- Individual offices have locked doors

The BORN human resources agent or designate arranges for an access card and office key as follows:

- CHEO human resources issues a CHEO Employee Staff Action Notice (ESAN) for all new BORN Agents; an ESAN identifies the name, start date and status of the employment arrangement (permanent or temporary, for example)
- CHEO Human Resources issues a secure access card (also a CHEO identification badge)
- BORN Human Resources retains a copy of the ESAN and records the secure access card number and serial number of the office key in the BORN log **S-04: Log of Agents with Access to the BORN Premises**

Theft, Loss and Misplacement of Identification Cards, Access Cards and Keys
Where a BORN agent notes theft, loss or misplacement of identification card/access card to BORN offices:

- The BORN agent reports the missing badge to Ottawa Hospital Photo ID and Parking desk within the Security department (either by e-mail or in person) and the Ottawa Hospital de-activates the badge immediately
- The BORN agent notifies the BORN Human Resources agent of the cancelled badge and the BORN Human Resources agent or designate arranges for a new badge to be issued. BORN does not issue temporary badges
- The BORN Human Resources agent records the date of loss and the ID of the replacement badge in the BORN log **S-04: Log of Agents with Access to the Premises**

Where a BORN agent notes theft, loss or misplacement of an office key:

- The BORN agent reports the missing key to the BORN Human Resources Agent or designate who arranges for a replacement key to be cut

- The BORN Human Resources Agent or designate records the date of loss and the replacement key number in the BORN log **S-04: Log of Agents with Access to the Premises**

Where the BORN System Hosting Provider (agent) notes the theft, loss or misplacement of identification card/access card to the Data Centre:

- The BORN System Hosting Provider agent notifies CHEO security immediately (by phone, in person or by e-mail) as well as the System Hosting Provider Director and CHEO Human Resources
- CHEO security de-activates the badge
- CHEO Human Resources issues a new badge and informs CHEO Security of the new badge ID
- Where the BORN System Hosting Provider agent notes that a badge is missing but has not yet confirmed its loss, CHEO Security immediately de-activates the badge and issues a one-day temporary badge with automatic expiry

Termination of the Employment, Contractual or Other Relationship

BORN Agents and their supervisors must adhere to BORN policy **HR-10 Termination and Cessation of Employment** when a decision is taken to terminate their role. Badge and key return are part of **HR-10 Termination and Cessation of Employment**. The written notification detailed in **HR-10** sets out:

- Name of the Agent
- Date at which access is to be terminated and reason(s) for termination
    - Name of Agent
    - Termination date
    - Reasons for termination
- Date at which identification card, access card and/or keys will be returned by the Agent to the Privacy Officer

Where a BORN System Hosting Provider agent with access to the Data Centre is terminating their employment, the System Hosting Provider Director forwards the termination date to CHEO Security and the badge is de-activated on the last day of employment. This is captured in the log of agents with access to the Data Centre and maintained by the Secure System Hosting Provider.

Audits of Agents with Access to the Premises

BORN System Hosting Provider Director and the BORN Privacy Officer together verify the following:

- CHEO security audit list that includes names of agents granted approval to access the Data Centre, the date access was granted/access card enabled, ID number on the access card, the date of the next audit, date access terminated
    - This audit list is reviewed annually and used to confirm on-going access is required
- The Hosting Provider has an automated mechanism to capture events associated with card swiping. This log captures date, time and access card ID for each swipe into the Data Centre. The BORN System Hosting Provider and BORN Privacy Officer together review this log annually. Should there be indication of privacy or security breach, the BORN Privacy Officer acts immediately.

Policy, Procedures and Practices with Respect to Access by Visitors

Visitors to the BORN premises or to the Data Centre location are supervised by a BORN agent at all times. All visitors 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.

If the visitor does not sign out appropriately, it is the duty of the responsible Agent to validate that the visitor has left and provide an estimate of time and other relevant details of departure.

All documentation related to the identification, screening and supervision of visitors is retained by:

- BORN Human Resources agent with respect to visitors to the BORN premises
- BORN System Hosting Provider with respect to visitors to the secure server location

Documentation related to visitors is retained for a minimum of one year to allow for audit in case of breach or similar occurrence.

2.4 Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity

The BORN Human Resources agent or designate is responsible for securely maintaining the **Log of Agents with Access to the BORN Work Premises** that captures the following fields:

- Name of agent granted approval
- Location(S) within the premises to which access is granted
- Date access granted
- Date ID card, access card and/or keys granted
- ID number on ID card and/or keys granted
- Date of next audit of access
- Date ID card, access card and/or keys granted were returned
- Date ID card, access card and/or keys granted were lost, stolen or misplaced
- List of visitors to the BORN office premises

The BORN System Hosting Provider is responsible for the secure retention of:

- A log of agents granted approval to access the Data Centre that captures the name of the agent granted approval to access the secure server room, the date access was granted/access card enabled, ID number on the access card, the date of the next audit, date access terminated.
- List of visitors to the Data Centre

2.5 Policy and Procedures for Secure Retention of Records of Personal Health Information

BORN has in place a policy to ensure the secure retention of records of personal health information in paper and electronic format. While provisions for paper records of personal health information are currently outlined in this policy, BORN no longer permits paper records of personal health information. The policy will be updated to reflect this practice in the 2014-15 annual review of security policies and procedures.

The policy sets out 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. This period of time is also reflected in all BORN collection data sharing agreements. As per BORN policy **P-04: Collection of Personal Health Information**, the data is then converted to de-identified format.

With respect to records of personal health information in paper format, which are prohibited by BORN, the following three statements will be removed from this policy:

- Records of Personal Health Information in paper format are stored securely in locked filing cabinets within locked premises.

- Paper records are only kept long enough to ensure transfer to secure electronic format and are then destroyed as per BORN policy **S-08: Secure Disposal of Records of Personal Health Information**.
- **Note**: This is an interim state pending full electronic adoption where there will be no collection, use or disclosure of personal health information in paper format.

With respect to records of personal health information used for research purposes, the policy sets out that these records must not be retained for a period longer than set out in the research agreement, where all research agreements are dependent upon research ethics board approval. Disposal is monitored by BORN.

The Privacy Officer has responsibility for the secure retention of records of Personal Health Information.

For records of Personal Health Information retained in electronic format, the following safeguards are employed:

- Personal Health Information is securely collected via VPN connection or SSL-secured portal for manual data entry as per BORN policy **S-07: Secure Transfer of Records of Personal Health Information**
- Access to and use of personal health information through the BORN System is role based as per BORN policy **P-08: Limiting Agent Access to and Use of Personal Health Information**
- Access to BORN premises is controlled as per BORN policy **S-03: Ensuring Physical Security of Personal Health Information**
- The BORN System stores the date, time and name of the user entering, accessing, using or transferring personal health information within system audit logs as per BORN policy **S-10: System Control and Audit Logs**. The BORN System has the capability of ascertaining the data values which were created, viewed, updated and deleted at any given time

The BORN policy on secure retention of personal health information clearly states that BORN agents are required to take steps that are reasonable in the circumstances to ensure that personal health information is retained securely and is protected against theft, loss and unauthorized use or disclosure, copying, modification or disposal. The safeguards discussed above include "reasonable steps".

BORN does not contract a third party service provider to retain records of personal health information.

BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **S-15: Security Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

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

BORN has developed and implemented a policy to ensure that personal health information stored on authorized mobile computing equipment is maintained securely and is protected against theft or loss and unauthorized use, access, copying, modification, disclosure or disposal.

It is BORN policy that personal health information not be removed from BORN secured premises for use by BORN agents. Personal health information will not be stored on mobile computing equipment except in very specific and exceptional circumstances.

As per the BORN policy, mobile computing equipment includes laptops, universal serial bus (USB) flash drives, external hard drives, CDs, DVDs and other mobile and mass storage devices as authorized in writing by the Privacy Officer.

As per policy directions, BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and/or the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**. The policy also states that agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics in accordance with BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

Where Personal Health Information is Permitted to be Retained on a Mobile Device
The BORN policy sets out that agents may retain records of personal health information on a mobile device only when the information is being used for research purposes (as per BORN policy **P-10: Use of Personal Health Information for Research**) or for the purpose of facilitating and improving the provision of health care, and when the elements of this policy have been satisfied.

Approval Process
As per policy directions, in order to retain personal health information on a mobile device or to access personal health information remotely, an agent must make a request to the Privacy Officer via e-mail setting out:

- The circumstances requiring the retention of personal health information on a mobile device or remote access of personal health information
- Why de-identified and/or aggregate information will not serve the identified purpose
- The length of time the information is required to be retained or the length of time remote access is required to achieve the purpose

In determining whether to approve the request, the Privacy Officer considers the following factors:

- Is remote access or use of a mobile device required to achieve the agent's functions
- Will de-identified and/or aggregate information serve the identified purpose
- Is the amount of personal health information requested the minimum required to meet the identified purpose
- Has the agent's use of personal health information been approved under BORN policy **P-08: Limiting Agent Access to and Use of Personal Health Information**
- Is the timeframe the minimum necessary to achieve the purpose

The policy sets out that the Privacy Officer enters all approvals in the BORN log **S-06B: Log of Agent Use of Mobile Devices/Remote Access** and e-mails the agent, with copy to the agent's supervisor, with the approval indicating that the mobile device can be removed and remote access can be initiated when BORN template agreement **S-06A: Agreement for Use of Mobile Devices/Remote Access** has been signed.

Conditions or Restrictions on the Retention of Personal Health Information on a Mobile Device
The BORN policy requires:

- Agents must ensure that a strong and complex password is used and that the password for the mobile device and for remote access is different from passwords for files containing the personal health information and that the password is supported by "defense in depth" measures as per BORN policy **S-09: Passwords**.
- Mobile devices must use full disk encryption.

- Where mobile devices have display screens or where personal health information is being accessed remotely, mandatory password-protected screen savers are enabled after 15 minutes of inactivity.

The Privacy Officer is responsible for ensuring these security protections are in place.

As per the policy, agents granted approval to securely retain records of personal health information on mobile devices must sign a BORN agreement (**Agreement for Use of Mobile Devices**) that includes the following provisions:

- Agents are prohibited from retaining personal health information on the mobile device or remotely accessing personal health information if other information, such as de-identified and/or aggregate information, will serve the purpose.
- Personal health information must be de-identified to the fullest extent possible. The code needed to unlock the personal health information must be stored separately and securely.
- Agents are prohibited from retaining more personal health information on the mobile device or from remotely accessing more personal health information than is reasonably necessary for the identified purpose.
- Agents are prohibited from retaining personal health information on the mobile device or for remotely accessing personal health information for longer than necessary to meet the identified purpose.
- Agents must ensure that a strong and complex password is used and that the password for the mobile device and for remote access is different from the passwords for files containing the personal health information and that the password is supported by "defense in depth" measures as per BORN policy **S-09: Passwords.**

In relation to mobile devices, the policy states that once the intended purpose and use is accomplished, the agent will securely remove or destroy personal health information within five days of completion of the work that necessitated its storage on the mobile computing device as per BORN policy **S-08: Secure Disposal of Records of Personal Health Information.**

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

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.

Approval Process

The policy states that a BORN agent accessing through the internet must establish a VPN connection to the eHO network (provided by the Hosting Provider) and then login to the BORN portal. The BORN System has idle timeouts implemented to safeguard the data. Access to BORN data remotely must be approved and is described fully in the following policies:

- Access to the BORN Information System (web login): BORN policy **P-08: Limiting Agent Access to and Use of Personal Health Information.**
- Remote access to the CHEO system: BORN policy **S-14: Acceptable Use of Technology**.

Both of these policies (**P-08: Limiting Agent Access to and Use of Personal Health Information and S-14: Acceptable Use of Technology)** identify the process that must be followed and the agent responsible for receiving, reviewing and determining whether to approve or deny a request for remote access to personal health information. This includes a discussion of what documentation must be completed, by which agent, to whom this documentation must be provided, the content of the documentation, approval/denial process (requirements and criteria to be considered, including whether de-identified

and/or aggregate information will serve the purpose instead, and that no more personal health will be accessed than is reasonably necessary to meet the identified purpose). Conditions and restrictions are outlined in each of the policies, as is the manner/method/format of communicating the decision to approve/deny a request and to whom. Safeguards required by agents in remotely accessing personal health information are referenced as appropriate from each policy.

2.7 Policy and Procedures for Secure Transfer of Records of Personal Health Information

BORN has in place a policy and supporting procedure to ensure the secure transfer of records of personal health information regardless of format.

The policy requires the following:

- Records of personal health information in electronic format must be transferred in a secure manner
- Agents must use only the approved methods of transferring records of personal health information in electronic format
- Paper-based transfers of personal health information are not permitted
- Agents are not permitted to transfer personal health information by fax

Transfer Out of BORN

BORN uses a secure FTP server and password protection to transfer personal health information to recipients. Where the transfer of personal health information is permitted, the Scientific Manager or designate:

- Reviews the file containing personal health information to be transferred to ensure that it is consistent with the approved request for personal health information
- Ensures the file containing personal health information is further secured using password protection
- Places the information on the secure FTP server
- Notifies the recipient via e-mail that the file containing personal health information is available on the FTP server

The recipient must call the BORN Scientific Manager or designate to confirm receipt of the data and to obtain the password to de-crypt the data set.

The BORN Scientific Manager or designate removes the file from the secure FTP server when the recipient acknowledges receipt of the data.

When receipt has been confirmed, the Scientific Manager updates **P-11A: Data Tracking Log** with the date and time of transfer, nature of the records of personal health information transferred, mode of transfer, recipient of the records and date receipt of records was confirmed.

Where use of the FTP server is not possible, the Scientific Manager may approve transfer of personal health information as follows:

- The personal health information is stored on a disk encrypted with secure socket layer encryption and password protected as per BORN standards.
- The Scientific Manager or designate reviews the file containing personal health information to be transferred to ensure that it is consistent with the approved request for personal health information
- The recipient must call the BORN Scientific Manager or designate to confirm receipt of the data and to obtain the password to de-crypt the data set.

When receipt has been confirmed, the Scientific Manager updates **P-11A: Data Tracking Log** with the date and time of transfer, nature of the records of personal health information transferred, mode of transfer, recipient of the records and date receipt of records was confirmed.

Records of personal health information transferred out of BORN are subject to retention and destruction guidelines in the associated research agreement or data sharing agreement.

Transfer in to BORN
Personal health information collected electronically from health information custodians is transferred over the eHO ONE network protected by VPN, and via secure FTP. Health information custodians located in facilities connected to eHO connect to the BORN portal using their Internet browser utilizing industry standard SSL encryption. Users located on the Internet must establish a VPN connection to the eHO network (provided by Hosting Provider) and then login to the BORN portal or connect via a secure FTP connection. BORN applications have idle timeouts implemented to safeguard the data.
Where personal health information is transferred between BORN and prescribed entities, BORN Ontario will use the secure network provided by the prescribed entity.

The Privacy Officer ensures that policies and procedures regarding secure transfer are updated on an on-going basis to reflect:

- Orders issued by the Information and Privacy Commissioner of Ontario under the *Personal Health Information Protection Act, 2004* and its regulation
- Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario, including Privacy Protection Principles for Electronic Mail Systems and Guidelines on Facsimile Transmission Security; and
- Evolving privacy and security standards and best practices

BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with BORN policy **S-15: Security Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

2.8 Policy and Procedures for Secure Disposal of Records of Personal Health Information

BORN has in place a policy and related procedure to securely dispose of records of personal health information in both paper and electronic format.

Note that paper records of personal health information are prohibited at BORN and references in this policy to the handling of paper records of personal health information will be removed in the next iteration of this policy.

“Disposed of in a secure manner" as per BORN policy means that the records are destroyed in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstances.

As per the policy, records of personal health information in paper format paper are disposed of using a cross-cutting shredding method and incineration to eliminate the possibility of reconstructing the documents.

The Privacy Officer is responsible for ensuring that paper records of personal health information intended for secure disposal are maintained separately from other records intended for recycling in a

designated and locked bin clearly marked for the secure retention of records of Personal Health Information pending their secure disposal.

Records of personal health information in electronic form and/or on removable devices such as floppy disks, CDs, USB keys, and hard drives are disposed of by physically damaging the item to render it useless (e.g. snapping into pieces, hammering, drilling holes into, obliterating, or pulverizing). If re-use is being considered (such as re-using a hard drive or USB key), the device will be wiped using a secure wiping utility that is specific to the device/media.

The Privacy Officer is responsible for ensuring that CDs, USB keys and hard drives intended for destruction are maintained separately in a designated and locked bin clearly marked for the secure retention of records of Personal Health Information, pending their secure disposal.

The Privacy Officer reviews the policies and procedures regarding secure destruction on an on-going basis to ensure that they remain consistent with:

- The *Personal Health Information Protection Act, 2004* and its regulation
- Orders issued by the Information and Privacy Commissioner
- Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner

BORN Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with **BORN policy S-15: Security Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

2.9 Policy and Procedures Relating to Passwords

BORN has developed and implemented a policy to ensure that it maintains system integrity through appropriate password creation, security and administration. The policy states that agents are required 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 sets out that the authentication systems within the BORN System require that passwords contain:

- A minimum of six (6) characters
- Both upper case and lower case letters
- A minimum of one numeric or non-alphanumeric character(s)

As per the policy:

- Passwords expire automatically every 90 days and cannot be reused for at least five iterations
- The BORN system de-activates a user after five (5) failed log-in attempts, at which point the user account becomes inactive until the user can successfully authenticate him or herself to an appropriate system administrator to have it reactivated/unlocked
- The application automatically logs users out after 15 minutes of inactivity forcing users to re-authenticate in order to continue

The policy mandates that agents must ensure the privacy of their passwords and must not:

- Write down passwords

- Display, reveal, hint at, provide, share or otherwise make their password known to any other individual, including another BORN agent

It is clear in the policy that BORN users and agents must change their password immediately if they suspect it has become known to another individual including another agent.

