

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

**2017 Three-Year Review of the  
Prescribed Persons and Prescribed  
Entities**



## Table of Contents

I.	Introduction .....	6
II.	Mandatory Requirements and Implementation of, and Adherence to Practices and Procedures .....	7
III.	Statement on Non-compliance .....	8
IV.	Appendix “B”: Compliance to IPC Requirements .....	10
	BORN Compliance to IPC Manual Part 1 – Privacy Documentation .....	10
	1.1 Privacy Policy in Respect in Respect of CHEO’s Status as a Prescribed Person .....	10
	1.2 Policy and Procedures for Ongoing Review of Privacy and Security Policies, Procedures and Practices .....	14
	1.3 Policy on the Transparency of Privacy Policies, Procedures and Practices .....	15
	1.4 Policy and Procedure for the Collection of Personal Health Information AND Statements of Purpose for Data Holdings Containing Personal Health Information .....	16
	1.5 List of Data Holdings Containing Personal Health Information .....	18
	1.6 Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information .....	18
	1.7 Statements of Purpose for Data Holdings Containing Personal Health Information .....	18
	1.8 Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information .....	19
	1.9 Log of Agents Granted Approval to Access and Use Personal Health Information .....	22
	1.10 Policy and Procedures for the Use of Personal Health Information for Research .....	22
	1.11 Log of Approved Uses of Personal Health Information for Research .....	25
	1.12 Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research .....	25
	1.13 Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements .....	29
	1.14 Template Research Agreement .....	33
	1.15 Log of Research Agreements .....	36
	1.16 Policy and Procedures for the Execution of Data Sharing Agreements .....	36
	1.17 Template Data Sharing Agreement .....	37
	1.18 Log of Data Sharing Agreements .....	40
	1.19 Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information .....	41
	1.20 Template Agreement for All Third Party Service Providers .....	42
	1.21 Log of Agreements with Third Privacy Service Providers .....	45
	1.22 Policy and Procedures for the Linkage of Records of Personal Health Information .....	45
	1.23 Log of Approved Linkages of Records of Personal Health Information .....	46
	1.24 Policy and Procedures with Respect to De-Identification and Aggregation .....	47
	1.25 Privacy Impact Assessment Policy and Procedures .....	48
	1.26 Log of Privacy Impact Assessments .....	50
	1.27 Policy and Procedures in Respect of Privacy Audits .....	51
	1.28 Log of Privacy Audits .....	52
	1.29 Policy and Procedures for Privacy Breach Management .....	52

1.30 Log of Privacy Breaches .....	56
1.31 Policy and Procedures for Privacy Complaints .....	56
1.32 Log of Privacy Complaints .....	58
1.33 Policy and Procedures for Privacy Inquiries.....	59
BORN Compliance to IPC Manual Part 2 – Security Documentation.....	60
2.1 Information Security Policy.....	60
2.2 Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices .....	62
2.3 Policy and Procedures for Ensuring Physical Security of Personal Health Information .....	62
2.4 Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity .....	65
2.5 Policy and Procedures for Secure Retention of Records of Personal Health Information .....	65
2.6 Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices.....	67
2.7 Policy and Procedures for Secure Transfer of Records of Personal Health Information.....	69
2.8 Policy and Procedures for Secure Disposal of Records of Personal Health Information.....	71
2.9 Policy and Procedures Relating to Passwords .....	72
2.10 Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs .....	73
2.11 Policy and Procedures for Patch Management .....	74
2.12 Policy and Procedures Related to Change Management .....	75
2.13 Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information .	78
2.14 Policy and Procedures on the Acceptable Use of Technology.....	78
2.15 Policy and Procedures In Respect of Security Audits.....	80
2.16 Log of Security Audits .....	81
2.17 Policy and Procedures for Information Security Breach Management .....	81
2.18 Log of Information Security Breaches.....	84
BORN Compliance to IPC Manual Part 3 – Human Resources Documentation.....	85
3.1 Policy and Procedures for Privacy and Security Training and Awareness .....	85
3.2 Log of Attendance at Initial Privacy and Security Orientation and Ongoing Privacy and Security Training .....	87
3.3 Policy and Procedures for the Execution of Confidentiality Agreements by Agents.....	87
3.4 Template Confidentiality Agreement with Agents .....	88
3.5 Log of Executed Confidentiality Agreements with Agents .....	89
3.6 Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program .....	89
3.7 Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program .....	90
3.8 Policy and Procedures to Termination or Cessation of the Employment or Contractual Relationship .....	91
3.9 Policy and Procedures for Discipline and Corrective Action.....	92
BORN Compliance to IPC Manual Part 4 – Organizational and Other Documentation .....	94
4.1 and 4.2 Privacy and Security Governance and Accountability Framework .....	94
4.3 Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program .....	96