The Privacy Officer, as per the policy, reviews policies and procedures related to passwords on an on-going basis to ensure that they are consistent with:

- Orders issued by the Information and Privacy Commissioner
- Guidelines, fact sheets, and best practices issued by the Information and Privacy Commissioner
- Evolving privacy and security standards and best practices

As per policy directions, BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and/or the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**. The policy also states that agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics in accordance with BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy

2.10 Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs

BORN has developed a policy to ensure system integrity through review of system controls. 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 policy states that:

- 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 (including screen names and report view names), the name of the user that performed the action or operation and the changes to values, if any. Each of these events is retained in the audit logs.
- System design parameters include the capabilities to undertake a complete ascertainment of the data values which were created, viewed, updated, and deleted at any given time.
- The BORN Application Service Provider is responsible for the day-to-day maintenance of the information in the system control and audit logs including:
    - Date and time that personal health information is accessed
    - Name of user accessing personal health information
    - Network name or identification of computer through which the connection is made
    - Creation, amendment, deletion or retrieval of personal health information, the date and time of the action, the name of the user and the changes to values if any
- The Manager of Health Informatics and the Privacy Officer are responsible for determining the nature and scope of events to be audited and for monitoring that all audits are logged in the audit logs.
- BORN System Hosting Provider is responsible for ensuring that:
    - The system does not allow the audit log to be tampered with such that the audit history can be altered or cleared of any events that have been captured
    - The audit controls remain operational at all times and cannot be bypassed through any method

    - Audit history is retained on-line such that it can be reviewed for a period of two years from the date of the event. After two years, audit history will be retained off-line for an indefinite period of time
    - Each event is retained in the logs
- The Manager of Health Informatics is responsible for monitoring the logs on a monthly basis and, should there be an indication of privacy or security breach or an attempted privacy or security breach, the Manager of Health Informatics immediately reports to the Privacy Officer as per BORN policy **P-29: Privacy Breach Management** or BORN policy **S-17: Security Breach Management**.
- The Manager of Health Informatics provides a report regarding the monitoring of the system control and audit logs to the Privacy Officer on a monthly basis.
- The Privacy Officer is responsible for reporting to the Privacy and Security Review Committee on a monthly basis. The monthly reporting includes:
    - Number and type of audits undertaken
    - Findings of the audits
    - Efforts undertaken to address findings
    - Status of these efforts
- The Privacy Officer is responsible for addressing the findings arising from the review of system control and audit logs by:
    - Assigning agents to address the findings
    - Establishing timelines to address the findings
    - Monitoring and ensuring the findings are addressed within timelines

As per policy directions, BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and/or the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**. The policy also states that agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics in accordance with BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

2.11 Policy and Procedures for Patch Management

BORN has in place a policy for patch management. As per the BORN policy, the BORN System Hosting Provider and the Application Service Provider notify the BORN System Administrator when a patch becomes available and make a recommendation regarding whether or not the patch should be installed. For Microsoft products supported by Windows Update service (WSUS), patches become available automatically on a monthly basis. For all other products, the recommended procedure from the vendor will be followed.

The BORN policy sets out that the Hosting Provider and the Application Service Provider notify the BORN System Administrator about patches using the BORN form **S-12B: Change Request Form**. While the policy contains this instruction, current practice is that notice is done via e-mail. BORN is evaluating which method is the most effective and will update the policy if e-mail remains the chosen method.

The BORN System Administrator is responsible for approving or denying the patch. The BORN System Administrator uses the information that accompanies the patch (e.g. release notes and comments from Hosting Provider and Application Service Provider) to make a final decision regarding whether the patch must be applied. In determining whether to apply the patch and when, the BORN System Administrator

considers the balance between ensuring maximal system security and efficiency vs. the potential service disruption and general risk in applying the patch.

The policy states that where it is determined a patch *should not be* implemented, the BORN System Administrator documents the following details in the BORN log **S-12A: Log of Change Requests**:

- Description of the patch
- Date the patch became available
- Severity level of the patch
- Information system, technology, equipment, resource, application or program to which the patch relates
- Rationale for not implementing

The policy also states that where it is determined a patch *should be* implemented, the BORN System Administrator documents in the change request ticketing system:

- Description of the patch
- Date that the patch became available
- Implementation timeframe, where applicable
- Severity level of the patch
- Priority level of the patch
- Information system, technology, equipment, resource, application or program to which the patch relates
- Rationale for the determination that the patch should be implemented
- Date the patch was implemented
- Agent(s) responsible for implementing the patch
- Date when the patch was tested
- Description/procedure of required patch testing
- Agent(s) responsible for testing
- Whether or not the testing was successful

As per policy directions, BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and/or the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**. The policy also states that agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics in accordance with BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

2.12 Policy and Procedures Related to Change Management

BORN has in place a policy and supporting procedure in place for receiving, reviewing and determining whether to approve or deny a request for a change to its operational environment.

The policy identifies that the Manager of Health Informatics (or delegate) receives and reviews change requests as follows:

- Change requests are submitted on a Change Request form that includes a description of the proposed change, rationale for the change, impact of executing or not executing the change, and the impact on privacy and security of the proposed change.

The Manager of Health Informatics reviews the request and makes a recommendation to approve a change request based on the following criteria:

- Change will prevent system failure, change will fix a bug, change solves an identified problem, the importance of the change outweighs anticipated downtime, the balance between maximal system security and the possibility of a privacy or security risk being introduced.

Where a decision is made to approve the change based on the criteria outlined above but there is a possibility of a privacy or security risk, the Manager of Health Informatics sends an e-mail to the Privacy Officer setting out a description of the change and describing the nature of the privacy or security risk. The Privacy Officer forwards the e-mail to the Privacy and Security Review Committee for approval to proceed. When the Committee e-mails approval, the Privacy Officer forwards the approval to the Manager of Health Informatics.

Where a change request is denied, the Manager of Health Informatics notifies the requestor via e-mail and documents the decision in the log of change requests, including: change requested, name of agent requesting change, date change requested, date change denied, rationale for not implementing the change.

Approved changes to the operational environment proceed as follows:

- The Manager of Health Informatics notifies the requestor, the Application Service Provider and Hosting Provider about the approved changes via e-mail.
- The Manager of Health Informatics documents all decisions in the Log of Change Requests including the following information:
    - Change requested
    - Name of Agent requesting change
    - Date change requested
    - Date change approved
    - Potential risk to privacy and security of the change
    - Rationale for approval
    - The priority assigned to the change
    - The expected timeframe for implementation
    - The expected timeframe for testing
    - The expected procedure for testing
    - The date the ticket was given to the BORN System Hosting Provider

Depending on the nature of the change, either the BORN System Hosting Provider or the Application Service Provider is responsible for implementation of the change.

When the change is implemented, the responsible Provider sends a confirmation e-mail to the Manager of Health Informatics who updates the records in the Log of Change Requests including:

- Date change tested
- Date change was implemented
- Confirmation that ticket closed

BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and/or the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**.

Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics in accordance with BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

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

BORN has in place a policy for the systematic back-up and recovery of records of personal health information to maintain the security of records of personal health information in its custody.

The BORN policy specifically identifies the types of back-up storage devices that are used, the minimum frequency with which records of personal health information are backed up, the agent responsible for this activity (BORN System Hosting Provider), as well as the process that must be followed.

The policy clearly states the minimum encryption that must be used on all back-up media containing personal health information.

The policy is also clear in where and how back-ups are stored.

The policy outlines the steps for testing back-ups of records of personal health information, the agents responsible for this testing, the frequency with which the testing is completed (quarterly) and the documentation that results from the testing.

The policy identifies the BORN System Hosting Provider as the agent responsible for ensuring that the back-up storage devices containing records of personal health information are retained in a secure manner, compliant to the BORN policy **S-05: Secure Retention of Records of Personal Health Information**. The policy also states the length of time they are required to be retained.

As per policy directions, BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and/or the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**. The policy also states that agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics in accordance with BORN policy **S-17: Security Breach Management** as appropriate. Consequences of breach are detailed in each respective breach policy.

2.14 Policy and Procedures on the Acceptable Use of Technology

BORN has in place policy **S-14: Acceptable Use of Technology** to ensure that BORN agents understand how to abide by the acceptable use of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by BORN.

The BORN policy contains the following list of elements that are prohibited without exception. The list includes:

- Using unencrypted mobile media such as USB keys
- Removing from the premises computers containing personal health information
- E-mailing personal health information
- Faxing personal health information
- Attempting to gain access to any data or programs for which written authorization from the Privacy Officer does not exist
- Use of information systems for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, harassment, intimidation, impersonation and computer tampering (e.g. spreading of computer viruses or other malicious software)
- Creating, viewing, copying, altering, or deleting information systems data belonging to BORN without permission

- Sharing information system account passwords with another person or attempting to obtain another person's information system account password. Information system accounts are only to be used by the registered user
- Use of information systems in any way that violates BORN policies and procedures

The BORN policy contains the following list of elements that are permitted only with prior approval:

- Use of encrypted mobile media devices such as USB key which contain containing personal health information as per:
    - BORN policy **S-06: Secure Retention of Records of Personal Health Information on Mobile Devices**
        - This policy identifies the process that must be followed and the agent responsible for receiving, reviewing and determining whether to approve or deny a request for remote access to personal health information. This includes a discussion of what documentation must be completed, by which agent, to whom this documentation must be provided, the content of the documentation, approval/denial process (requirements and criteria to be considered, including whether de-identified and/or aggregate information will serve the purpose instead, and that no more personal health will be accessed than is reasonably necessary to meet the identified purpose). Conditions and restrictions are outlined in each of the policies, as is the manner/method/format of communicating the decision to approve/deny a request and to whom. Safeguards required by agents in remotely accessing personal health information are referenced as appropriate from the policy.
- Remote access to applications and resources through Internet access on a computer equipped with an approved remote access client, as per the CHEO Information Services remote access control form, which documents and tracks:
    - Requested applications and resources for which access is being requested
    - Request date and time
    - Determination that the user's job requires remote access to CHEO applications
    - Name of person submitting form
    - Name and signature of Authorized Person approving the access, where Authorized Person is defined as a Director
    - Department to receive the form
    - Method and format for the approval to be communicated to the employee, and the department issuing the communication

As per policy directions, BORN agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and/or the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**. The policy also states that agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with BORN policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics in accordance with BORN policy **S-17: Security Breach Management** as appropriate.

2.15 Policy and Procedures In Respect of Security Audits

BORN has in place a policy, **S-15: Security Audits,** to ensure that BORN conducts regular security audits. As per the policy, BORN conducts the following types of security audits:

- Compliance with security policies and procedures
- Threat Risk Assessments (both internal and external)

- Vulnerability assessments
- Penetration testing
- Ethical hacks
- Audit of security controls (implemented and planned) to assess effectiveness
- Reviews of system control and audit logs

The policy states that an annual audit plan is written by the Privacy Officer and the Manager of Health Informatics and must contain, for each audit conducted:

- Purpose of the security audit
- Nature and scope of the security audit (e.g. interviews, site visits, inspections)
- Timeframe for the security audit
- Framework for the audit, including questions or areas of concern
- Agent responsible for conducting the security audit
- Frequency with which each security audit will be conducted
- Circumstances in which the security audit will be conducted
- Process to be followed in conducting the security audit
- Whether notification will be provided, to whom it will be provided and the content of the notification

As per the policy, the Manager of Health Informatics implements the annual security audit plan and provides a written report to the Privacy Officer that outlines, for each audit conducted:

- Audit as identified in the annual plan
- Scope of the audit
- Methodology employed
- Findings/risk scores
- Recommendations

The policy sets out that the Privacy Officer assigns agents to address any recommendations arising from the security audit, sets out timelines for completion, and updates the BORN log **S-16: Log of Security Audits** as well as the BORN log **O-07: Consolidated Log of Recommendations**. As per the policy, the Privacy Officer monitors to ensure that recommendations are implemented within stated timeframes.

BORN's security audit policy requires the Privacy Officer to securely maintain the following documentation:

- Log of Security Audits
- Log of Consolidated Recommendations
- Description of security audits, recommendations and actions taken in BORN Privacy and Security Reports (quarterly and annual reports)
- Audit reports from the Manager of Health Informatics

The Privacy Officer includes a description of security audits, recommendations and actions taken in:

- Quarterly privacy reports to the Privacy and Security Review Committee and the Leadership Team
- Annual Report on Privacy and Security

The BORN Executive Lead is a member of the Leadership Team.

The policy requires agents responsible for conducting security audits to notify the Privacy Officer and the Manager of Health Informatics at the first reasonable opportunity of a security breach or suspected security breach in accordance with BORN policy **S-17: Security Breach Management**, and of a privacy

breach or suspected privacy breach in accordance with BORN policy **P-29: Privacy Breach Management**. Consequences of breach are detailed in each respective breach policy.

2.16 Log of Security Audits

BORN has in place a policy that requires the maintenance of a log of security audits that that have been completed. The log sets out the nature and type of the security audit conducted, the date the security audit was completed, the agent(s) responsible for completing the security audit, any recommendations arising from the security audit as well as the agent responsible for addressing each recommendation and the date that each recommendation is expected to be addressed and is addressed, and the manner in which each recommendation is to be addressed.

2.17 Policy and Procedures for Information Security Breach Management

BORN has developed and implemented a policy for security breach management to address the identification, reporting, containment, notification, investigation and remediation of security breaches.

The policy defines a security breach as follows:

- Any act or incident in contravention of the security policies and procedures and practices implemented by BORN
- Any act or incident, internal or external, that affects the confidentiality and integrity of information in the custody and control of BORN

The BORN security breach management policy requires every agent to notify the Privacy Officer and the Manager of Health Informatics as soon as reasonably possible, and to do whatever is reasonably possible to contain a security breach or suspected security breach, whether internal or external, and to mitigate its effects immediately.

The policy provides contact information for both the Privacy Officer and the Manager of Health Informatics. The policy states that notification of a security breach may be made verbally to the Privacy Officer and the Manager of Health Informatics and must include:

- Type of suspected breach
- Location of suspected breach
- Any actions taken by the reporting agent to contain the breach

Where the breach is reported by an individual observing a contravention of security policy and an oral report is made to the Privacy Officer and the Manager of Health Informatics, the individual completes and forwards a Breach Reporting Form to the Privacy Officer and the Manager of Health Informatics, where the form contains the following:

- Name and position of the individual who discovered the incident
- Date and time of discovery of the incident
- Estimated time and date the breach occurred, if known
- Type of breach (loss, theft, inadvertent disclosure)
- Cause of breach, if known
- Description of information involved in the breach
- Actions taken by agent reporting the breach to contain the breach, if applicable
- Any other individuals or organizations involved in the breach (or its notification) and contact information for relevant individuals

The Privacy Officer and the Manager of Health Informatics, together with the Hosting Provider and the Application Service Provider (as applicable), determine what (if any) personal health information has been stolen, lost or accessed, used, disclosed, copied, modified or disposed of in an unauthorized

manner. If the Privacy Officer determines that the information security breach involves the unauthorized collection, use, disclosure, retention, or disposal of personal health information in violation of the *Personal Health Information Protection Act, 2004* and its regulation or in violation of any of the BORN privacy policies and procedures, then BORN policy **P-29: Privacy Breach Management** applies.

As per the BORN policy, the Privacy Officer notifies the BORN Director as soon as reasonably possible that a security breach has occurred, indicating that:

- A security breach or potential security breach has occurred and whether it is internal or external
- A brief description of the nature and extent of the breach, including what information has been breached
- Actions taken by agent reporting the breach, the Privacy Officer, and the Manager of Health Informatics, BORN System Hosting Provider, Application Service Provider (as applicable) to contain the breach
- The police have been notified and why, if applicable

The BORN Director forwards the Privacy Officer's notification e-mail and a description of any further efforts at containment to the Leadership Team as soon as is reasonably possible. The BORN Executive Lead is a member of the Leadership Team.

Containment of a security breach, as per the BORN policy, begins immediately as the agent who discovers a breach must, as per policy requirements, initiate the process of containment as appropriate to the breach. Once the breach has been reported, the Privacy Officer and the Manager of Health Informatics, together with the Hosting Provider and Application Service Provider (as applicable) work immediately to further contain the breach and where it is determined that a breach or potential breach would allow unauthorized access to any other data, any action necessary is taken to ensure no further breaches can occur through the same means (e.g. change password, shut down the system) and that the breach is contained.

The BORN policy states that the BORN Director, in consultation with the Privacy Officer, the Manager of Health Informatics, and the relevant agent, reviews the containment measures implemented to determine that the security breach has been effectively contained. Where further measures are required, the BORN Director works with the Privacy Officer, Manager of Health Informatics, Hosting Provider and Application Service Provider (as applicable) to ensure secure containment. The containment measures are documented in the Privacy Officer's e-mail to the BORN Director.

The BORN security breach management policy states that whenever personal health information is lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization, the Privacy Officer sends a written notification to the heath information custodians or organization who provided the information at the first reasonable opportunity in order that they may notify individuals whose privacy was breached as per section 12(2) of the *Personal Health Information Protection Act, 2004*. As a prescribed registry, BORN does not directly notify individuals whose information has been breached.

The written notification will include:

- Date of the security breach
- A general description of the extent of the breach
- Nature of the information that was the subject of the security breach
- Date that the security breach was contained and the nature of the containment measures
- Steps that have been taken to reduce the possibility of future breaches
- Steps the individual can take to further mitigate the risk of harm (where applicable)

- Notice that the Information and Privacy Commissioner has been contacted
- Name and phone number of contact person within BORN who can answer questions
- A statement that individuals have a right to complain to the Information and Privacy Commission and the contact information for the Commissioner.

The BORN policy on security breach management includes the following directions with respect to notification of other persons or organizations:

- The BORN Leadership Team is notified by the BORN Director (who forwards the Privacy Officer's e-mail and a description of any further efforts at containment) as soon as is reasonably possible.
- The Information and Privacy Commissioner may be notified; the decision to notify made between the Privacy Officer and the BORN Director and, if deemed necessary, results in an e-mail from the Privacy Officer to the office of the Information and Privacy Commissioner indicating that:
    - A security breach has occurred
    - A brief description of the nature and extent of the security breach, including what information has been breached
    - Actions taken by the agent reporting the security breach and the Privacy Officer to contain the breach
    - The police have been notified and why (if applicable)
- BORN staff, the Leadership Team and the CHEO Chief Privacy Officer receive e-mail updates from the Privacy Officer on a regular basis.

Investigation

When the breach has been contained and the BORN Director informed, the Privacy Officer together with the appropriate BORN agents initiates a comprehensive investigation, including interviews, document reviews, site visits and inspections. The review will determine:

- Organizations involved in the breach
- Cause of the breach
- Data elements involved
- Number of individuals affected by the breach
- Identification of individuals affected by the breach
- Any harm that may result from the breach, including:
    - Security risk
    - Identity theft or fraud
    - Hurt, humiliation, damage to reputation
- Actions required to prevent future breaches

The Privacy Officer completes the comprehensive investigation within four weeks of the time the breach was reported and prepares a comprehensive report for the Director, including:

- Date of the security breach
- Date that the security breach was identified or suspected
- Nature of the security breach, that is, whether it was determined to be a security breach and whether it was internal or external
- Nature of the information that was the subject matter of the security breach
- Facts or events relevant to the security breach
- Date that the security breach was contained and the nature of the containment measures
- Date that the health information custodian or other organization that disclosed the personal health information to BORN was notified
- Date that the investigation of the security breach was completed

- Agent(s) responsible for conducting the investigation
- Recommendations for corrective measures arising from the investigation
- Agent(s) assigned to address each recommendation and the date each recommendation is expected to be addressed

The BORN Director reviews the report and forwards it to the Leadership Team for approval to proceed with implementation of the recommendations. Once approved, the Privacy Officer:

- Assigns agent(s) to implement changes
- Establishes and monitors timelines for implementation
- Monitors and tracks these activities to ensure that recommendations are implemented within the stated timelines

The BORN Privacy Officer is responsible for maintaining a log of security breaches and for ensuring that the recommendations arising from the investigation of security breaches are addressed within identified timelines.

The Privacy Officer is responsible for securely maintaining correspondence related to the security breach, the investigative report on the security breach, and the log of security breaches.

BORN agents are required to comply with the security breach management policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer and the Manager of Health Informatics in accordance with BORN policy **S-15: Security Audits**. Consequences of breach are detailed in each respective breach policy.

2.18 Log of Information Security Breaches

BORN maintains a log of information security breaches that contains the following information:

- Date of Information Security Breach
- Date Information Security Breach Identified or Suspected
- Nature of the Information Security Breach
- Nature and Extent of PHI Information, if any, that was Affected and the nature and effect of the security breach
- Date Information Security Breach Contained
- Nature of Containment Methods
- Date HIC or other Org that disclosed the Information was notified, if applicable
- Date Investigation Completed
- Agents Conducting Investigation
- Recommendations Resulting from Investigation
- Responsible Agents for Addressing each Recommendation
- Date Each Recommendation is expected to be addressed
- Date Each Recommendation was addressed
- Manner in which each recommendation was or is expected to be addressed

BORN Compliance to IPC Manual Part 3 – Human Resources Documentation

3.1 Policy and Procedures for Privacy and Security Training and Awareness

The BORN **Privacy and Security Training and Awareness Policy** sets out the requirements for mandatory privacy and security training for all BORN staff.

Pursuant to the Policy:

- New employees complete initial privacy and security orientation prior to being given access to personal health information and all employees receive ongoing privacy and security training on an annual basis
- Initial privacy and security orientation is given within two weeks of the start date of a new BORN agent. This session includes role-based training to ensure that agents understand how to apply the privacy and security policies and procedures in their day-to-day employment, contractual or other responsibilities
- The BORN Privacy Officer is responsible for providing initial privacy and security orientation and ongoing privacy and security training for all BORN
- Agents. The hiring manager or designate advises the Privacy Officer via e-mail one week in advance of the starting date of new employees and contractors. The e-mail contains the name of the new agent or contractor, start date and copy of the job description or contract

The BORN Privacy and Security Training and Awareness policy clearly identifies the content of the initial privacy and security orientation to ensure formalized and standardized training. This content includes:

- A description of the status of BORN as a prescribed person under PHIPA as well as the duties and responsibilities that arise as a result of BORN having registry status, including :
    - Having in place practices and procedures to protect the privacy of individuals whose personal health information BORN receives
    - Maintaining the confidentiality of that information
    - Ensuring these practices and procedures are reviewed and approved by the Information and Privacy Commissioner of Ontario
- A description of the nature of the personal health information collected as determined by the BORN Data Collection Review Committee, and the health information custodians from whom this information is typically collected
- An explanation of the purposes for which personal health information is collected and used and how this collection and use is permitted by the *Personal Health Information Protection Act*, *2004* and its regulation
- Limitations placed on access to and use of personal health information based on the “need to know” principle
- A description of the procedure that must be followed in the event that an agent is requested to disclose personal health information
- An overview of BORN privacy and security policies and procedures and the obligations for agents arising from these policies and procedures
- The consequences for agents of breaching BORN privacy or security policies and procedures
- An explanation of the privacy and security program, including the key activities of the program and the role of the Privacy Officer.
- The administrative, technical and physical safeguards implemented by BORN to protect personal health information against theft, loss and unauthorized use or disclosure and against unauthorized copying, modification or disposal
- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by BORN, including the Manager of Health Informatics, the Scientific Manager, the System Administrator, the System Hosting Provider, and the Privacy and Security Review Committee
- A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute, and the key provisions of the Confidentiality Agreement

- An explanation of the policies **P-29: Privacy Breach Management** and **S-17: Security Breach Management** and the duties and responsibilities imposed on agents to identify, report, contain, and participate in the investigation and remediation of privacy and security breaches

The BORN Privacy and Security Training and Awareness policy and procedure identifies that ongoing privacy and security training must be given annually and is formalized and standardized. The content includes:

- Role-based training to ensure that agents understand how to apply the privacy and security policies and procedures in their day-to-day employment, contractual or other responsibilities
- New privacy and security policies and procedures and significant amendments to existing privacy and security policies and procedures, and privacy and security training updates resulting from privacy impact assessments, investigations of breaches and complaints, and privacy and security audits including threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs

This policy also identifies that the Privacy Officer maintains the **Log of Privacy and Security Training**, which includes the name of the agent, the date the agent attended the initial privacy and security orientation, the dates that the agent attended ongoing privacy and security training and the specifics of training provided at each session.

The policy includes a process to track the attendance at the initial privacy orientation as well as the ongoing privacy training.

As per the policy, the Privacy Officer monitors the **Log of Privacy and Security Training** on a monthly basis to ensure that all agents receive required training within acceptable timeframes, sends appropriate reminders, and informs the supervisor and BORN Director if applicable training has not been completed. The Privacy Officer also removes agent(s) name(s) from the **Log of Privacy and Security Training** upon receiving notice of termination, as per policy **P-08: Limiting Agent Access to and Use of Personal Health Information.**

In terms of documentation, the policy states that the Privacy Officer is responsible for securely maintaining the **Log of Attendance at Privacy and Security Training**, attendance sheets from training sessions and all correspondence with agents and supervisors and all training materials. Documents are securely retained as per policy **S-05: Secure Retention of Records of Personal Health Information.**

The BORN policy on **Privacy and Security Training and Awareness** identifies the mechanisms implemented by the Privacy Officer to foster a culture of privacy and to raise awareness of the privacy and security programs and the privacy and security policies and procedures, the frequency of communications with agents in relation to these mechanisms and the nature and method of communication.

The BORN policy on Privacy and Security Training and Awareness clearly states that agents must comply with the policy, that compliance is audited on an ongoing basis by the Privacy Officer in accordance with policy **P-27: Privacy Audits** and policy **S-15: Security Audits** as appropriate, and that if an agent breaches or believes there may have been a breach of this policy or procedures, the agent must notify the Privacy Officer at the first reasonable opportunity, as per policy **P-29: Privacy Breach Management,** or the

Privacy Officer and the Manager of Health Informatics, as per policy **S-17: Security Breach Management** as appropriate.

3.2 Log of Attendance at Initial Privacy and Security Orientation and Ongoing Privacy and Security Training

BORN has in place a **Log of Attendance at Privacy and Security Training** to track the attendance of all BORN agents who attend and obtain initial privacy and security orientation and ongoing privacy and security training. The log sets out the name of the agent, the date that the agent attended the initial privacy and security orientation and the dates that the agent attended ongoing privacy and security training.

3.3 Policy and Procedures for the Execution of Confidentiality Agreements by Agents

BORN has in place policy **HR-05 Execution of Confidentiality Agreements by Agents** to ensure all agents are aware of and confirm their obligations to protect the privacy and confidentiality of the personal health information for which BORN is responsible. As per this policy, BORN agents execute Confidentiality Agreements (as per policy **HR-06: Template Confidentiality Agreement with Agents**) 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 BORN policy identifies that the Privacy Officer is responsible for ensuring that a Confidentially Agreement is signed with each agent of BORN at the commencement of the employment as well as re-signed or re-acknowledged annually.

The policy also clearly states that BORN supervisors or designates are required to inform the Privacy Officer via e-mail one week in advance of the starting date for new employees and contractors, where the e-mail must contain the name of the new agent or contractor, start date and copy of the job description or contract.

The BORN Privacy Officer tracks the execution of Confidentiality Agreement as per the policy by maintaining the **Log of Executed Confidentiality Agreements with Agents**. The policy sets out that where the agent or contractor has not executed or renewed the Confidentiality Agreement by the renewal date, the Privacy Officer informs the supervisor and the BORN Director within a defined time period.

The policy also indicates that the Privacy Officer is responsible for securely storing Confidentiality Agreements and the **Log of Executed Confidentiality Agreements with Agents**.

The BORN policy on the **Execution of Confidentiality Agreement by Agents** clearly states that agents must comply with the policy, that compliance is audited on an ongoing basis by the Privacy Officer in accordance with policy **P-27: Privacy Audits** and/or policy **S-15: Security Audits** as appropriate, and that if an agent breaches or believes there may have been a breach of this policy or procedures, the agent must notify the Privacy Officer at the first reasonable opportunity as per policy **P-29: Privacy Breach Management**.

3.4 Template Confidentiality Agreement with Agents

The content of the BORN Confidentiality Agreement executed by all agents includes:

General Provisions
The BORN template confidentially agreement describes the status of BORN under the Act, as a prescribed registry, as well as the duties and responsibilities that arise from having registry status. The agreement states that the individuals signing the agreement are agents of BORN and outlines the responsibilities associated with this status.

The Confidentiality Agreement also states that agents are responsible and accountable for ensuring they act in accordance with the Act and its regulation as related to BORN, the provisions of the Confidentiality Agreement, and the BORN privacy and security policies and procedures.

The BORN Confidentiality Agreement provides a definition of personal health information which is consistent with the Act and its regulation.

The Confidentiality Agreement is executed at the end of the initial privacy and security orientation, at which point each agent is also provided with the BORN Privacy and Security Management Plan, which contains all privacy and security policies and procedures. As agents have not yet had time to read this book, the Confidentiality Agreement does not satisfy the following IPC required statement:
Agents must also be required to acknowledge that they have read, understood and agree to comply with the privacy and security policies, procedures and practices implemented by the prescribed person or prescribed entity and to comply with any privacy and security policies, procedures and practices as may be implemented or amended from time to time following the execution of the Confidentiality Agreement.

Rather, each agent is required to reply to an e-mail from the privacy officer, after they have undergone privacy training and have read through all BORN privacy and security policies and procedures, to confirm the following:
I have read, understood and agree to comply with the privacy and security policies and procedures implemented by BORN and I will comply with any privacy and security policies and procedures that may be implemented or amended from time to time.

Obligations with Respect to Collection, Use and Disclosure of Personal Health Information
The BORN Confidentiality Agreement clearly identifies the purpose for which BORN is permitted to collect, use and disclose personal health information (for the purposes of facilitating and improving the provision of health care to mothers, infants and children). The agreement further sets out that any personal health information collected, used or disclosed must be in accordance with the Act and its regulation, the provisions of the Confidentiality Agreement, the BORN privacy and security policies and procedures, or as required by law.
This agreement further includes the following obligations:
Agents agree they will not access or use personal health information if other information will serve the purpose and will not access and use more personal health information than is reasonably necessary to meet the purpose.

Termination of the Contractual, Employment or Other Relationship
The BORN Confidentiality Agreement identifies that agents must return to their supervisor all property of BORN including records of personal health information and all identification cards, access cards and/or keys, on or before the date of termination of employment, contractual or other relationship as per policy **HR-10: Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship**.

Notification
The BORN Confidentiality Agreement sets out that agents agree to notify the BORN Privacy Officer as soon as reasonably necessary if they breach or become aware of a breach of the Confidentiality Agreement, any BORN privacy policy or procedure as per policy **P-29: Policy and Procedures for Privacy Breach Management** and inform the Privacy Officer and Manager of Health Informatics of a breach of security policy or procedure as per policy **S-17: Policy and Procedures for Information Security Breach Management**.

Consequences of Breach and Monitoring Compliance
The BORN Confidentiality Agreement sets out for agents that non-compliance with this agreement or BORN policies and procedures is a serious matter that may be subject to disciplinary action up to and including termination of employment, contractual or other relationships, and that compliance with this agreement will be monitored on an ongoing basis by the Privacy Officer.

3.5 Log of Executed Confidentiality Agreements with Agents

BORN maintains a log of Confidentially Agreements that have been executed by agents at the commencement of their employment, contractual or other relationships, and also on an annual basis. This log contains agent last name, first name, date of commencement of employment, date Confidentiality Agreement initially executed, dates Confidentiality Agreement renewed.

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

BORN has in place a job description for a Privacy Officer who is responsible for the day-to-day management of the privacy program at BORN. The Privacy Officer, as per the job description, reports as follows:

- To the BORN Director
- To the Privacy and Security Review Committee and the Leadership Team on a regular basis about compliance with privacy and security policies and applicable legislation, including quarterly and annual reporting, where the BORN Executive Lead is a member of the Leadership Team

The Privacy Officer job description contains the following responsibilities:

- Developing, implementing, reviewing and amending privacy and security policies and procedures
- Ensuring compliance with the privacy and security policies and procedures implemented at BORN
- Ensuring that the BORN privacy policies and procedures are transparent
- Facilitating compliance with the Act and its regulations
- Ensuring agents are aware of the Act and its regulation and their duties under the Act
- Ensuring that BORN agents are aware of the privacy and security policies and procedures implemented by BORN and that agents are appropriately informed of their duties and obligations
- Directing and delivering the initial privacy and security orientation and the ongoing privacy training and fostering a culture of privacy at BORN
- Conducting, reviewing and approving privacy impact assessments at BORN

- Receiving, documenting, tracking, investigating, remediating and responding to privacy complaints pursuant to the Policy and Procedures for Privacy Complaints
- Receiving and responding to privacy inquiries pursuant to the policy and procedures on privacy inquiries
- Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the policy on privacy breach management
- Conducting privacy audits pursuant to the policy on privacy audits

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

BORN has in place a job description for a Manager of Health Informatics who is responsible for the day-to-day management of the security program at BORN. The Manager of Health Informatics position reports to the Director of BORN on all security-related matters; the BORN Director reports to the BORN Executive Lead.

The Manager of Health Informatics job description contains the following responsibilities:

- Developing, implementing, reviewing and amending security policies and procedures
- Ensuring compliance with the BORN security policies and procedures
- Fostering a culture of information security awareness
- Receiving, documenting, tracking, investigating and remediating information security breaches or suspected information security breaches pursuant to the policy on security breach management
- Conducting security audits pursuant to the policy on security audits

The following two IPC requirements listed under the Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program are the responsibility of the Privacy Officer at BORN, and are included in the job description for the Privacy Officer:

1. Ensuring agents are aware of the security policies and procedures implemented by the prescribed person or prescribed entity and are appropriately informed of their duties and obligations thereunder
2. Directing, delivering or ensuring the delivery of the initial security orientation and the ongoing security training

While the content of all security policies and procedures relies heavily on the Manager of Health Informatics, the training and awareness of all policies and procedures at BORN, for both privacy and security, is delivered by the Privacy Officer.