4.4 Corporate Risk Management Framework.....	96
4.5 Corporate Risk Register.....	98
4.6 Policy and Procedures for Maintaining a Consolidated Log of Recommendations.....	98
4.7 Consolidated Log of Recommendations .....	99
4.8 Business Continuity and Disaster Recovery Plan .....	99
V. Appendix “C”: Privacy, Security and Other Indicators.....	102
Part 1: Privacy Indicators .....	102
General Privacy Policies, Procedures and Practices .....	102
Collection .....	107
Use .....	108
Disclosure.....	109
Data Sharing Agreements .....	111
Agreements with Third-Party Service Providers.....	111
Data Linkage.....	111
Privacy Impact Assessment.....	112
Privacy Audit Program .....	116
Privacy Breaches .....	125
Privacy Complaints.....	125
Part 2: Security Indicators.....	126
General Security Policies and Procedures .....	126
Physical Security .....	131
Security Audit Program.....	132
Information Security Breaches .....	137
Part 3: Human Resources Indicators.....	137
Privacy Training and Awareness .....	137
Security Training and Awareness.....	140
Confidentiality Agreements .....	143
Termination or Cessation.....	143
Part 4: Organizational Indicators .....	144
Risk Management .....	144
Business Continuity and Disaster Recovery .....	145

## I. Introduction

The Better Outcomes Registry and Network (BORN) is Ontario's pregnancy, birth and childhood registry and network. 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, 2016 unless otherwise noted.

## **II. 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 [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.

### III. 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.

BORN has two non-compliances to report, as follows:

#### 1. Privacy Policy P-16: Data Sharing Agreements

The BORN privacy policy on data sharing agreements states:

*BORN Ontario requires the execution of a data sharing agreement when BORN Ontario is collecting Personal Health Information from health information custodians (hospitals, midwifery practice groups and laboratories, clinics) for the purposes of BORN Ontario.*

##### **Specific non-compliance:**

BORN collects personal health information from all Midwifery Practice Groups in Ontario and puts in place appropriate data sharing agreements. These data sharing agreements were due for renewal in September, 2015. Despite best efforts to put new agreements in place in a timely fashion, some of the data sharing agreements lapsed. Collection of personal health information continued uninterrupted and BORN will honour all provisions of the data sharing agreements for any lapse in coverage.

##### **Background of non-compliance:**

A review of the BORN data sharing agreement template by the Association of Ontario Midwives (AOM), on behalf of their member organizations, resulted in a delay in execution of BORN data sharing agreements by many Midwifery Practice Groups. BORN delivered amendments to the original data sharing agreements, extending the term by six months, in order to allow time for the AOM review. BORN worked closely with the AOM to address all concerns. The AOM ultimately recommended the signing of BORN data sharing agreements by member organizations via a communication delivered on or about June 20, 2016.

##### **Update on non-compliance:**

As of October 28, 2016 all midwifery practice groups have signed data sharing agreements with BORN.

#### 2. Security Policy S-05: Secure Retention of Records of Personal Health Information

The BORN policy on the secure retention of records of personal health information identified the BORN Information System as the only repository for personal health information.

##### **Specific non-compliance:**

BORN stores the following records of personal health information on the BORN PHI Drive, which was not documented in policy S-05: Secure Retention of Records of Personal Health Information:

- Record-level data files, where the data may be:
  - Collected under a data sharing agreement, as per **P-04: Collection of Personal Health Information**



- Research and analysis data files including but not limited to internal and external research datasets, analysis related to data quality, BORN Information System testing, data requests and disclosures
- Historical datasets pre-dating the BORN Information System
  - Collected under a data sharing agreement, as per **P-04: Collection of Personal Health Information**

**Background of non-compliance:**

It is important to note that while the BORN policy and procedure was not clear regarding the acceptable use of the BORN PHI Drive for secure storage, it was always BORN's intention for this drive to be used. The personal health information on this drive is used for research and analysis, an important part of BORN's Ministry mandate. The non-compliance is with respect to the content of the written procedure, but not with respect to privacy and security practices in place in the organization.

Access to the BORN PHI Drive is via dual authorization (BORN Scientific Manager and BORN Privacy Officer) based on the role of the BORN Agent and their need to access and use records of personal health information to fulfill BORN's mandate (data analysts, for example). The BORN PHI Drive is equipped with auditing controls and uses role-based authentication and is managed by Microsoft Active Directory groups.

**Compliance strategy and milestones:**

Ensure the following policy and procedure updates are in place:

*S-05: Secure Retention of Records of Personal Health Information:* update to ensure the BORN PHI Drive is appropriately reflected

- Milestone for achieving compliance: March 2017 (current draft version of policy approved and in use at the time of this report filing)
- Individuals responsible for achieving compliance: BORN Privacy Officer and BORN Manager of Health Informatics

*P-08: Limiting Agent Access to and Use of Personal Health Information, including P-08A: BORN PHI Access Request Form and P-09: Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information:* ensure the application, approval process and renewal procedure applies to the BORN PHI Drive

- Milestone for achieving compliance: March 2017
- Individuals responsible for achieving compliance: BORN Privacy Officer and BORN Manager of Health Informatics

*S-10: System Control and Audit Logs:* update policy and procedure to reflect system control and audit logging features on the BORN PHI Drive

- Milestone for achieving compliance: March 2017
- Individuals responsible for achieving compliance: BORN Privacy Officer and BORN Manager of Health Informatics

## IV. 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 Informatics, who report to the BORN 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 and early childhood periods).