3.8 Policy and Procedures to Termination or Cessation of the Employment or Contractual Relationship

BORN has in place policy **HR-10- Termination or Cessation of the Employment or Contractual Relationship** to address voluntary and involuntary termination or cession of the employment or contractual relationship. All policies and procedures are in alignment with the Children's Hospital of Eastern Ontario (CHEO) Human Resources policies and requirements, and are in full compliance with current employment legislation.

The policy indicates that agents and their supervisors are required to give the BORN Director and the Privacy Officer notice of termination of employment. The notice must be done via e-mail and must contain the name of the agent, the termination date and the reason for termination. Notice is to be

provided two weeks in advance, where possible. Within three days of receipt of this notice, the BORN Director or designate forwards the name of the agent and the termination date to:

- CHEO Human Resources to process termination in payroll system
- Security for termination of access to the building
- Manager of Health Informatics who arranges for the withdrawal of access to personal health information on termination date and updates the **Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information.**

The policy sets out that the agent return all property to the Director, or designate, on or before the date of termination. BORN's definition of property includes 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 as identified.

The policy specifies the following steps with respect to the secure return of property:

- Within three days, the BORN Director, or delegate, e-mails to the Agent (with copy to their supervisor) a request for the secure return to the BORN Director, or designate of all BORN Ontario property on or before the termination date. The BORN Director, or delegate, includes a list of property to be returned and indicates that payroll will be withheld if the specified property is not returned on or before termination date. As well, the BORN Director, or delegate, reminds the Agent of the confidentiality requirements contained in the signed Confidentiality Agreement.
- When the Agent returns the property, the BORN Director, or delegate, checks the list of property and both the Agent and the BORN Director, or delegate, sign the list to acknowledge receipt. The BORN Director retains the signed list in the Agent's employee file. This return of physical property is done in person; return of Personal Health Information is verified as follows:
    - BORN Agents are not expected to have any Personal Health Information in their possession. Personal Health Information, as per the BORN Agent Confidentiality Agreement and policy **S-05: Secure Retention of Records of Personal Health Information** is retained only on the secure CHEO network. BORN does not permit paper records of Personal Health Information? The BORN Director or delegate verifies verbally with the Agent that they do not have any Personal Health Information to return and that they have abided by the obligations of a BORN Agent with respect to Personal Health Information.
- If the Agent does not return the property on or before termination date, the BORN Director, or delegate, sends an e-mail to the Agent requesting return of the property. If the property is not returned within one month from the date of the e-mail the BORN Director mails a registered letter to the Agent requesting the return of the property and indicating the potential for legal action if the property is not returned within one month. If the property has not been returned within one month from the date the registered letter was mailed, a second registered letter will be mailed. If within one month there has been no response, the BORN Director consults with the CHEO Human Resources regarding legal action.

With respect to access to the premises of BORN Ontario to locations where records of personal health information are retained and to the information technology operational environment, all access is terminated on the last day of employment. The BORN Director, or designate is responsible for terminating access. On the last day of employment the agent returns the security badge to the BORN Director or delegate and access to the premises where records of personal health information are

retained and the technology operational environment is no longer possible. Where an Agent does not return the badge, the badge is de-activated by CHEO security The BORN Director, or delegate, signs off on the return of the badge as part of the return of personal property process which is signed by both the agent and the Director, or delegate.

This policy indicates that BORN agents must comply with this policy and procedures and that compliance is audited on an ongoing basis by the Privacy Officer in accordance with policy **P-27: Privacy Audits** and policy **S-15: Security Audits** as appropriate and that if an agent breaches or believes there may have been a breach of this policy or procedures, the agent must notify the Privacy Officer at the first reasonable opportunity, as per policy **P-29: Privacy Breach Management** or the Privacy Officer and Manager of Health Informatics as per policy **S-17: Security Breach Management** as appropriate.

3.9 Policy and Procedures for Discipline and Corrective Action

BORN has in place a policy and procedure for discipline and corrective action in respect of personal health information. The policy sets out that the BORN Privacy Officer investigates all privacy and security related disciplinary matters. In undertaking the investigation to ascertain the facts the Privacy Officer interviews all individuals who have knowledge of the breach incident, interviews the agent involved and his/her supervisor jointly, and reviews all applicable documentation and records. Based on an assessment of the facts, the Privacy Officer meets with the agent and his supervisor jointly to report on findings and to indicate that disciplinary action is being applied. As soon as reasonably possible after this meeting the Privacy Officer sends a written letter to the agent (with copy to the supervisor) documenting the date and time of the follow-up meeting, a brief statement of the issue, the salient facts of the discussion, and the conclusion reached in the meeting regarding disciplinary action. The Privacy Officer, in consultation with the BORN Director and CHEO Human Resources where applicable, determines the type of disciplinary action appropriate to the issue, including:

- Oral warning and/or additional privacy and security training as appropriate for minor first offences
- Written warning and/or additional privacy and security training as appropriate for a more serious offence or after an agent has received an oral warning, where the written warning clearly identifies that the letter is a disciplinary warning, describes the situation which prompted the warning, indicates why the behavior merits a warning and states that should there be a repetition of the behavior, additional corrective action will be taken which could result in termination
- Suspension without pay and/or additional privacy and security training, as appropriate for serious offences or after the agent has received an oral and written warning. The agent is notified in writing and the letter outlines the reasons for the suspension, and the dates of the suspension
- Termination of employment as a penalty for a very serious offence or the culmination of the progressive discipline process. The Privacy Officer and the supervisor hold a pre-termination meeting with the agent to review the past record and/or the circumstances leading to the termination

The policy and procedure indicate that all documentation related to discipline and corrective action is maintained in the agent's file by the BORN Director.

BORN Compliance to IPC Manual Part 4 – Organizational and Other Documentation

4.1 Privacy and Security Governance and Accountability Framework

BORN has a combined policy for **Privacy and Security Governance and Accountability Framework**. This policy is in place to ensure compliance with the Act and its regulation and to ensure compliance with BORN privacy and security policies and procedures.

The BORN Privacy and Security Governance and Accountability Framework establishes that the Chief Executive Officer of CHEO is accountable for ensuring that BORN and its agents comply with PHIPA and its regulation as well as the BORN privacy and security policies and procedures.

The policy identifies that the Chief Executive Officer of CHEO delegates day-to-day responsibility for ensuring that BORN and its agents comply with the Act and its regulation as well as the BORN privacy and security policies and procedures to the BORN Leadership Team. The BORN Leadership Team has delegated authority to manage the day-to-day requirements of the BORN privacy program to the Privacy Officer and the day-to-day requirements of the BORN security program to the Manager of Health Informatics, who both report to BORN Leadership Team on all related privacy and security matters.

The associated responsibilities and obligations of the Privacy Officer and the Manager of Health Informatics are defined in the BORN policy **HR-08 and HR-09: Job Description for Position(s) Delegated Day-to-Day Authority to Manage the Privacy and Security Programs**.

The BORN Privacy and Security Governance and Accountability Framework policy clearly identifies the other individuals, committees and teams that support the Privacy Officer and the Manager of Health Informatics in respect of the privacy and security program. These supports include:

- Privacy and Security Review Committee
- Data Collection Review Committee
- Disclosure of PHI Review Committee
- CHEO Electronic Health Information Laboratory (eHIL)
- BORN Director
- BORN Scientific Manager
- Manager of Health Informatics
- Privacy Officer
- Senior Systems Technical Architect

The **BORN Privacy and Security Governance and Accountability Framework** policy sets out that Privacy Officer provides a quarterly report on privacy and security to the Privacy and Security Review Committee as well as the Leadership Team. This same report is delivered with an annual view as the **BORN Annual Report on Privacy and Security**. Provided by the Privacy Officer, this annual report is reviewed and approved by the BORN Leadership Team and then forwarded to the Chief Executive Officer of CHEO by the BORN Director, who in turn forwards it to the CHEO Board of Directors.

The policy mandates the content of the **BORN Annual Report on Privacy and Security** that is ultimately provided to the CHEO Board of Directors. The **BORN Privacy and Security Governance and**

Accountability Framework policy refers to BORN privacy policy **P-02 A: Annual and Quarterly Reports on Privacy and Security** which is a template for the report, the contents of which are:

BACKGROUND

- BORN's status under the *Personal Health Information Protection Act, 2004*
- Privacy and Security Governance at BORN

YEAR IN REVIEW

Training and Awareness

- Privacy and security training for staff

Data Sharing

- Data collections and health information custodians from whom the data are collected
- Data uses and disclosures
- Data Sharing Agreements and Research Agreements

Audits and Compliance

- Privacy impact assessments, privacy and security audits and threat risk assessments, their recommendations, and the status of their implementation

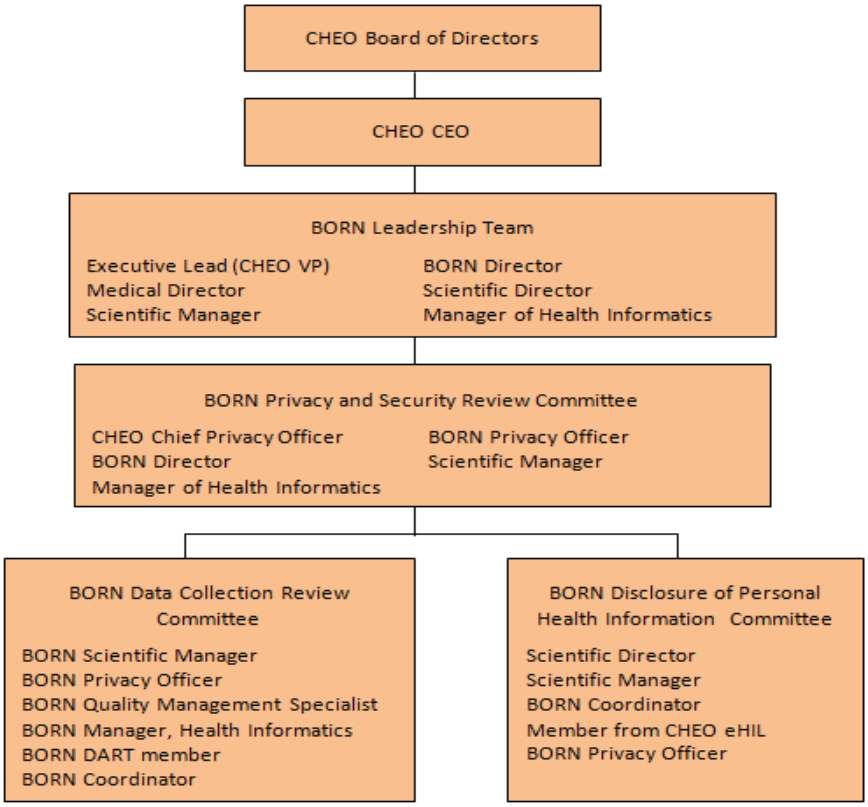
Incident Management

- Privacy inquiries and complaints and their resolution
- Privacy and security breaches, if any, related recommendations and the status of their implementation.
- Any other privacy and security related issues, as applicable

Review of Privacy and Security Policies

- Annual review of privacy and security policies, recommendations and status of implementation
- Changes to website and communications materials
- Review by the Information and Privacy Commissioner, recommendations and their status, as applicable

The BORN policy on **Privacy and Security Governance and Accountability Framework** includes a privacy and security governance organization chart:



As set out in the policy, the Privacy Officer ensures that the BORN Ontario privacy and security accountability framework, including security and privacy governance structure are:

- Updated in the BORN Ontario Privacy and Security Management Plan
- Included in BORN Ontario privacy and security training that is provided by the Privacy Officer or designate

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

BORN has established three committees in respect of the privacy and security program as follows:

1. Privacy and Security Review Committee
2. Data Collection and Review Committee
3. Disclosure of PHI Review Committee

The BORN policy **O-03 Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program** establishes terms of reference for all three BORN committees. Each of the BORN committee Terms of Reference include:

- Membership, including chair person, and reporting structure
- Mandate and responsibilities or tasks of the committee
- Meeting frequency
- Minutes and where they are stored

4.3 Corporate Risk Management Framework

BORN has developed and implemented a comprehensive policy on **Corporate Risk Management Framework** to identify, assess, mitigate and monitor risks, including risks that may negatively affect

BORN's ability to protect the privacy of individuals whose personal health information is received, and to maintain the confidentiality of that information.

The BORN policy on **Corporate Risk Management Framework** states that risk management is the responsibility of the Privacy and Security Review Committee and that the Privacy Officer is the agent who undertakes the process of identifying risks related to BORN's ability to protect the privacy and confidentiality of the personal health information in the custody and control of BORN. The process followed by the Privacy Officer in identifying these risks is clearly described in the procedure and includes:

- Reviewing security audit reports, including threat risk assessments, vulnerability assessments, penetration assessments
- Reviewing privacy audit reports, privacy impact assessments, reports on breach incidents and complaints
- Consulting with the Manager of Health Informatics, the BORN System Hosting Provider, the Scientific Manager and other agents and stakeholders, as appropriate.

As per the policy, the Privacy Officer completes and securely maintains the Corporate Risk Register to manage risks and works closely with the Manager of Health Informatics and subject matter experts as appropriate in identifying risks and strategies to address the risks (risk reduction, risk avoidance, risk coping). The Privacy Officer forwards the Corporate Risk Register/plan to BORN Leadership Team for their review and approval. The content of the register includes:

- What is the risk?
    - Risk #
    - Risk Description
    - Identified By
- How important is this risk and why (assign and justify a ranking)?
    - Risk Likelihood (A) (1-10)
    - Risk Severity (B) (1-10)
    - Risk Impact (A*B)
- How will this risk be addressed? Select one and describe response. Where risk is to be mitigated, record risk grade as per Recommended Actions for Grades of Risk.
    - Avoid, Mitigate, Transfer, Accept
    - Response Description
- Date Mitigation Strategy Will be Implemented
- Date Mitigation Strategy was Implemented
- Agent Assigned to Mitigation Strategy
    - Frequency with which agent will report risk status to Privacy Officer
- When will this risk be monitored by Privacy Officer?
    - Define frequency of monitoring and next monitoring date.

The policy identifies that the Privacy Officer manages the process to assess risks according to documented criteria for ranking, which includes probability of occurrence and impact on ability to maintain the security of records of personal health information should a risk occur. The Privacy Officer works closely with the Manager of Health Informatics on this exercise and documents the exercise in the Corporate Risk Register.

As per the policy, each risk is assigned a mitigation grade with an associated risk mitigation strategy as per the defined Recommended Actions for Grades of Risk in the policy. These results are documented and tracked in the Corporate Risk Register, which also identifies the agent assigned to each risk mitigation strategy as well as monitoring timelines for each risk.

The risk management Corporate Risk Register is a standing item on monthly BORN Leadership Team meetings. It is maintained and monitored by the Privacy Officer, where monitoring timelines are documented in the register (per risk). Written approval of the Corporate Risk Register is given by the Leadership Team to the Privacy Officer on an annual basis. The BORN Leadership Team includes the BORN Director and the BORN Executive Lead.

The risk management framework is incorporated into BORN policies and procedures via the completion, management and monitoring of the BORN Corporate Risk Register. The BORN policy on **Corporate Risk Management** also includes a provision for the Privacy Officer and project managers to work together on new projects to ensure risk management is identified on a per project basis.

4.4 Corporate Risk Register

BORN has in place **O-05: Corporate Risk Register** to identify each risk that may negatively affect BORN's ability to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. For each risk identified, the corporate risk register captures the following elements:

- What is the risk?
    - Risk #
    - Risk Description
    - Identified By
- How important is this risk and why (assign and justify a ranking)?
    - Risk Likelihood (A) (1-10)
    - Risk Severity (B) (1-10)
    - Risk Impact (A*B)
- How will this risk be addressed? Select one and describe response. Where risk is to be mitigated, record risk grade as per Recommended Actions for Grades of Risk.
    - Avoid, Mitigate, Transfer, Accept
    - Response Description
- Date Mitigation Strategy Will be Implemented
- Date Mitigation Strategy was Implemented
- Agent Assigned to Mitigation Strategy
    - Frequency with which agent will report risk status to Privacy Officer
- When will this risk be monitored by Privacy Officer?
    - Define frequency of monitoring and next monitoring date.

4.5 Policy and Procedures for Maintaining a Consolidated Log of Recommendations

BORN policy **O-06 Maintaining a Consolidated Log of Recommendations** is in place to capture all privacy and security related recommendations arising from:

- Privacy impact assessments
- Privacy audits
- Security audits
- Investigation of privacy and security breaches and privacy complaints

- Investigation of privacy and security issues raised by BORN staff
- Recommendations made by the Information and Privacy Commissioner of Ontario

As per the policy, the Privacy Officer is responsible for the creation and maintenance of the **Consolidated Log of Recommendations** and inputs all recommendations into the log within a week of recommendations being received. They are reviewed by the Privacy Officer on an ongoing basis, but at a minimum they are reviewed monthly to ensure that all recommendations are addressed in a timely manner.