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 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:

- Identifying where appropriate care has not been received and facilitating 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)
- Facilitating continuous improvement of health care delivery tools to minimize adverse outcomes
- Raising alerts where maternal and/or newborn outcomes are clinically or statistically discrepant with accepted norms
- Enabling health care providers to improve care by providing them the information and tools to compare themselves with peers and/or benchmarks

- Knowledge translation strategies to improve the quality and efficiency of care for mothers, infants and children
- Creating reports that can be used to provide the Ministry of Health and Long-Term Care, Local Health Integration Networks (LHIN) 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
  - Information provided in reports to the Ministry, Local Health Information Networks and Public Health does not contain personal health information or identify individuals; reports 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](http://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 states clearly:

- BORN prohibits **paper** records of personal health information.

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 combined policy for the ongoing review of privacy and security policies and procedures. 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 and procedure, 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 and must include:

- Subject matter expert consultation
- 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**.
- Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective Action** which clarifies:
  - The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

### 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: <ul style="list-style-type: none"> <li>• Prenatal and Newborn screening providers</li> <li>• Hospitals</li> <li>• Midwives</li> <li>• Outpatient clinics</li> <li>• Fertility clinics</li> <li>• Family Health Teams/Primary Care Providers</li> <li>• Birth Centres</li> <li>• Autism Treatment Centres</li> <li>• Public Health Units</li> </ul>
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.
7	NIPT (non-invasive prenatal testing)	Historical dataset for NIPT (prior to Ontario patriation of NIPT).
8	Cytogenetics	Historical datasets for antenatal and newborn cytogenetic analyses from regional cytogenetics laboratories

### 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 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.

### 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 procedure defines five types of access, classified as roles, as follows:

1. Data Entry Roles: create, read, update, delete privileges
2. Reporting Roles: read only
3. Administrative Roles: each administrative role has defined privileges for create, read, update, delete or view, as appropriate
4. Administrative Roles for the Online Data Dictionary Tool Roles: multiple roles exist, each with defined privileges for create, read, update, delete, or read only
5. Direct Database Access: read only back end access

**Note:** *The Agent Data Access Form does not assign the authority to disclose Personal Health Information. Any disclosure of Personal Health Information must follow the appropriate disclosure policy.*

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 the access to and use of personal health information required for the agent to fulfill his or her mandate. The immediate supervisor submits the Form to the Privacy Officer along with a

justification for access as relates to the agent's job. 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:

- Whether 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

#### *Conditions or Restriction on the Approval*

The BORN policy on Limiting Agent Access to and Use of Personal Health Information sets out that access to personal health information is conditional on each agent having a signed Confidentiality Agreement in place, as per BORN policy HR-05: Execution of Confidentiality Agreements by Agents.

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 prohibits:

- Agents from accessing and using Personal Health Information except as necessary for his or her employment or contractual responsibilities.
- Access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose

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.

As part of the review and approval process, the policy is clear that the BORN Privacy Officer ensures access requests to personal health information are permitted by the Act and its regulation.

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.

Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective Action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

### 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 **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, Scientific Manager or designate in the 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 **S-17: Security Breach Management** as appropriate.

Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action**:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

*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 section 13(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 Privacy Officer monitors disposal dates in P-18: Log of Data Sharing Agreements 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 or designate 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 or designate 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 contact the BORN Scientific Manager or designate to confirm receipt of the data
- The Scientific Manager or designate ensures the e-mail contains the following boiler plate information:
  - This message, including any attachments, contains confidential information and is for the sole use of the intended recipient(s). Any unauthorized use, disclosure or distribution is prohibited. If you are not the intended recipient, please notify the sender immediately and destroy the original message. The intended recipient of this message will not use the information, either alone or with other information, to attempt to identify or re-identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

### 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 or designate:

- 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 or designate 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 or designate 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 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 researcher must call the BORN Scientific Manager or designate to confirm receipt of the data and to obtain the password.

The Scientific Manager or 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 Privacy Officer or designate monitors disposal dates in P-15: Log of Research Agreements 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:

- 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
- Signed Research Agreement

#### ***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

Researchers 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 as via the Research Agreement (for de-identified information) or via e-mail (for aggregate information).

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, for any purpose, except as required by law

#### *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 requirements with respect to 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
- **Secure Destruction** means permanently destroying or erasing personal health information in such a manner that the reconstruction of the personal health information is not reasonably foreseeable in the circumstances and which for greater clarity does not include the simple recycling, discarding, or removal of the paper documents and/or electronic media containing personal health information from the Recipient's custody or control
- 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 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 designate, where the Privacy Officer or designate 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 designate 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 or disclosed.

In identifying the approved use of the personal health information being *collected* by BORN, 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
- 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 only for as long as reasonably necessary to fulfill the Purpose and in compliance with the BORN policy *S-05: Secure Retention of Records of Personal Health Information*. PHI that is no longer required by BORN for the Purpose will be converted to a de-identified format as set out in BORN's policy *P-24: De-identification and Aggregation Policy* after which the identifiable PHI will be disposed of in a secure manner as set out in the BORN policy *S-08: Secure Disposal of Records of Personal Health Information*.

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. 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 provide 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**.

Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action

## 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 and/or transfer) 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 and/or transfer 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, recipient and mode of transfer of records of personal health information and confirming receipt of the records. The contractor agrees to only transfer records of personal health information to a recipient that has been approved in writing by BORN, and 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 3.11, 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. 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**.

Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action

### 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**.

Consequences of breach are detailed in each respective breach policy (i.e. P-29 and S-17) as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action

### 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

### 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 defined 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 health 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
- Notice 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**.

Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action

### 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.

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 is 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**.

Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

### 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 **P-29: Privacy Breach Management**
- Relates to a privacy complaint and should be addressed as per **P-31: Privacy Complaints**

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**.

Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the

*Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

## **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 part of 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 combined 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 addressed in this document in section [1.2 Policy and Procedures for Ongoing Review of Privacy and Security Policies, Procedures and Practices](#).

## 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 as well as in in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

*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 the BORN Human Resources agent who alerts CHEO Human Resources and the Ottawa Hospital Photo ID and Parking desk within the Security department (either by e-mail or in person) and badge de-activation occurs immediately

- The Ottawa Hospital is notified as well as CHEO because BORN rents space from The Ottawa Hospital, who enables access to the building via their CHEO HR-arranged badge; to full de-activate a badge both organizations must be notified
- 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 HID card use. 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*

The BORN policy sets out that visitors to the BORN premises or to the Data Centre location must be supervised by a BORN agent at all times.

With respect to the Data Centre:

- The policy clearly sets out what documentation must be completed including name, date and time of arrival, time of departure and the name of the Agent with whom the visitor is meeting. If the visitor does not sign out appropriately, the policy states that 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.
- The policy states that all documentation related to the identification, screening and supervision of visitors to the Data Centre is retained by the BORN System Hosting Provider for a minimum of one year to allow for audit in case of breach or similar occurrence.

With respect to the BORN premises:

- The policy clarifies that visitors must be supervised by a BORN agent at all times, including departure. The policy does not call for sign in or out of the main BORN premises as BORN does not receive many visitors, meeting rooms are not within the main BORN premises, access to the building is via HID card only, and visitors are supervised at all times.

### **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 electronic format. BORN prohibits paper records of personal health information.

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.

The BORN policy prohibits the retention of records of personal health information for a period longer than that set out in the data sharing agreement.

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 in the BORN Information System, 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**
- Access to the BORN Data Centre, managed by the BORN System Hosting Provider, 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

For records of personal health information retained in electronic format on the BORN PHI Drive, the following safeguards are employed:

- Personal Health Information is collected via secure FTP as per BORN policy **S-07: Secure Transfer of Records of Personal Health Information** and pursuant to a data sharing agreement as per **P-16: Data Sharing Agreements**
- Access to and use of Personal Health Information on the BORN Analysis Drive is based on the need-to-know principle tied to the job description of a BORN Agent
- BORN Scientific Manager authorizes access to specific folders on the BORN PHI drive and the Privacy Officer maintains a log of access to this drive
- Access to BORN Ontario premises is controlled as per BORN policy **S-03: Ensuring Physical Security of Personal Health Information**
- Access to the BORN Data Centre, managed by the BORN System Hosting Provider, is controlled as per BORN policy **S-03: Ensuring Physical Security of Personal Health Information**
- The BORN PHI drive is equipped with audit capabilities that store the date, time and name of the user accessing Personal Health Information, as well as create and delete functions

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 as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

## **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 e-Health Ontario (eHO) ONE 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-encrypt 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 or designate 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-encrypt the data set

When receipt has been confirmed, the Scientific Manager or designate 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 electronic records of personal health information.

Note that paper records of personal health information are prohibited at BORN.

“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.

The policy states that the BORN Privacy Officer and the Manager of Health Informatics are responsible for securely disposing of records of personal health information.

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

Records of personal health information in electronic form and/or 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.

For electronic records of Personal Health Information the policy states that:

- When electronic records of Personal Health Information are to be destroyed the Privacy Officer selects the appropriate secure destruction of the data within 10 days of determining that the data is no longer required.
- The Privacy Officer informs the Manager of Health Informatics which method of destruction is to be performed (either physically destroying the device or securely wiping the device for reuse) and requests that the Manager of Health Informatics or designate:
  - Performs the secure destruction as per S-08B: Certificate of Destruction

- Complete and returns to the Privacy Officer the S-08B: Certificate of Destruction

The BORN Certificate of Destruction of Personal Health Information contains the following components:

- Description of the personal health information destroyed
- The date, time and method of secure disposal of the records of personal health information
- The name and signature of the Agent who destroyed the records of personal health information

Certificates of destruction must be completed and return to the Privacy Officer within one month of destruction of records.

BORN does not use third party service providers in securely destroying records of personal health information.

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 for operating system patches and other hosting system upgrades.

As per the BORN policy, the BORN System Hosting Provider notifies the BORN System Administrator and the BORN Application Servicer Provider via e-mail when a critical patch becomes available. For Microsoft products supported by Windows Update service (WSUS), patches become available automatically on the WSUS application which is checked weekly by the BORN System Hosting Provider. All other patches are placed in a queue of approved patches.