The policy indicates that BORN agents must comply with the policy and procedures and that compliance is audited on an ongoing basis by the Privacy Officer in accordance with policy **P-27: Privacy Audits** and policy **S-15: Security Audits** as appropriate. In addition the policy states that if an agent breaches or believes there may have been a breach of this policy or procedures, the agent must notify the Privacy Officer at the first reasonable opportunity, as per policy **P-29: Privacy Breach Management** or policy **S-17: Security Breach Management** as appropriate.

4.6 Consolidated Log of Recommendations

BORN maintains a consolidated and centralized log of recommendations, as per **O-07: Consolidated Log of Recommendation** for all recommendations arising from privacy impact assessments, privacy audits, security audits, investigation of privacy and security breaches and privacy complaints, investigation of privacy and security issues raised by BORN staff, and recommendations by the Information and Privacy Commissioner of Ontario.

The log captures the following elements:

- Recommendation
- Name and date of document, investigation, audit, review
- Manner in which the recommendation is to be addressed
- Responsible agent
- Proposed completion date
- Actual completion date
- Comments

4.7 Business Continuity and Disaster Recovery Plan

BORN is working with CHEO and the BORN System Hosting Provider to develop a robust business continuity and disaster recovery plan that provides effective prevention and recovery procedures in the event of an incident.
A draft of the CHEO disaster recovery plan has been prepared and includes all aspects of disaster recovery, including:

- Data Centre protections
- Cooling System
- Power Distribution
- Fire/Smoke detection and suppression
- Full description of all hardware, including phone systems
- Contact list and communication protocol
- Assessment and containment phases
- Full shutdown and recovery steps

In addition to the continued work on a complete, documented business continuity and disaster recovery plan, **BORN policy S-13 Back-up and Recovery of Records of Personal Health Information**, which provides systematic back-up of personal health information in the custody of BORN, is operational. Back-up tapes are collected nightly and stored in fire-proof rooms. The backup tapes undergo a monthly recovery test.

The BORN policy on Business Continuity and Disaster Recovery is scheduled for completion in June 2015.

IV. Appendix "C": Privacy, Security and Other Indicators

As per the Information and Privacy Commissioner of Ontario process on the Three-Year Review of Prescribed Persons and Prescribed Entities, this written report must report on, provide information concerning and assess the performance of the prescribed person or prescribed entity with respect to each of the privacy, security and other indicators set out in Appendix "C" to the Manual for the Review and Approval of Prescribed Persons or Prescribed Entities.

This chapter provides the required information with respect to Appendix "C".

Part 1: Privacy Indicators

General Privacy Policies, Procedures and Practices

Indicator:
The dates that the privacy policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.

BORN Response:
BORN practices and procedures are documented in the BORN Privacy and Security Management Plan which contains all BORN policies and procedures with respect to:

- Privacy
- Security
- Human Resources
- Organizational and Other

The BORN Privacy and Security Management Plan received initial approval from the IPC in August and October, 2011. The BORN system (called the BORN Information System, or the "BIS") was fully launched in April 2012 and the first review of all policies and procedures was planned for the following year, with an actual start date of July 2013. The review was conducted in two parts:

1. July 2013 – September 2013:
   All policies and procedures reviewed by subject matter experts as per requirements in BORN policy **P-02: Ongoing Review of Privacy and Security Policies and Procedures**. This review served two purposes:
   i. Annual review
   ii. Implementation check – how well had policies and procedures been put into operation and were they working as planned? BORN policies and procedures were written and approved prior to the actual launch of the BORN Information System and it was expected that the first review of policies and procedures would result in updates to ensure alignment between work flow and procedures. This implementation check was broken off into a second more in-depth review as described in the next bullet (#2).
2. Summer 2013 – on-going (completion date and new version of Privacy and Security Management Plan due December 2014)
   This second very in-depth review has three goals:
   i. Ensure all policies are fully implemented
   ii. Work with BORN agents to ensure that the policies most applicable to their role are clear and efficient and that the policies and procedures as written and approved prior to

the actual launch of the BORN Information System are updated if necessary to align with workflow.

iii. Ensure all policy and procedure updates maintain compliance to IPC requirements as set out in Appendix "A" of the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities

During the course of this on-going review, BORN has been approving policy and procedure updates on an ad-hoc basis (enabling the deployment of individual policies as changes are made). A formal review and approval capturing all updates from ad-hoc updates is planned for December 2014.

Indicator:
Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.

BORN Response:
The following is a list of privacy policy updates undertaken and on-going as a result of the annual review:

- P-02 and S-02: Ongoing Review of Privacy and Security Policies and Procedures Updated to reflect final approval of policy changes:
    - Final approval lies with Privacy and Security Review Committee rather than Leadership Team. Leadership Team participates in review and has full input.
- P-04: Collection of Personal Health Information and P-06 Statements of Purpose for Data Holdings Containing Personal Health Information:
    - Minor updates to reflect flow of approvals and documentation.
- P-05: List of Data Holdings Containing Personal Health Information:
    - Updated the list of data holdings to reflect the founding member datasets that contributed to the BORN System and are now held as legacy datasets.
    - Updated the list of unique data collections provided by various health information custodians to include the antenatal record and fertility data.
- P-08: Limiting Agent Access to and Use of Personal Health Information:
    - Updated to remove approval by the Privacy and Security Review Committee for each BORN agent's access to PHI. Approval lies in dual approval from agent's supervisor and the Privacy Officer.
    - Updated P-08A Agent Data Access Form to better reflect the way access to the BORN System is enabled.
- P-09: Log of Agents Granted Approval to Access and Use Personal Health Information:
    - Added two new columns at the request of the privacy officer: "date access terminated" and "reason access terminated".
- P-10: Use of Personal Health Information for Research Purposes:
    - Updated policy to reflect current de-identification practices and approval process, introduction of delegated duties, updated procedure for provision of data and transfer of data.
- P-10E: Data Request Review Process:
    - Under current review to update use of de-identification tool and corresponding risk thresholds based on improvements to the tool.
- P-12: Disclosure of Personal Health Information for Purposes Other Than Research:

    - Updated procedure to add clarity with respect to data sharing agreements, introduction of delegated duties, updated use of de-identification tool, provision and transfer of data.
- P-13: Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements:
    - Updated procedure to add clarity with respect to use of de-identification tool, introduction of delegated duties, provision and transfer of data, tracking of refusals.
- P-16: Data Sharing Agreements:
    - Updated to include privacy coordinator's role in preparation and execution of data sharing agreements.
- P-17A: Template Data Sharing Agreement: Collection of Personal Health Information:
    - Collection data sharing agreement updated as a result of legal review to improve clarity.
- P-22: Linkage of Records of Personal Health Information:
    - Under current review to ensure all types of data linkages are addressed.

The following is a list of other policy updates of note that were undertaken as a result of the annual review:

- O-01 and O-02: Privacy and Security Governance and Accountability Framework:
    - Updated Privacy and Security Governance to reflect correct membership on four committees.
- O-03: Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program:
    - Updated the Terms of Reference for the Data Collection Review Committee.
    - Updated terms of reference for the Privacy and Security Review Committee.
- HR-10: Termination or Cessation of the Employment or Contractual Relationship:
    - Updated to indicate immediate removal of PHI access privileges for employees terminated with cause and immediate recovery of sensitive assets.

Indicator:
Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.

BORN response:
No new policies and/or procedures have been identified.

Indicator:
The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.

BORN Response:
The BORN Ontario Privacy and Security Management Plan, which includes all privacy policies and procedures, will be updated and communicated by e-mail to all BORN agents within one month of final approval of the current review. The e-mail will include:

- The new version of the BORN Ontario Privacy and Security Management Plan.
- A summary of the changes to policies and procedures.

- A request that all agents read the new BORN Ontario Privacy and Security Management Plan and acknowledge this by e-mail to the Privacy Officer when complete.

Webinars or in-person training sessions will be conducted by the Privacy Officer if need is identified.

Annual privacy training is scheduled for May 2014 and an update on the status of all policies will be part of this training exercise.

Indicator:
Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.

BORN Response:
An updated version of the BORN Ontario Privacy and Security Management Plan, which includes all privacy policies and procedures, will be published to the BORN Ontario website within one month of its final approval.

Collection

Indicator:
The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.

BORN Response:
Six (6) data holdings containing personal health information as per BORN policy **P-05: List of Data Holdings Containing Personal Health Information**.

Indicator:
The number of statements of purpose developed for data holdings containing personal health information.

BORN Response:
Six (6) statements of purpose developed for data holdings containing personal health information, as per BORN policy **P-07: Evidence: Statements of Purpose for Data Holdings Containing Personal Health Information.**
These are existing statements of purpose and have not been amended since BORN received registry status in 2011.

Indicator:
The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
Six (6) statements of purpose for data holdings containing personal health information were reviewed on October 15, 2013, labeled A-F as per BORN policy ***P*-07: Evidence: Statements of Purpose for Data Holdings Containing Personal Health Information.**

Indicator:

Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made.

***BORN Response**:*
No amendments made to statements of purpose.

Use

Indicator:
The number of agents granted approval to access and use personal health information for purposes other than research.

BORN Response:
61 agents have approval to access and use personal health information for purposes other than research, as of October 25, 2013.

Indicator:
The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
22 requests received.

Indicator:
The number of requests for the use of personal health information for research purposes that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
22 requests granted; 0 denied.

Disclosure

Indicator:
The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
30 requests received:

- 29 requests from Public Health Units in Ontario
- One (1) request from Public Health Ontario (PHO)

Indicator:
The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:

BORN interprets “granted” to mean that the request has been analysed and approved by BORN. It does not mean that a data sharing agreement has been executed or that the data has been released.

- 26 requests granted:
    - 25 requests from Public Health Units
    - One (1) request from Public Health Ontario
- 0 requests denied:
    - Three (3) requests from Public Health Units being clarified prior to being granted.

Indicator:
The number of requests received for the disclosure of personal health information for research purposes since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
Four (4) requests received.

Indicator:
The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
BORN interprets “granted” to mean that the request has been analysed and approved by BORN. It does not mean that a data sharing agreement has been executed or that the data has been released yet.

- Four (4) requests granted.
- No requests denied.

Indicator:
The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
Two (2) research agreements executed.
Two (2) research agreements pending.

Indicator:
The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
218 requests received.

Indicator:
The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:

Five (5) agreements executed. These agreements were executed for de-identified record level datasets. BORN *does* receive acknowledgement for aggregate disclosures but these have not been tracked. Moving forward, BORN will track acknowledgement of receipt of aggregate data in BORN log **P-11A: Data Tracking Log** as per BORN policy **P-12: Disclosure of Personal Health Information for Purposes Other Than Research**.

Data Sharing Agreements

Indicator:
The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.

BORN response:
220 collection data sharing agreements executed.

Indicator:
The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
10 disclosure data sharing agreements executed.

Agreements with Third-Party Service Providers

Indicator:
The number of agreements executed with third-party service providers with access to personal health information since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
One (1) third-party service provider agreement executed.

Data Linkage

Indicator:
The number and a list of data linkages of PHI approved since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
11 data linkages approved as follows:

1. BORN-CIHI: Proposal for Enhanced Congenital Anomalies Surveillance in Ontario
2. BORN-ICES: Infant outcomes in the first year of life associated with maternal H1N1 vaccination
3. BORN-ICES: Predicting Future Health Status Based on Newborn Screening Metabolites levels and other markers of perinatal health in the general population and in vulnerable subgroups of children born in Ontario
4. BORN-ICES: The effect of H1N1 pandemic influenza illness and vaccination on pregnancy outcomes
5. BORN-ST.MICHAEL'S HOSPITAL: H1N1 vaccine in pregnancy: a registry for the fall and winter of 2009

6. BORN-CNN (Canadian Neonatal Network): A study to evaluate the outcomes of preterm infants between 30 weeks and 31 weeks' gestation receiving care in Level III vs Level IIc NICUs
7. BORN-CIHI: To determine if the benefits of scheduling planned repeat caesarean deliveries (PRCD) at or after 39 weeks outweigh the risks of such scheduling practices in terms of adverse maternal and neonatal health outcomes
8. BORN-ICES: Exploring variations in prenatal screening services in Ontario
9. BORN-CIHI: Evaluation of MOREOB Program Implementation in Ontario Hospitals
10. BORN-CIHI: Infant mortality
11. BORN-NSO: Evaluation of missed screens that were not caught by a BORN System alert

Privacy Impact Assessment

Indicator:
The number and a list of privacy impact assessments completed since the prior review by the Information and Privacy Commissioner of Ontario and for each privacy impact assessment:

- The data holding, information system, technology or program,
- The date of completion of the privacy impact assessment,
- A brief description of each recommendation,
- The date each recommendation was addressed or is proposed to be addressed, and
- The manner in which each recommendation was addressed or is proposed to be addressed.

BORN Response:
One (1) privacy impact assessments was completed, as follows:

- June 2012 "Delta" PIA

Data holding, information system, technology or program included:

- Personal health information that is stored within BORN components to be located at CHEO.
- Personal health information that is transmitted between BORN member database partners and BORN components located at CHEO and eHO.
- Security related and other sensitive information that is stored within BORN components.
- Dependent technology and services used by BORN to store or transmit PHI or other sensitive information.
- Delta PIA:
  - Enhancements to the Midwifery Invoicing System to enable payment for midwifery services by the Ontario Ministry of Health and Long Term Care.
  - Enhancements to enable batch uploading of the antenatal records from physician EMRs.
  - Enhancements to enable inclusion of Assisted Reproductive Technology data in BORN.

Date of Completion:
June 29, 2012

A brief description of each recommendation, the date each recommendation was addressed or is proposed to be addressed and the manner in which each recommendation was addressed or is proposed to be addressed:
See BORN Privacy Impact Assessment Log on page 122.

Indicator:

The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion.

BORN Response:
One (1) privacy impact assessment undertaken but not completed (yet). Completion date scheduled for March 2014. This privacy impact assessment is being conducted by a third party to address a group of initiatives and projects at BORN. The scope includes:

- Collection, or changes to the collection, of personal health information related to Ontario's 18-month well-baby visit, autism, fertility, and midwifery care
- Protocol to assist with follow-up test reminders for women who developed gestational diabetes
- Secure messaging system within the BORN Information System to assist hospitals, midwifery practice groups, etc safely communicate with BORN agents regarding their data
- Relevant portions of the BORN privacy program and privacy safeguards

Indicator:
The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion.

BORN Response:
No privacy impact assessments "not undertaken".

Indicator:
The number of determinations made since the prior review by the Information and Privacy Commissioner of Ontario that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.

BORN Response:
BORN has not undertaken any new data collections without a privacy impact assessment.

Indicator:
The number and a list of privacy impact assessments reviewed since the prior review by the Information and Privacy Commissioner and a brief description of any amendments made.

BORN Response:
Two (2) privacy impact assessments reviewed as follows:

1. June 2012 "Delta" PIA reviewed and all recommendations addressed with a plan for resolution, as per detailed response to first Privacy Impact Assessment indicator in this section, above.
2. Privacy Impact Assessment of BORN Congenital Anomalies Surveillance System (CASS) Assessment for Champlain LHIN (September, 2011) reviewed to ensure no amendments left outstanding. No further amendments made.

Privacy Audit Program

Indicator:
The dates of audits of agents granted approval to access and use personal health information since the prior review by the Information and Privacy Commissioner of Ontario and for each audit conducted:

- A brief description of each recommendation made,

- The date each recommendation was addressed or is proposed to be addressed, and
- The manner in which each recommendation was addressed or is proposed to be addressed.

BORN Response:
BORN performed a series of audits of agents granted approval to access and use personal health information as summarized here:

- BORN agents granted approval to access personal health information must have in place an Agent Data Access form signed by their manager as well as the Privacy Officer. When access is enabled, it is captured on a log (log **P-09: log of Agents Granted Approval to Access/Use/Disclose Personal Health Information)**. The audit cross checked the individual hard copy BORN Agent Data Access forms and the log of Agents Granted Approval to Access/Use/Disclose Personal Health Information to ensure alignment.
- Verify with all BORN agents that computers are equipped with an automated password-protected screen saver after a 15-minute time-out.
- Re-acknowledgement from each BORN Agent to the BORN Confidentiality Agreement as well as BORN privacy policies and procedures (via e-mail).
- Series of combined privacy and security audits to review audit logs for several BORN agents to verify:
    - What a user changed during a period of time
    - What a particular user accessed within the system during a period of time.

  These audits were performed to ensure no inappropriate access to personal health information by a BORN agent occurred. Audits were performed by the Privacy Officer and Senior Technical Architect (together). The audit consisted of a review of user activity across a period of time (ranging from two weeks to four months of activity) and involved the review of hundreds of logs. Details on these specifics combined privacy and security audits can be found in BORN Privacy Audit Program on page 125 where reviews of system control and audit logs are recorded as Audit # 14 (14.1, 14.2, 14.3 inclusive).
- First annual audit of level of BORN Agent access to personal health information performed by providing to each applicable manager a list of employees/agents and their associated access to personal health information to ensure access needs are correct and up-to-date.
- First annual audit of all BORN agents to acknowledge the following with respect to personal health information:
  1. No personal health information on desks in paper format
  2. No personal health information on portable devices, i.e. USB keys, CDs, DVDs
  3. All computers are encrypted

These audits occurred on the following dates: October 27, 2013, October 27, 2013, October 28, 2013, February 19, 2014 and February 20, 2014. Details can be found in BORN Privacy Audit Program beginning on page 125 where the six audits of agents granted approval to access and use personal health information are:

1. Audit # 2
2. Audit # 6
3. Audit # 13
4. Audit # 14 (14.1, 14.2, 14.3)
5. Audit # 17
6. Audit # 18

These formal privacy audits mark the start of the BORN audit program as there were no audits planned in 2012, the first year the BORN system was launched. Auditing will continue on an annual basis as per BORN policy **P- 27: Privacy Audits**.