The policy sets out that due to the high volume of Microsoft patches, it is impracticable that each patch is reviewed individually; patch recommendations from the vendor are followed. The BORN System Hosting Provider has determined that accepting vendor recommended patches takes into consideration the balance between ensuring maximal system security and efficiency vs. the potential service disruption and general risk in applying the patch.

Notice of patches:

- Notice of critical patches are sent by the BORN System Hosting Provider via e-mail to the BORN System Administrator and the BORN Application Service Provider for immediate deployment
- All other patches are placed in a queue of approved patches
- The BORN Application Service Provider is responsible for applying Microsoft recommended patches (critical or otherwise) from the queue of approved patches to the BORN User Acceptance Testing (UAT) environment for testing
- Patches undergo soak testing in the UAT environment for a minimum of one week
- After successful testing in UAT the patches are approved and the BORN System Hosting Provider deploys the patches to the live servers
  - Where a patch does not test successfully, the BORN System Hosting Provider is responsible for denying the patch by removing the offending patch from the UAT environment prior to deploying to the live environment

The policy also states that the BORN System Hosting Provider can query upon request the WSUS application server log updates for a list of all patches (approved or denied). Each patch has a unique Microsoft Knowledge Base article which contains:

- The reason for the product update
- When Microsoft released the given update/when the patch became available
- Severity of the update (critical or regular)
- Type of update (product update, or security update)
- Name of the update
- Description of the update, including the information system, technology, equipment, resource, application or program to which the patch relates)
- Release date of update
- Date the update was approved/declined for use by WSUS
- Date a given Microsoft OS based server applied the approved update
- Rationale for not implementing

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 as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

## 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 (where BORN's operational environment is the BORN Information System).

The BORN policy sets out that BORN formally opens and tracks tickets in the Application Service Provider's change management system for all requests. Tickets contain, at a minimum, the following details:

- Description of the proposed change
- Rationale for the change
- Impact of executing or not executing the change
- Steps to reproduce the issue and test the resolution of the issue

As per BORN policy, the Manager of Health Informatics receives, reviews and approves or denies all requests and considers 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, cost of proposed change.

If a decision is made to approve the change, the procedure states that it is evaluated for any privacy or security considerations. The Terms of Reference for BORN's Data Collection Review Committee set out the types of changes that require approval from the Data Collection Review Committee.

If the decision is made *not* to approve the change, the procedure states that the Manager of Health Informatics updates the status of the change request (cancels the ticket) and the change management system tracks this decision and triggers an e-mail to relevant stakeholders. Documentation includes:

- Change requested
- Name of Agent requesting change
- Date change requested
- Date change denied/closed
- Rationale for not implementing the change (stored in the comments field)

Approved changes to the operational environment proceed as follows as set out in the BORN procedure: The Manager of Health Informatics is responsible for determining the timeframe for implementation of all approved changes. Changes which address existing vulnerabilities are given priority over changes which improve user experience.

### **Implementing a Change Request**

The Manager of Health Informatics and other technical staff with access to the change management system enter status updates, including decisions, into the change management system. The change management system tracks:

- Change requested
- Name of Agent requesting change
- Date change requested
- Date change approved
- Rationale for approval
- The priority assigned to the change
- The expected procedure for testing (the change management system notes the procedure for replicating the problem; once a problem has been fixed the steps to replicate it must be tested, verified and documented in the change management system)
- Approval from the Manager of Health Informatics (in the Comments field)

The Application Service Provider is responsible for implementation of the change. When the change is implemented, the Application Service Provider updates the change management system to reflect:

- Date change tested
- Date change was implemented in the test environment
- Sets the ticket status to “Resolved” in the change management system

### **Testing a Change Request**

When the Application Service Provider sets a ticket to “Resolved”:

- The change management system sends an automated e-mail to the requestor of the change
- The requestor tests the change, ensuring that the procedure to replicate the problem (as noted in the change management system) has been addressed
- When testing is complete, the requestor sets the ticket to “Ready for Production” in the change management system

### **Deploying a Change Request to the Live System**

Decisions regarding deployment of a change to the production (live) environment can only be made by the Manager of Health Informatics.

The Manager of Health Informatics together with the Application Service Provider reviews all tickets in the change management system with a status of “Ready for Production” and considers:

- 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
- Cost of proposed change

Where a change is not accepted for deployment the Manager of Health Informatics updates the ticket to “Under Review” enters the reason in the “Comments” field, and the ticket remains assigned to the requestor.

Where a change is accepted for deployment the Manager of Health Informatics leaves the ticket status as “Ready for Production” and the change is included in the next scheduled update.

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 as well as in **P-01: Privacy Policy in Respect of CHEO’s Status as a Prescribed Person** and **HR-11: Discipline and Corrective action** which clarifies:

- The BORN Ontario Confidentiality Agreement states that a breach of the terms of the Confidentiality Agreement, BORN Ontario policies and procedures, and/or the provisions of the *Personal Health Information Protection Act, 2004* may result in disciplinary action which can include termination of employment or legal action.

### 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, by e-mail, BBM or any known appropriate channel 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 health 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, contract, or job responsibilities

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 and the dates that the agent attended ongoing privacy and security training. The specifics of training provided at each session are available in the presentation or slide deck prepared and presented at any given training session. Copies of all privacy and security training slides are saved on the BORN privacy drive.

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 Confidentiality 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, contract or job responsibilities.

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 confidentiality 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 and 4.2 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 each 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
- BORN Director
- BORN Scientific Manager
- Manager of Health Informatics
- Privacy Officer

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

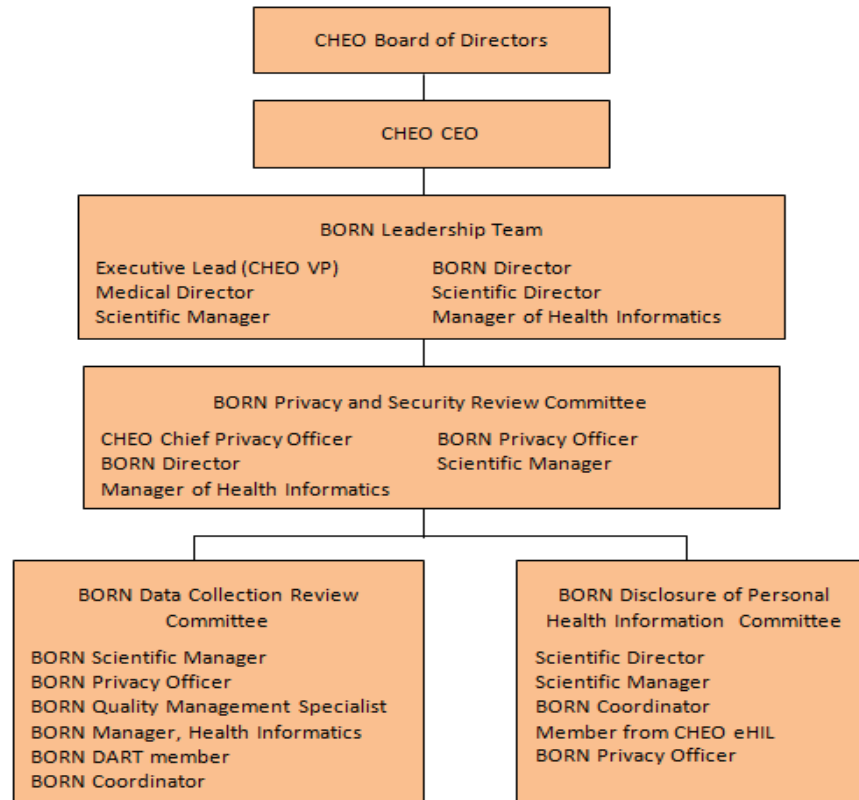
### ***Incident Management***

- 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

#### 4.3 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

#### 4.4 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.

#### 4.5 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

#### 4.6 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.

#### 4.7 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

#### 4.8 Business Continuity and Disaster Recovery Plan

BORN has in place a policy and procedure for business continuity and disaster recovery with the following stated purpose:

- To protect and ensure the continued availability of the BORN information technology environment in the event of short and long-term business interruptions and in the event of threats to the operating capabilities including natural, human, environmental and technical interruptions and threats.

The policy clearly sets out that the BORN business continuity and disaster recovery responsibilities and procedures are supported jointly by CHEO IT, as the BORN System Hosting Provider, and BORN staff and are documented in:

1. CHEO IT Disaster Recovery Plan
2. CHEO/BORN Hosting Agreement
3. BORN Ontario: Outage Communication Process
4. BORN Ontario Emergency Phone Tree Process

## 5. BORN Ontario Emergency Contact log

The BORN policy and procedure clearly address the following matters:

- Notification of the interruption or threat
- Documentation of the interruption or threat
- Assessment of the severity of the interruption or threat
- Activation of the business continuity and disaster recovery plan
- Recovery of personal health information

With respect to notification of the interruption of threat, BORN's procedure identifies that BORN staff, stakeholders, and end users must be notified by the BORN System Administrator. The detail of this activity is documented in the **BORN Outage Communication Process** which is referenced in the procedure itself. This **Outage Communication Process** sets out requirements for the manner and format of notification, timeframe of notification, the nature of the information that must be provided, and the template that must be completed in case of an incident. BORN mandates that each incident be documented in a **BORN Business Continuity Incident Summary Report**. With respect to time frame of notification, this is incident dependent. The BORN Information System is not a critical system to end users and as such, BORN has a reasonable tolerance for down time.