Indicator:
The number and a list of all other privacy audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:

- A description of the nature and type of audit conducted,
- The date of completion of the audit,
- A brief description of each recommendation made,
- The date each recommendation was addressed or is proposed to be addressed, and
- The manner in which each recommendation was addressed or is proposed to be addressed.

BORN Response:
See BORN Privacy Audit Program beginning on page 125 which provides details on the following 12 audit activities, where one audit activity may contain many individual audits (for example, audit activities 7 and 8 each involved the audit of 71 individual data sharing agreements):

1. Audit # 1
2. Audit # 3
3. Audit # 4
4. Audit # 7
5. Audit # 8
6. Audit # 9
7. Audit # 10
8. Audit # 11
9. Audit # 12
10. Audit # 15
11. Audit # 16
12. Audit # 19

Privacy Breaches

Indicator:
The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
One (1) confirmed breach; zero (0) suspected breaches

Indicators and BORN Responses:
The date that the notification was received:
E-mail notification of breach received by BORN agent at 2:25 pm on Thursday, November 29, 2012.

The extent of the privacy breach or suspected privacy breach:
Organizations (health information custodians) disclose data (personal health information) to BORN pursuant to collection data sharing agreements between each organization and BORN by entering data into the BORN system. These organizations can then review their own data in various reports in the

BORN System. A BORN system user at one such organization ran a report and recognized that the report was displaying data for other organizations rather than filtering and displaying data only for the organization under which the user was logged in.

This occurred when a filter in the reporting system had been inadvertently removed. This filter, when in place and working correctly, ensures a report provides details only for the organization associated with the logged-in user, and not for any other organization.

The filter had been mistakenly disabled during testing of a new feature in the report. It was disabled for a total of 16 days, during which time the report was run by 22 individual users at 22 organizations, as recorded in BORN audit logs. Five of these users were BORN agents. The remaining 17 users were contacted by the BORN Privacy Officer and interviewed by telephone, as per details in the next indicator (notification). It was determined that this breach was limited to the person who notified BORN of the issue.

Whether it was internal or external.
External (reported by an external user).

The nature and extent of personal health information at issue:
The report contains the following fields of personal health information:

- OHIP #
- Last name, first name
- Estimated date of birth
- Pregnancy outcome
- Number of fetuses
- Birth date
- Birth location type
- Hospital name

The user who reported the issue to BORN had retrieved 2600 client records in her report. She did not save, print or read this report, other than to notice that it contained data for other practice groups, at which point she closed the report and notified BORN. BORN determined the number of records retrieved in the report based on reproducing the user's activity. While the user who reported the breach did not actually read any of the personal health information in the report, BORN determined that classifying the incident as a privacy breach and following BORN breach protocol was the most prudent course of action.

The date that senior management was notified:
BORN Director notified at 8:59 am on November 30, 2012.

The containment measures implemented:
There were three containment components to this privacy breach:

1. **Containment 1**: BORN System Administrator removed all access to the suspect report to ensure no user or organization could run the report.
2. **Containment 2**: As a result of determining that the breach was caused when a new feature was being introduced into this report, BORN pulled offline 10 other reports that had undergone any type of system change within a two-month timeframe to conduct a full permissions review.

This was communicated internally to BORN users by the Manager of Health Informatics by e-mail.

3. **Containment 3**: BORN Privacy Officer verified with the user who reported the incident that no copy of the report was saved or printed and that the user did not read/recall/take on board any personal health information.
4. **Containment 4**: BORN Privacy Officer followed up with all 16 other users who ran the report in the timeframe that it may have displayed inappropriate personal health information, to ensure no records were viewed, saved, printed or otherwise compromised.
   Phone conversations with these users revealed:
   - Four users experienced system problems and had been unable to run the report properly.
   - Nine users ran the report and did not notice anything unusual. All users had had recent BORN training on this particular report and had been testing it out of curiosity, rather than for any reconciliation purposes. None of the users saved and/or printed the report.
   - One user recalled running the report and viewing the name of another organization; she shut the report and thought nothing of it.
   - One user was never reached. BORN Privacy Officer called three times and left a message on the third try. User did not call back.
   - One user said the report ran properly – displayed information for her practice group only.

   The BORN Privacy Officer asked, in each interview, if each user knew what to do in the event of any irregular data or suspected breach. Without exception they all knew to call either the BORN Help Desk or their BORN Coordinator.

The date(s) that the containment measures were implemented:

1. **Containment 1**: November 30, 2012 at 8:49 am.
2. **Containment 2**: November 30, 2012 at 2:00 pm.
3. **Containment 3**: December 4, 2012.
4. **Containment 4**: phone calls made to 16 organizations from December 6 – 12, 2012.

The date(s) that notification was provided to the health information custodians or any other organizations:

The health information custodians (organizations) who ran the suspect report were all followed up with by the BORN Privacy Officer during the course of notification, as described in **Containment 4** in the previous indicator. No other notification was provided to health information custodians. BORN breach protocol indicates that where personal health information is accessed by unauthorized persons, the BORN Privacy Officer sends written notification to the health information custodians or organizations who provided the information at the first reasonable opportunity in order that they may notify individuals whose privacy was breached. Based on conversations between the Privacy Officer and the organizations that ran or attempted to run the report during the time it was compromised, the users/organizations that ran the report were unable to recall the names of other organizations that appeared on the report and had not looked at any individual names and no copies of the report were downloaded. BORN determined that no further notification was necessary.

The date that the investigation was commenced:

The investigation commenced November 30, 2012.

The date that the investigation was completed:

The investigation was completed on December 12, 2012.

A brief description of each recommendation made:
One recommendation resulted from the investigation into this security breach:

- **Recommendation 1**: provide a more robust test environment so that new features and system enhancements can undergo testing in a sufficiently robust environment.

The date each recommendation was addressed or is proposed to be addressed:

- **Recommendation 1** was addressed on May 10, 2013.
  The recommendation was addressed in the following manner:
  BORN launched a "staging" environment which provides a robust test environment for all new features and enhancements.

Privacy Complaints

Indicator:
The number of privacy complaints received since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
No complaints received.

Indicator:
Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint investigated:

- The date that the privacy complaint was received,
- The nature of the privacy complaint,
- The date that the investigation was commenced,
- The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation,
- The date that the investigation was completed,
- A brief description of each recommendation made,
- The date each recommendation was addressed or is proposed to be addressed,
- The manner in which each recommendation was addressed or is proposed to be addressed, and
- The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.

***BORN Response*:**
No complaints received.

Indicator:
Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint not investigated:

- The date that the privacy complaint was received,
- The nature of the privacy complaint, and
- The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.

BORN Response:
No complaints received.

Part 2: Security Indicators

General Security Policies and Procedures

Indicator:
The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.

BORN Response:

BORN practices and procedures are documented in the BORN Privacy and Security Management Plan that contains all BORN policies and procedures with respect to:

- Privacy
- Security
- Human Resources
- Organizational and Other

The BORN Privacy and Security Management Plan received initial approval from the IPC in August and October, 2011. The BORN system (called the BORN Information System, or the "BIS") was fully launched in April 2012 and the first review of all policies and procedures was planned for the following year, with an actual start date of July 2013. The review was conducted in two parts:

3. July 2013 – September 2013:
   All policies and procedures reviewed by subject matter experts as per requirements in BORN policy **P-02: Ongoing Review of Privacy and Security Policies and Procedures**. This review served two purposes:
   iii. Annual review
   iv. Implementation check – how well had policies and procedures been put into operation and were they working as planned? BORN policies and procedures were written and approved prior to the actual launch of the BORN Information System and it was expected that the first review of policies and procedures would result in updates to ensure alignment between work flow and procedures. This implementation check was broken off into a second more in-depth review as described in the next bullet (#2).
4. Summer 2013 – on-going (completion date and new version of Privacy and Security Management Plan due December 2014)
   This second very in-depth review has three goals:
   iv. Ensure all policies are fully implemented
   v. Work with BORN agents to ensure that the policies most applicable to their role are clear and efficient and that the policies and procedures as written and approved prior to the actual launch of the BORN Information System are updated if necessary to align with workflow.
   vi. Ensure all policy and procedure updates maintain compliance to IPC requirements as set out in Appendix "A" of the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities

During the course of this on-going review, BORN has been approving policy and procedure updates on an ad-hoc basis (enabling the deployment of individual policies as changes are made). A formal review and approval capturing all updates from ad-hoc updates is planned for December 2014.

Indicator:
Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.

BORN Response:
The following is a list of security policy updates undertaken and on-going as a result of the annual review:

- S-03: Ensuring Physical Security of Personal Health Information:
    - Updated the levels of access to the main data centre from three to four and described fourth.
- S-07: Secure Transfer of Records of Personal Health Information:
    - Updated to reflect current practice of transferring data out via secure FTP (not encrypted CD via bonded courier).
    - Updated to address PIA recommendation re secure destruction (where secure destruction is directed in the applicable data sharing agreement or research agreement).
- S-09: Passwords:
    - Updated the minimum password length from eight characters to six characters, which correctly reflects the BORN System.
- S-12: Change Management:
    - Under current review to ensure more rigorous process in place which involves committee approval is accurately reflected.
- S-13: Back-up and Recovery of Records of Personal Health Information:
    - Updated frequency of recovery testing of backup tapes; testing occurs monthly rather than quarterly.

Indicator: Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.

BORN Response:
No new policies and/or procedure have been identified.

Indicator:
The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.

BORN Response:

The BORN Ontario Privacy and Security Management Plan, which includes all security policies and procedures, will be updated and communicated by e-mail to all BORN agents within one month of final approval of the current review. The e-mail will include:

- The new version of the BORN Ontario Privacy and Security Management Plan.
- A summary of the changes to policies and procedures.
- A request that all agents read the new BORN Ontario Privacy and Security Management Plan and acknowledge this by e-mail to the Privacy Officer when complete.

Webinars or in-person training sessions will be conducted by the Privacy Officer and/or Senior Systems Architect and/or Manager of Health Informatics if need is identified.

Annual security training is scheduled for May 2014 and an update on the status of all policies will be part of this training exercise.

Indicator:
Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.

BORN Response:
An updated version of the BORN Ontario Privacy and Security Management Plan, which includes all security policies and procedures, will be published to the BORN Ontario website within one month of its final approval.

Physical Security

Indicator:
The dates of audits of agents granted approval to access the premises and locations within the premises where records of personal health information are retained since the prior review by the Information and Privacy Commissioner and for each audit:

BORN Response:
Audit date and scope: Friday, October 25, 2013.

Agent audited: BORN System Hosting Provider, who, for clarity, is an agent of BORN.
The BORN System Hosting Provider was audited to verify physical security parameters as per BORN policy **S-03: Ensuring Physical Security of Personal Health Information**. All personal health information in the custody of BORN Ontario is securely stored by the BORN System Hosting Provider and access to personal health information by BORN agents is exclusively via remote login to the infrastructure provided by the BORN System Hosting Provider.

In-person audit consisted of a site tour of the data centre and verification of all of the elements of physical security as per BORN policy **S-03: Ensuring Physical Security of Personal Health Information** following elements of physical security:

A brief description of each recommendation made:
Update the policy **S-03 Ensuring Physical Security of Personal Health Information** to note that there are four, not three, levels of access necessary in order to access physical servers as well as a security camera and a sign-in log.

The date each recommendation was addressed or is proposed to be addressed.
Addressed on October 28, 2013.

The manner in which each recommendation was addressed or is proposed to be addressed:
Updated policy **S-03: Ensuring Physical Security of Personal Health Information** which appears in v 1.9a of the BORN Ontario Privacy and Security Management Plan submitted with this report.

This audit is also documented as audit 10.5 (10.5.1, 10.5.2, 10.5.3, 10.5.4 inclusive) in the BORN Security Audit Program on page 132.

Security Audit Program

Indicator:
The dates of the review of system control and audit logs since the prior review by the Information and Privacy Commissioner of Ontario and a general description of the findings, if any, arising from the review of system control and audit logs.

BORN Response:
System control and audit logs were reviewed via a series of ad-hoc audits as part of a combined privacy and security audit to assess effectiveness of the BORN system logging capabilities. These audits serve to demonstrate to BORN that events are tracked as per system design (date and time personal health information accessed, date and time of disconnection, name of user accessing personal health information, creation, amendment, deletion or retrieval of records of personal health information, date and time of the action, and so on) and can demonstrate to BORN:

- What a user changed during a period of time
- The revision history for a patient over a period of time
- What a particular user accessed within the system during a period of time

BORN verified audit logs for a series of pregnancies captured in the BORN Information System and also thoroughly reviewed system control and audit logs for several BORN agents. The review of BORN agent system activity is performed on a single date, spans user activity across a period of time (ranging from two weeks to four months of activity), and involves the verification of hundreds of logs. All reviews were conducted by the BORN Privacy Officer and the BORN Senior Technical Architect (together) on the following dates: October 2, 2013, October 28, 2013, February 19, 2014. There were 12 individual reviews of logs across these three dates. Details can be found in BORN Security Audit Program on page 132 where reviews of system control and audit logs are recorded as

1. Audit # 1.1
2. Audit # 1.2
3. Audit # 1.3
4. Audit # 1.4
5. Audit # 1.5
6. Audit # 1.6
7. Audit # 1.7
8. Audit # 1.7a
9. Audit # 1.8
10. Audit # 1.9
11. Audit # 1.10
12. Audit # 3

There were no findings as a result of these reviews.

Of note, audit logs are often verified in the course of addressing BORN user queries. This may happen, for example, where a data entry clerk at an organization (where the organization enters records of personal health information into the BORN system) notices an error in a record or cannot find a record that was previously entered. The data entry clerk may contact BORN for help and a BORN System Administrator is able, in each case, to verify system control and audit logs and review with the user precisely what actions they performed in the BORN system and thus address the user questions. To date these audit log reviews have not been recorded. BORN will begin documenting these reviews in 2014.

Indicator:
The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:

- A description of the nature and type of audit conducted,
- The date of completion of the audit,
- A brief description of each recommendation made,
- The date that each recommendation was addressed or is proposed to be addressed, and
- The manner in which each recommendation was addressed or is expected to be addressed.

BORN Response:
See BORN Security Audit Program on page 132 where the following 14 security audits are detailed:

1. Audit # 2
2. Audit # 4.1
3. Audit # 5.2
4. Audit # 5.3
5. Audit # 5.5
6. Audit # 5.6
7. Audit # 6
8. Audit # 7
9. Audit # 8
10. Audit # 9
11. Audit # 10.1
12. Audit # 10.2
13. Audit # 10.3
14. Audit # 10.5 (10.5.1 – 10.5.4)

Information Security Breaches

Indicator:
The number of notifications of information security breaches or suspected information security breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
One (1) notification received
Indicators and BORN Responses:
With respect to each information security breach or suspected information security breach:
The date that the notification was received:
E-mail notification of breach received by BORN Coordinator at 10:47 pm Wednesday, October 3, 2012.

The extent of the information security breach or suspected information security breach:
The breach was discovered by a BORN system user who manages the BORN system at a particular organization (where the organization enters data into the BORN system pursuant to a collection data sharing agreement). The user observed that another BORN user at that organization was able to view certain invoice details that are appropriate only for senior staff at the organization. .

The breached view of the invoice was a screen capture – a snapshot – of the tabs of data available in this particular invoice. The view presented static data that could be not be manipulated or further accessed.

The most sensitive information on the invoice, and the focus of the breach and the breach investigation, was some administrative data that contained, for 16 health information custodians employed at this organization, several fields of information including first name, last name, and a number that maps to level of pay.

The nature and extent of personal health information at issue:
No personal health information was involved in this security breach.

The date that senior management was notified:
BORN Director notified October 5, 2012.

The containment measures implemented:
There are two containment components to this security breach:

1. **Containment 1** – Disable the user account that accessed the unauthorized view of the invoice:
    - Account disabled within 30 minutes of initial report (e-mail sent to BORN Coordinator @ 10:47 pm October 3, 2012 and user account disabled by BORN Coordinator @ 11:10 pm on October 3, 2012).
2. **Containment 2** – Ensure the problem is fixed and cannot be reproduced:
    - It was determined that the breach could be reproduced in three scenarios as per invoice vendor investigation and therefore needed more robust containment measures than disabling a user account, as described in Containment 1 above. The second containment measure was a patch introduced into the system by close of business on October 4th, 2012. This patch eliminated the problem completely – no longer reproducible.

The date(s) that the containment measures were implemented:

1. **Containment 1**: October 3, 2012
2. **Containment 2**: October 4, 2012.

The date(s) that notification was provided to the health information custodians or any other organizations:
Letters of notification were sent on November 9, 2012, from the BORN Director and BORN Privacy Officer, as follows:

- Personalized letters were sent to the 16 distinct health information custodians whose information was exposed in this incident. The letters highlighted:
    - A security (NO PHI) breach occurred and a small amount of information relating to their fee level was viewed by a practice administrator.