Contact lists are referenced in the BORN procedure; notification from the BORN System Administrator to all stakeholders including BORN staff and end users of the BORN Information System is documented in:

- The **BORN Outage Communication Process** (within Occurring Outages, and Appendix: Contact Information); maintained by the BORN System Administrator
- The **BORN Ontario Emergency Contact log**, maintained by the BORN Administrative Assistant

As per the BORN procedure, assessment of an interruption or threat, including assessment of the severity level, is set out in the **CHEO IT Disaster Recovery Plan** (Assess Phase section) which includes:

- The department responsible for assessment
- The criteria on which an assessment is based, including early assessment (which occurs within 30 minutes)
- The time frame by which the assessment must be completed (one hour)
- Any applicable initial and detailed damage assessment exercises and documentation of these exercises, which includes technical and physical infrastructure and business processes
- The persons or organizations that must be consulted

The **CHEO IT Disaster Recovery Plan** also sets out the group responsible for an assessment, as well as documentation requirements for an assessment. The assessment is documented as part of the SBAR (Situation, Background, Assessment and Recommendation) which is appended to the **CHEO IT Disaster Recovery Plan**. This document, and any others requested, is shared with senior management to facilitate on-going review of an incident. It is completed by the BORN System Hosting Provider.

The **CHEO IT Disaster Recovery Plan** identifies that relevant CHEO IS staff will be assigned duties for resumption and recovery. The plan lists the priority of infrastructure and application for recovery, assigning a priority level 1 – 4; the BIS is level 1 (last to recover) as it is not a critical system to end users and as such, BORN has a reasonable tolerance for down time . The plan also sets out timelines for applications to be restored, and all necessary assessment and consultation, including the agents/other persons required to be consulted with respect to resumption and recovery activities (the recovery team for each type of failure is outlined in the plan), as well as the documentation that must be completed, to whom it must be provided, and what it must contain (IS staff and IS management team prepare a report for the CHEO Executive Team outlining timelines, actions taken and possible root causes).

In support of the recovery operations the policy states that the BORN System Administrator maintains a detailed inventory of all critical applications and business functions and of all hardware and software, software licenses, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and network settings for firewalls, routers, domain name servers, and the like. The BORN System Administrator works with the BORN System Hosting Provider and the vendor of the BORN Information System to ensure the inventory is up-to-date. Each is responsible for maintaining their own list and providing updates to the BORN System Administrator as required.

The **CHEO IT Disaster Recovery Plan** and the **BORN Outage Communication Process** address the procedures by which decisions will be made and actions taken during an incident, including documentation.

Communication of the recovery from CHEO IS to BORN is the responsibility of CHEO IS, as detailed in the **CHEO IT Disaster Recovery Plan** as well as the System Hosting Provider Agreement between BORN and CHEO. Communication of the recovery from BORN to staff, stakeholders and end users is the responsibility of BORN (BORN System Administrator) as detailed in the **BORN Ontario Outage Communication Process** (Completed Outage section), where communication is via e-mail and includes date, time, affected system and a description of the outage. Testing, maintenance and assessment of the business continuity and disaster recovery plan is addressed in the policy as follows:

- The agents responsible for ensuring the plan is tested, maintained and assessed are identified as the BORN Technical Lead with support from the BORN System Hosting Provider
- The frequency and procedure for testing, maintaining, and assessing the plan are outlined in clear steps, naming appropriate agents for each activity
- The agents responsible for amending and approving any changes to the plan as a result of testing, maintenance and assessment are identified and outlined as follows:
  - The BORN Technical Lead provides amendments to the BORN Privacy Officer
  - BORN Privacy Officer obtains final approval from the BORN Privacy and Security Review Committee

The BORN policy on business continuity and disaster recovery planning sets out that BORN Agents are required to read the policy as part of their initial privacy training and that all BORN Agents are required to review the policy, including any amendments, as part of the annual acknowledgement of the BORN Confidentiality Agreement.

The BORN policy on business continuity and disaster recovery planning includes a list of relevant documents, the responsible agent for each document, and the storage location of each document.

## V. 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 policy P-02 and S-02: Ongoing review of Privacy and Security Policies and Procedures notes that BORN undertakes a review of polices annually or more frequently, as follows:*

BORN Ontario undertakes a review of its privacy and security policies and procedures on an annual basis or more frequently if required. The purpose of a review is to determine whether amendments are needed or whether new policies and procedures are required to ensure that BORN Ontario meets or exceeds industry standards and best practices.

To date, BORN has performed reviews of its policies and procedures more frequently than a single annual review. BORN privacy policies have been reviewed (all policies) on an on-going basis since 2014. The goal of this review is to verify implementation of all policies and procedures and make any amendments necessary. The review process was conducted as follows:

##### **Summer 2013 – Fall 2016**

All policies and procedures in the BORN Privacy and Security Management Plan were reviewed by subject matter experts and by end users. This on-going review was to solidify the operationalization of BORN policies and procedures, monitor their implementation and make any further updates on an on-going basis. BORN has been fine-tuning policy and procedure details since it first implemented all policies and procedures in 2012, when the BORN Information System was introduced. Review results and updates were captured in sequential drafts of the BORN Privacy and Security Management during this time. The result of this review will enable BORN to move to an efficient annual review of policies and procedures.

Members of BORN’s Privacy and Security Review Committee were involved in many of the individual policy reviews and updates. On October 24, 2016, the BORN Privacy Officer sent a detailed publication history recapping all changes to policies and procedures to members of this committee. All changes were accepted.