- BORN takes privacy seriously and took action immediately, including an investigation and recommendations.
- Contact BORN for more information.

The date that the investigation was commenced:
Investigation commenced October 5, 2012.

The date that the investigation was completed:
Early November 2012.

A brief description of each recommendation made.
The date each recommendation was addressed or is proposed to be addressed.
The manner in which each recommendation was addressed or is proposed to be addressed:

BORN Response:
Four recommendations resulted from the investigation into this security breach:

- **Recommendation 1**: Faster communication of breach to relevant community outside of BORN.
- **Recommendation 2**: Notify the Privacy Officer immediately of any suspected breach.
- **Recommendation 3**: Ensure reporting user (BORN local administrator at the organization that reported the breach) logs into the BORN Information System using only her own credentials.
- **Recommendation 4**: Be aware of the risk of inadvertently re-breaching or worsening a breach when reporting or investigating.

The recommendations were addressed on these dates:

- **Recommendation 1**: November 2012
- **Recommendation 2**: April 2013
- **Recommendation 3**: Addressed during breach investigation
- **Recommendation 4**: May 24, 2013

The recommendations were addressed in the following manner:

- **Recommendation 1**: Reviewed breach procedure to ensure notification is covered. Privacy Officer to consider earlier notification in any future breach.
- **Recommendation 2**: Reminder to all involved that immediate reporting is mandatory. Annual organizational privacy training on May 24, 2013 shared this reminder with all BORN employees (review of breach protocol).
- **Recommendation 3**: Reporting user reminded on October 3rd (in immediate response to breach by BORN) that she should not log in under any user other than herself, even to verify system settings, unless she is on the phone or beside the user and they are completing the verification together.
- **Recommendation 4**: Promote awareness, within BORN, of how easy it is to inadvertently worsen a breach when passing on information to report or investigate an incident. The ease with which this might be done accidentally was raised in the investigation of this breach. This was included in BORN annual privacy training on May 24, 2013.

Part 3: Human Resources Indicators

Privacy Training and Awareness

Indicator:
The number of agents who have received and who have not received initial privacy orientation since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:

- 82 agents have received initial privacy orientation. This number includes those agents who no longer work for BORN.
- All agents received privacy training; there are no agents awaiting privacy training.

Indicator:
The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation.

BORN Response:
No agents have yet to receive initial privacy training.

Indicator:
The number of agents who have attended and who have not attended ongoing privacy training each year since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
2012-2013 organizational privacy/security training:

There were 52 BORN agents in the 2012 – 2013 fiscal year.

- 30 agents attended organizational privacy/security training.
- 22 agents did not attend training. Of these 22 agents:
    - 8 agents joined BORN after date of annual training; all received initial privacy/security orientation.
    - 9 agents did not attend annual privacy/security training.
    - 5 agents are CHEO IS employees who are also BORN agents and who provide help desk services for the BORN system; CHEO IS employees attend mandatory CHEO privacy training every two years.

2013-2014 organizational privacy/security training:

There were 67 BORN agents in the 2013 – 2014 fiscal year.

- 39 agents attended organizational privacy/security training.
- 28 agents did not attend organizational privacy/security training. Of these 28 agents:
    - 16 agents joined BORN after the organizational training was delivered; all received initial privacy/security `orientation.
    - 7 agents did not attend annual privacy/security training.
    - 5 agents are CHEO IS employees who are also BORN agents and who provide help desk services for the BORN system; CHEO IS employees attend mandatory CHEO privacy training every two years.

BORN mandates annual organizational privacy and security training for all agents and notes the following with respect to ensuring that each agent receives this training every year:

- CHEO IS employees will be included in annual organizational training
- The BORN Privacy Officer will arrange a follow-up training session for all BORN agents who were unable to attend organizational privacy and security training which is delivered at a face-to-face team meeting each year

Indicator:
The dates and number of communications to agents by the prescribed person or prescribed entity in relation to privacy since the prior review by the Information and Privacy Commissioner of Ontario and a brief description of each communication.

BORN Response:
The following privacy and security communications have occurred:

1. May 24, 2013: Privacy Officer delivered organizational privacy and security training to all BORN employees during a two-day employee meeting. Training included a game of Privacy Jeopardy.
2. December 13, 2012: Privacy Officer e-mailed BORN Coordinators with guidance on how to safely work with hospital BORN users who need BORN help with data entry into patient records and may inadvertently e-mail sensitive data (chart ID, for example). Main guidelines were:
    a. BORN does not permit the e-mailing of personal health information.
    b. Where chart ID must be shared, save it in a password protected excel file.
    c. Always be aware of potential risk of re-identification.

    Yammer updates as follows (Yammer is a communication tool – like Facebook for the workplace – that is used internally by BORN):
3. October 17, 2012 Yammer update: Privacy Officer posted an update at privacy conference where privacy principles applicable to First Nations communities were mentioned.
4. July 23, 2013 Yammer update: Privacy Officer posts article about firing of six employees for snooping in the birth records of Kim Kardashian (famous socialite).
5. July 23, 2013 Yammer update: Privacy Officer posts reminder of privacy guideline when using the BORN Yammer tool:
    Keep in mind that Yammer is a social media tool and hacking is not an impossibility.
    - *Only post information or content that passes the "comfort test" – would you be comfortable if you knew one of our stakeholders read your post?*
    - *Be careful when naming people – use organization names where more appropriate (kudos to co-workers is of course a-ok!)*
    - *Never post confidential or inappropriate information.*
6. October 8, 2013 Yammer update: Privacy Officer posts article about a lost, unencrypted USB stick by Peel Public Health as a reminder of why BORN does not permit the storage of sensitive data on USB keys.
7. October 25, 2013 Yammer update: Privacy Officer posts a privacy and security audit update describing the audit of physical security of BORN PHI that verified each level of card access and the visitor sign-in log, as well as fire suppression. Update included photograph:

Security Training and Awareness

Indicator:
The number of agents who have received and who have not received initial security orientation since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:

- 82 agents have received initial security orientation. This number includes those agents who no longer work for BORN.
- All agents received security training; there are no agents awaiting security training.

Indicator:
The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation.

BORN Response:
No agents have yet to receive initial security training.

Indicator:
The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
2012-2013 organizational privacy/security training:

There were 52 BORN agents in the 2012 – 2013 fiscal year.

- 30 agents attended organizational privacy/security training.
- 22 agents did not attend training. Of these 22 agents:
    - 8 agents joined BORN after date of annual training; all received initial privacy/security orientation.
    - 9 agents did not attend annual privacy/security training.
    - 5 agents are CHEO IS employees who are also BORN agents and who provide help desk services for the BORN system; BORN is confirming the security training requirements for these agents.

2013-2014 organizational privacy/security training:

There were 67 BORN agents in the 2013 – 2014 fiscal year.

- 39 agents attended organizational privacy/security `training.
- 28 agents did not attend organizational privacy/security `training. Of these 28 agents:
    - 16 agents joined BORN after the organizational training was delivered; all received initial privacy/security `orientation.
    - 7 agents did not attend annual privacy/security training.
    - 5 agents are CHEO IS employees who are also BORN agents and who provide help desk services for the BORN system; BORN is confirming the security training requirements for these agents.

BORN mandates annual organizational privacy and security training for all agents and notes the following with respect to ensuring that each agent receives this training every year:

- CHEO IS employees will be included in annual organizational training
- The BORN Privacy Officer will arrange a follow-up training session for all BORN agents who were unable to attend organizational privacy and security training which is delivered at a face-to-face team meeting each year

Indicator:
The dates and number of communications to agents by the prescribed person or prescribed entity to agents in relation to information security since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
Please see the list of privacy and security communications provided as evidence to support the final indicator under Privacy Training and Awareness section.

Confidentiality Agreements

Indicator:
The number of agents who have executed and who have not executed Confidentiality Agreements each year since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
All agents execute an initial Confidentiality Agreement as part of their privacy and security orientation training. There is no access to personal health information at BORN without a signed Confidentiality Agreement.

The first re-acknowledgement of the BORN Confidentiality Agreement was done on October 27, 2013. Of the 67 BORN agents in this fiscal year:

- **45** agents re-acknowledged their commitment and understanding to the BORN Confidentiality Agreement.
- **2** agents were on maternity leave on this date.
- **5** agents left BORN before this date.
- **3** agents joined BORN after this date and signed Confidentiality Agreements as part of their initial privacy/security orientation.

- **6** agents joined BORN less than six months before this date and have current Confidentiality Agreements on file.
- **6** agents did not re-acknowledge. Of these 6, 3 do not have access to personal health information. All agents are expected to re-acknowledge.

This annual mandatory re-acknowledgement will be repeated every year, with 2013 marking the first time this annual audit was performed.

Indicator:
The date of commencement of the employment, contractual or other relationship for agents that have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.

BORN Response:
All agents have executed Confidentiality Agreements.

Termination or Cessation

Indicator:
The number of notifications received from agents since the prior review by the Information and Privacy Commissioner of Ontario related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.

BORN Response:
Three (3) termination notices have been received from full-time BORN agents who have terminated their employment with BORN Ontario.
16 contract employees have reached the end of their contract. No notices are received with respect to their termination as their end date is known prior to their start date.

Part 4: Organizational Indicators

Risk Management

Indicator:
The dates that the corporate risk register was reviewed by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
The BORN Privacy Officer, Manager of Health Informatics and Director will begin implementing formal risk assessment as per BORN policy **O-04: Corporate Risk Management Framework** March 25, 2014. Identified risks will be managed in the corporate risk register where they will be monitored. Risk assessment to be completed within three months of start date. Prior to this date, BORN has performed risk management informally.

Indicator:
Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.

BORN Response:

No amendments.

Business Continuity and Disaster Recovery

Indicator:
The dates that the business continuity and disaster recovery plan was tested since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
BORN Ontario is working with CHEO and the BORN System Hosting Provider to develop a robust business continuity and disaster recovery plan that provides effective prevention and recovery procedures in the event of an incident.
A draft of the CHEO disaster recovery plan has been prepared and includes all aspects of disaster recovery, including:

- Data Centre protections
- Cooling System
- Power Distribution
- Fire/Smoke detection and suppression
- Full description of all hardware, including phone systems
- Contact list and communication protocol
- Assessment and containment phases
- Full shutdown and recovery steps

In addition to the continue work on a complete, documented business continuity and disaster recovery plan, *BORN S-13 Back-up and Recovery of Records of Personal Health Information*, which provides systematic back-up of personal health information in the custody of BORN, is operational. Back-up tapes are collected nightly and stored in fire-proof rooms. The backup tapes undergo a monthly recovery test.

Indicator: Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.

BORN Response:
Status of new policy and procedure to be reflected in this indicator when BORN provides updates to this report in February, 2014.

Part 5: BORN Logs

BORN Privacy Impact Assessment Log

Recommendation	Manner in which the Recommendation is to be addressed	Actual Completion Date	Comments/Status
High priority RM1 – Update training strategy and program – Update training strategies and programs to include end-users who are not agents of BORN (e.g. staff in hospitals, MPGs) and expand program to include comprehensive security awareness training.	Updated as of Feb 27, 2014: 1) Extensive data entry training for end users is available on the BORN website. 2) Follow-up privacy and security training for BORN local administrators at external organizations (hospitals, mpgs) to be rolled out in June 2014. Training will emphasize privacy and security as it applies to the role and will be delivered by BORN Coordinators and subsequently published to the BORN website. This initiative to be evaluated in 2015.	Evergreen	Evergreen item. Discuss annually as BORN grows and new user types may potentially be added.
High priority RM2 – Continue implementation of a comprehensive information security management program – Implement a comprehensive information security management program based on international standards and best practices. Refer to TRA for more details.	Security program audit and management exercise underway September, 2013 - February, 2014.	Evergreen	Evergreen item. Discuss annually as current audit program will grow over time.
High priority RM4 – Ensure sufficient resources to audit logs and respond to security incidents – Ensure sufficient skilled resources to monitor audit logs and detect potential privacy and security breaches.	Security program audit and management exercise underway Fall 2013 - Spring 2014. Privacy resources increased and security log auditing to date does not currently require more resources. On-going, ad-hoc auditing well underway and no shortfall of resources noted.	February, 2014	Closed
Medium priority RM3 – Update HR policy – Update policy HR-10 to include immediate termination of access privileges and return of sensitive assets, particularly when someone is terminated for cause.	Completed/addressed: this update is included in the annual review of all privacy and security policies and procedures. Policy updated to indicate immediate removal of PHI access privileges for employees terminated with cause and immediate recovery of sensitive assets.	February, 2014	Closed
Medium priority RM5 – Update disposal policy – Update policy S-07 to address specific means for disposing and destroying media containing PHI and other security sensitive data	Completed/addressed. Records of personal health information transferred out of BORN are subject to retention and destruction guidelines in the associated research agreement or data sharing agreement. This is reflected in S-07.	February, 2014	Closed

Recommendation	Manner in which the Recommendation is to be addressed	Actual Completion Date	Comments/Status
and media, and for ensuring appropriate certificates and records of destruction are maintained.			
Medium priority RM7 – Update security policies– Update the PSMP to fill in gaps. Include policies on access control (including administrators and end-users who are not agents of BORN, e.g. hospitals, MPGs), systems acquisition, development and maintenance, protection from malicious and mobile code, and the protection of security sensitive information. Specific guidance on content can be found in IPC's Manual for the Review and Approval of Prescribed Persons and Prescribed Entities (pp. 75 & 76).	Completed/addressed. Each mandated element of the IPC policies and procedures is being verified against the BORN security policies and procedures and any non-compliances will be found and addressed as part of BORN's tri-ennial review by the IPC (2014 review).	February, 2014	Closed
Medium priority RM8 – Complete TRA on CHEO underlying infrastructure – Complete a TRA on the underlying infrastructure supporting the BORN solution.	CHEO TRA completed in march 2013.	3/19/2013	Closed
If BORN chooses to collect, use and disclose personally identifiable ART data from out-of-province FTCs, then BORN or its business partners should conduct a PIA for each jurisdiction to confirm,	BORN does not collect personally identifiable ART data from any out-of-province organization.	10/29/2013	Closed
a. that the FTC can disclose such information to BORN without consent,			
b. BORN's status under applicable out-of-province legislation, and			
c. the status of the FTC under applicable legislation.			

Recommendation	Manner in which the Recommendation is to be addressed	Actual Completion Date	Comments/Status
2. If BORN chooses to collect, use and disclose de-identified ART data from out-of-province FTCs, then BORN should confirm with the Electronic Health Information Laboratory that proposed methods for de-identification of data are effective and in compliance with applicable privacy legislation in each jurisdiction.	BORN does not collect personally identifiable ART data from any out-of-province organization.	29-Oct-13	Closed

BORN Privacy Audit Program

Privacy Audit Plan			Privacy Audit Results		
#	**Audit Description**	**Purpose of the privacy audit**	**Audit Date**	**Recommendations/Plan to address**	**Date or plan for recommendations to be addressed.**
1	Do policies and procedures in the Privacy and Security Management Plan continue to reflect IPC requirements?	Ensure all IPC requirements are met. This audit will review each of the requirements in the IPC Manual for the Review and Approval of Prescribed Persons and Prescribed Entities and ensure they are addressed in BORN policies and procedures in the BORN Privacy and Security Management Plan..	March 2014 – October 2014	All details of this audit documented in the IPC triennial review of BORN policies and procedures.	
2	Audit P-09: log of Agents Granted Approval to Access/Use/Disclose Personal Health Information	Compare BORN system produced report of users and their associated role/privileges with hard copy signed forms authorizing the access and role.	27-Oct-13	All hard copy forms on file.	No recommendations
3	Audit elements of one research agreement.	Audit of an external research agreement to obtain from the researcher reasonable assurances of compliance with the agreement, specifically: Terms of Use (seeking confirmation that the data is being used only for the purpose it was disclosed). Physical safeguards (where the data is stored) Confidentiality Agreements for each collaborator with access to the data	Scheduled for March 2014		

Privacy Audit Plan			Privacy Audit Results		
4	Audit third-party service provider agreement.	To ensure all elements of the third-party service provider agreement are covered in a vendor agreement signed prior to the creation of the BORN IPC-approved third party service provider agreement.	February 24, 2014	Recommendation to replace the agreement with the BORN template agreement for third party service providers.	Summer 2014
6	Audit of 45 agents to ensure computers are equipped with an automated password-protected screen saver after a period of 15 minutes or less.	To ensure that agents have automatic p/w protected screen savers on their computers. The audit e-mail also contained instructions on how to enable the screen saver if it was not already in place.	23-Oct-13	15 agents used the instructions in the audit e-mail to enable their automated password-protected screen saver (as it was not enabled).	No recommendation as BORN privacy training, as of early October 2013, mandates that each BORN agent confirm via e-mail to the privacy officer that their computer is equipped with this automated screen saver. This audit was conducted as a result of this change to ensure that all BORN agents had this feature in place.
7	Audit a cross-section of collection data sharing agreements (71 agreements) to ensure all appear in P-18: Log of Datasharing Agreements	To verify the accuracy of the collection data sharing agreement log.	February 6, 2014	All agreements were reflected in log. Log also captures the PHI covered under each agreement; this audit noted inconsistent terminology between the list of PHI in DSA log and the list of PHI in DSA itself.	Use consistent terminology for data elements across all organizations and data sharing agreements. Date to address this matter is March 2015 when all collection DSAs are due for renewal.

Privacy Audit Plan			Privacy Audit Results		
8	Audit a cross-section of collection data sharing agreements (71 agreements) to ensure PHI listed in agreement matches PHI coming into the BORN System.	Ensure PHI encounters named in agreements match the automated collection of PHI in the BORN system. Data sharing agreements were completed for more than 100 organizations when the BORN System went live in Jan – April 2012; this exercise will help determine the type of work needed to support renewed agreements which are due in 2015.	February 6, 2014	Three agreements contained discrepancies between the collection of PHI as noted in the agreement vs the collection of PHI coming into the BORN system. Three agreements to be updated.	Updates to be made during the March 2015 renewal of all BORN collection DSAs.
9	Audit all privacy logs.	To ensure all logs are implemented and up-to-date: P:09: Log of Agents Granted Approval to Access/Use/Disclose PHI P-11: Log of Approved Uses of PHI for Research P-11A: Data Tracking Log P-15: Log of Research Agreements P-18: Log of Agreements with Third Party Service Providers P-23: Log of Approved Linkages of Records of PHI P-26: Log of Privacy Impact Assessments Initiated/Completed P-26A: Log of Privacy Impact Assessments Not Undertaken P-28: Log of Privacy Audits P-30: Log of Privacy Breaches P-32: Log of Privacy Complaints and Enquiries	Logs verified during fall/winter of 2013-2014.	The following logs were not in use (contents were tracked and known, but not in the log files): P-11: Log of Approved Uses of PHI for Research P-18: Log of Agreements with Third Party Service Providers P-23: Log of Approved Linkages of Records of PHI P-26A: Log of Privacy Impact Assessments Not Undertaken	Mar-14
10	Consent model in fertility clinics	Verify a cross-section of patient consent forms at three clinics to ensure proper documentation of is in place.	Apr-14		

Privacy Audit Plan			Privacy Audit Results		
11	Verify that a BORN announcement of new collection of data is supported by existing data sharing agreements.	Ad-hoc audit following a BORN internal communication dated January 30th that announced a new data collection from two specific organizations. Verified the data sharing agreements for the organizations to ensure this collection was included in existing data sharing agreements.	January 31, 2014.	All agreements in place.	No recommendation
12	Verify that three organizations contributing data to the BORN System are implementing sensitive user roles correctly.	To ensure administrators of the BORN system at organizations contributing data to BORN have implemented a sensitive role in an appropriate way. This privacy audit is a reminder to from BORN to contributing organizations that specific roles have increased access privileges that are not appropriate or necessary for many users.	Start: February 20, 2014. End: on-going (2/3 organizations responded as of Feb 28, 2014)	As of Feb 28: Org 1: correct use of this role is in place. Org 2: correct use of this role in place. Org 3: response outstanding	As of Feb 28: Org 1: no recommendations Org 2: no recommendations Org 3: audit on-going
13	Annual audit: verify BORN agent adherence to BORN Confidentiality Agreement and privacy policies and procedures via e-mail survey with mandatory acknowledgement.	To ensure that all BORN employees acknowledge annually they are aware of and abiding by the privacy policies and procedures as part of their annual renewal of their Confidentiality Agreements.	27-Oct-13	All agents acknowledged.	No recommendation
14	Series of dual privacy/security audits to review activity and access to the BORN System by employees with access to PHI.	To ensure no intentional privacy breaches occurred (snooping) as detailed in next three rows (audits 14.1, 14.2, 14.3 where privacy audit details appear in bold text).			

Privacy Audit Plan			Privacy Audit Results		
14.1	**Verify user audit report to view audit logs of system activity by BORN System Administrator.**	Dual security and privacy audit. Security: ensure user access is demonstrable by system access audit logs. **Privacy: ensure user activity in line with role at BORN.**	February 19, 2014 11 am - 12 pm.	**None. All activity in line with expectations of BORN System Administrator role.**	**No recommendations**
14.2	**Verify user audit report to view audit logs of system activity by BORN employee with access to PHI.**	Dual security and privacy audit. Security: ensure user access is demonstrable by system access audit logs. **Privacy: ensure user activity in line with role at BORN.**	February 19, 2014 11 am - 12 pm.	**None. All activity in line with expectations of BORN employee (agent) with access to PHI.**	**No recommendations**
14.3	**Verify user audit report to view audit logs of system activity by BORN employee with access to PHI.**	Dual security and privacy audit. Security: ensure user access is demonstrable by system access audit logs. **Privacy: ensure user activity in line with role at BORN.**	October 28, 2013 @ 1:40 pm.	**None. All activity in line with expectations of BORN employee (agent) with access to PHI.**	**No recommendations**
15	Series of dual privacy/security audits to review access to high-profile patients in the BORN system.	To ensure no intentional privacy breaches occurred (snooping). BORN performed eight (8) such audits and issued no recommendations. Details appear in audits 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, and 1.7a in the **BORN Security Audit Program** table beginning on p. 48)			
16	Trial audit: prompt local administrators at organizations contributing data to the BORN System to review their list of BORN users and roles.	Produce a list of users at each organization; e-mail the list to each organization to prompt the local administrator to review the list of users and amend as necessary. Dual privacy and security audit to ensure security access controls are understood, reviewed, and applied with privacy in mind.	January - February 2013	Organizations responded as follows: 1) Existing list is correct; 2) List has been updated; 3) did not respond. Recommendations: 1) conduct audit annually 2) follow up	1) Add to 2014 audit plan 2) Follow up to occur in 2014 audit.

Privacy Audit Plan			Privacy Audit Results		
				with organizations that do not respond	
17	Annual audit: ensure BORN managers receive a list of their employees' access/role and confirms/updates it as necessary.	To ensure continued need to access PHI is reviewed and amended as necessary (dual security and privacy audit). Security: BORN System produces list of users, roles, and what each role accesses. Privacy: ensure level of access to PHI for each agent is correct and needed for the role.	Start date: February 20, 2014. Audit on-going.		
18	Audit for all BORN agents that there is: 1. No personal health information on desks in paper format 2. No personal health information on portable devices, i.e. USB keys, CDs, DVDs 3. All computers are encrypted	To ensure all BORN agents perform a random check and re-acknowledge these mandated privacy elements (no printed or portably-stored PHI and all systems are equipped with encryption).	Mar-14		
19	Assess organizational compliance with BORN privacy policies and procedures.	To ensure that BORN agents are compliant to BORN privacy policies and to ensure that BORN privacy policies as written are amended where necessary. BORN privacy policies were written and approved before the BORN System went live and started collecting personal health information; an assessment of their accuracy and applicability after the BORN system is	Start date: June 2013. End date: review on-going; updated and approved policies and procedures to be published in December 2014		

Privacy Audit Plan			Privacy Audit Results		
		up and running will ensure alignment of workplace practices and approved policies and procedures.			

BORN Security Audit Program

Security Audit Plan			Security Audit Results		
#	**Nature and type of security audit**	**Purpose of the security audit**	**Date security audit completed**	**Description of recommendation**	**Date and manner in which each recommendation was or is to be addressed**
1.1	Verify access to maternal and newborn records of high profile birth mother and baby.	Ensure no access by unauthorized users and/or evidence of "elevated activity" (dual security and privacy audit). Security: viewed system access audit logs. Privacy: ensure no inappropriate access (snooping) to high profile patient.	10/2/2013 14:00	No inappropriate access detected; repeat in several months to re-verify access to records.	Re-verify records in February 2014 and record as separate audit. See audit # 1.2 for results of follow-up audit.
1.2	Re-verify access to maternal and newborn records of high profile birth mother and baby in audit 1.1.	Ensure no access by unauthorized users and/or evidence of "elevated activity" (dual security and privacy audit). Security: viewed system access audit logs. Privacy: ensure no inappropriate access (snooping) to high profile patient.	February 19, 2014 @ 11:18 am.	No inappropriate access detected. Audit closed.	No recommendations
1.3	Check appropriateness of audit logs to verify access to baby records of a BORN employee.	Ensure no access by unauthorized users and/or evidence of "elevated activity" (dual security and privacy audit). Security: viewed system access audit logs. Privacy: ensure no inappropriate access (snooping) to records of BORN employee.	October 28, 2013 @ 2pm.	No inappropriate access detected; repeat in several months to re-verify access to records.	Re-verify records in February 2014 and record as separate audit. See audit # 1.4 for results of follow-up audit.
1.4	Re-verify audit logs to ensure no inappropriate access to baby records of a BORN employee (in audit 1.3).	Ensure no access by unauthorized users (dual security and privacy audit). Security: viewed system access audit logs. Privacy: ensure no inappropriate access (snooping) to records of BORN employee.	February 19, 2014 @ 11:30 am.	No inappropriate access detected. Audit closed.	No recommendations
1.5	Check appropriateness of audit logs to verify access to baby records of a BORN employee.	Ensure no access by unauthorized users and/or evidence of "elevated activity" (dual security and privacy audit). Security: viewed system access audit logs. Privacy: ensure no inappropriate	October 28, 2013 @ 2:06 pm.	No inappropriate access detected; repeat in several months to re-verify access to records.	Re-verify records in February 2014 and record as separate audit. See audit # 1.6 for results of follow-up audit.

Security Audit Plan			Security Audit Results		
		access (snooping) to records of BORN employee.			
1.6	Re-verify audit logs to ensure no inappropriate access to baby records of a BORN employee (in audit 1.5).	Ensure no access by unauthorized users (dual security and privacy audit). Security: viewed system access audit logs. Privacy: ensure no inappropriate access (snooping) to records of BORN employee.	February 19, 2014 @ 11:36am.	No inappropriate access detected. Audit closed.	No recommendations
1.7	Placeholder to verify maternal and newborn records of high-profile birth mother and baby.	Ensure no access by unauthorized users (dual security and privacy audit. Security: viewed system access audit logs. Privacy: ensure no inappropriate access (snooping) to high profile patient.	March 2014		Recommendation will be to re-verify records in August 2014 and record as separate audit (1.7a).
1.7a	Placeholder to re-verify maternal and newborn records of high-profile birth mother and baby after a period of four months (re-verification of audit 1.7).	Ensure no access by unauthorized users and/or evidence of "elevated activity"(dual security and privacy audit. Security: viewed system access audit logs. Privacy: ensure no inappropriate access (snooping) to high profile patient.	August 2014		
1.8	Verify user audit report to view audit logs of system activity by BORN System Administrator.	Dual security and privacy audit. Security: ensure user access is demonstrable by system access audit logs. Privacy: ensure user activity in line with role at BORN.	February 19, 2014 11 am - 12 pm.	None. All activity in line with expectations of BORN System Administrator role.	No recommendations
1.9	Verify user audit report to view audit logs of system activity by BORN employee with access to PHI.	Dual security and privacy audit. Security: ensure user access is demonstrable by system access audit logs. Privacy: ensure user activity in line with role at BORN.	February 19, 2014 11 am - 12 pm.	None. All activity in line with expectations of BORN employee (agent) with access to PHI.	No recommendations

Security Audit Plan				Security Audit Results		
1.10	Verify user audit report to view audit logs of system activity by BORN employee with access to PHI.	Dual security and privacy audit. Security: ensure user access is demonstrable by system access audit logs. Privacy: ensure user activity in line with role at BORN.		October 28, 2013 @ 1:40 pm.	None. All activity in line with expectations of BORN employee (agent) with access to PHI.	No recommendations
2	Verify access to CHEO hosted BORN drive designated for storage of PHI (encrypted).	Ensure access to PHI on encrypted drive is correctly controlled.		Spring 2014		
3	Verify use of super user account, via access control logs, used by third party service provider that builds the BORN system. View six month period of user activity.	Security and privacy: 1) Security: view audit logs to ensure access is in line with the expected use of this "super user" account. 2) Privacy: follow up with vendor to verify who has access, that they track and control it effectively, and that users understand the "super user" status of this account is for specific use only (outline use cases).	1) Feb 19, 2014 @ 3pm. 2) Feb 20, 2014 sent e-mail requesting vendor to verify and acknowledge use of account in line with BORN expectations (where expectations are outlined in e-mail).		1) None. All activity in line with expected use of this account. 2) None. Use of super user account by vendor and their understanding of its sensitivity is in line with expectations.	1) No recommendations 2) No recommendations
4.1	Audit FTP user accounts.	Remove/clean-up user accounts that are no longer needed. E-mail sent to FTP account users asking them to confirm continued need for account; non responses to result in deleted accounts; response due date included in e-mail.		Oct 15 - 22, 2013	Closed 14 of 42 accounts that are no longer needed. Accounts closed on three dates: Nov 6, 2013, Nov 13, 2013, and Dec 13, 2013	No recommendations
5.2	Audit BORN log: **S-06B Log of Agent use of mobile Devices/Remote Access**	To ensure that log is up-to-date and that any mobile devices indicated in the log have been returned/destroyed.		February 2014	Log up to date.	No recommendations
5.3	Audit S-12A Log of Change Requests	Ensure that all elements of this log are tracked by the Data Collection Review Committee (responsible for reviewing most changes to the BORN system) and by the Security team as	February 2014		The change management chair (Data Collection Review Committee) tracks far more than what is requested in the log; a thorough	Update log to reflect true work of Data Collection Review Committee once change management

Security Audit Plan			Security Audit Results		
		necessary.		review of change management at BORN is on-going. Update log to align with the work of the Data Collection Review Committee and the security team.	review is complete. Expected date: November 2014.
5.5	Audit S-18: Log of Security Breaches	Ensure log is up-to-date and any recommendations have been transferred to the Consolidated Log of Recommendations.	October 2013	None. Log up to date.	No recommendations
5.6	Audit P-09 Agent Data Access log	Verify that for each log entry there is a signed Agent Data Access Form.	October 2013	None. All signed forms on file.	No recommendations
6	Trial audit: prompt local administrators at organizations contributing data to the BORN System to review their list of BORN users and roles.	Produce a list of users at each organization; e-mail the list to each organization to prompt the local administrator to review the list of users and amend as necessary. Dual privacy and security audit to ensure security access controls are understood, reviewed, and applied with privacy in mind.	January - February 2013	Organizations responded as follows: 1) Existing list is correct; 2) List has been updated; 3) did not respond. Recommendations: 1) conduct audit annually 2) follow up with organizations that do not respond	1) Add to 2014 audit plan 2) Follow up to occur in 2014 audit.
7	Annual audit: ensure BORN managers receive a list of their employees' access/role and confirms/updates it as necessary.	To ensure continued need to access PHI is reviewed and amended as necessary (dual security and privacy audit). Security: BORN System produces list of users, roles, and what each role accesses. Privacy: ensure level of access to PHI for each agent is correct and needed for the role.	Start date: February 20, 2014. Audit on-going.		
8	Annual audit: verify BORN agent adherence to security policies and procedures via e-mail survey with mandatory	To ensure that all BORN employees acknowledge they are aware of and abiding by the security policies and procedures as part of their annual renewal of their Confidentiality Agreements.	10/27/2013	None. All BORN agents provided acknowledgement.	No recommendations

Security Audit Plan			Security Audit Results		
	acknowledgement.				
9	Verify that three organizations contributing data to the BORN System are correctly implementing sensitive BORN system user roles.	To ensure administrators of the BORN system at organizations contributing data to BORN have implemented a sensitive role in an appropriate way. Security: BORN logging capabilities track roles and privileges/organization. Privacy: reminder/review with contributing organizations that specific roles have increased access privileges that are not appropriate or necessary for many users; security access controls can only be understood and applied with strict privacy in mind.	Start date: February 20, 2014. Audit on-going.		
10.1	Threat Risk Assessment (internal and external)	Identify external and internal risks; to be completed by third party and planned as part of a project that will introduce changes to the BORN System.	August 2014		
10.2	Vulnerability Assessment and ethical hacking	Assess system vulnerabilities - on external facing applications.	Spring 2014 following the introduction of several enhancements to the BORN system.		
10.3	Penetration Testing	Testing of BORN portal from Internet and e-health Ontario.	Spring 2014 following the introduction of several enhancements to the BORN system.		
10.5	Audit of security controls to assess effectiveness	2013 security controls audit focused on physical security of premises where PHI is located (compliance audit to policy S-03: Ensuring Physical Security of PHI).			

Security Audit Plan			Security Audit Results		
		See audits 10.5.1, 10.5.2, 10.5.3, 10.5.4.			
10.5.1	HID card access # 1.	Verify card access in force.	10/25/2013	None. Card access verified.	No recommendation
10.5.2	HID card access #2.	Verify card access in force.	10/25/2013	None. Card access verified.	No recommendation
10.5.3	Locked cabinet (to servers).	Verify key access to locked cabinet.	10/25/2013	Update procedure to reflect the set up in place in new server room (stronger – third level of HID card access, visitors must sign in and out of a log book, and must be accompanied by an escort. Sever rack also equipped with a camera that is backed up.	November 2014.
10.5.4	Fire alarms, fire suppression (pre-action sprinkler and NOVEC 1230), HVAC redundancy, UPS redundancy, generator backup and dual power feeds.	Verify all fire prevention elements.	10/25/2013	None. Fire prevention elements verified and in place.	No recommendation