##### **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 and description of privacy policy amendments as a result of the on-going review:

**General updates:**

- Changed all references to "Data Dictionary Review Committee" to "Data Collection Review Committee"
- Updated membership in all diagrams of BORN Governance and Accountability Framework
- Clarified that BORN prohibits paper records of personal health information
- Updated contact information for Privacy Officer throughout manual
- Updated boiler plate text in most policies re compliance, audit, enforcement to better clarify consequences of breach
- Updated location of where all logs and template agreements are stored on the BORN privacy drive

**P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person**

- Clarified that day-to-day management of the security program is delegated to the Manager of Health Informatics (originally delegated to the Privacy Officer)
- Clarified that BORN *mandates* the use of the Privacy Analysis "PARAT" software to consider data de-identified
- Clarified that when BORN retains personal health information for 28 years, it is then de-identified and the identifiable PHI is destroyed. This is not a change but rather improved clarity on what happens at 28 years

**P-02 and S-02: Ongoing Review of Privacy and Security Policies and Procedures**

- Updated final approval of policies and procedure to 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
- Clarified in all spots that the Data Collection Review Committee approves not only new projects/data elements but also entire new "data holdings"

**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
- Added the following to the list of Health Information Custodians from whom BORN Collects: Family Health Teams/Primary Care Providers, Birth Centres, Autism Treatment Centres, Public Health Units
- Added cytogenetics and non-invasive prenatal testing to list of BORN Data Holdings
- Updated descriptions of data held in the BORN Information System to reflect new encounters in the health care system

**P-08 A: BORN PHI Access Request Form**

- Added two new columns: "date access terminated" and "reason access terminated"

**P-11 A: Data Tracking Log**

- Updated column regarding use of CHEO's electronic health information laboratory)to: De-identification Assessment required Y/N
- BORN developed PARAT expertise in-house and no longer uses CHEO's electronic health information laboratory for de-identification

**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
- Added standard boiler plate information to be included on all e-mails disclosing aggregate data as follows:  
*This message, including any attachments, contains confidential information and is for the sole use of the intended recipient(s). Any unauthorized use, disclosure or distribution is prohibited. If you are not the intended recipient, please notify the sender immediately and destroy the original message. The intended recipient of this message will not use the information, either alone or with other information, to attempt to identify or re-identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.*
- Clarified that recipients of aggregate data must provide acknowledgement of receipt of data
- Clarified that upcoming dates of disposal are monitored by the Privacy Officer or designate in log P-18 Log of Data Sharing Agreements for follow-up
- Added statement that the method of secure disposal mandated by the data sharing agreement is consistent with the Personal Health Information Protection Act, 2004 and its regulation, with orders issued by the Information and Privacy Commissioner of Ontario, including Order HO-001 and Order HO-006, and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario including Fact Sheet 10. The secure method of disposal has always been compliant to this standard and now the wording is reflected in the procedure
- Clarified the steps to review a de-identified dataset as follows:  
Verify the data against the approved list, check quality and frequencies, validate any documentation written to accompany the dataset (data dictionary, for example)

**P-12 A: Data Request Forms**

- Updated reference to note that aggregate and record-level data request form are available on the BORN website

**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
- Re-organized procedure to clearly set out three types of use of PHI for research purposes: 1) personal health information; 2) de-identified data; 3) aggregate data
- Clarified that the Scientific Manager may have a designate
- Updated an erroneous reference from health information custodian to researcher
- Clarified overtly that if data is not returned or destroyed as per the research agreement that BORN can contact the researcher's professional body and the Information and Privacy Commissioner
- Clarified that a researcher's obligations re PHI or de-identified data are documented in a research agreement (not a confidentiality agreement)
- Removed erroneous line from the aggregate data section of the procedure: *Approvals are conditional on the execution of a BORN Confidentiality Agreement which the Scientific Manager*



*verifies with the Privacy Officer. Replaced with updated steps on approval and provision of aggregate data, which mandates acknowledgement of receipt of data, and mandatory boiler plate information to be included on all e-mails disclosing aggregate data as follows: This message, including any attachments, contains confidential information and is for the sole use of the intended recipient(s). Any unauthorized use, disclosure or distribution is prohibited. If you are not the intended recipient, please notify the sender immediately and destroy the original message. The intended recipient of this message will not use the information, either alone or with other information, to attempt to identify or re-identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.*

- Clarified that research plans must be compliant to PHIPA section 44(2) and PHIPA Regulation 329/04 section 16
- Updated document retention as appropriate (clarified which documents are retained by the Scientific Manager or designate, and which are retained by the Privacy Officer)
- Clarified that the date of destruction is not flagged by a document management system but by reviewing the Log of Research Agreements

#### **P-15: Log of Research Agreements**

- Updated column regarding eHIL use (CHEO's electronic health information laboratory) to: De-identification Assessment required Y/N; BORN developed PARAT expertise in-house and no longer uses CHEO's eHIL for de-identification

#### **P-16: Data Sharing Agreements**

- Updated to include privacy coordinator's role in preparation and execution of data sharing agreements
- Removed policy statement that BORN enters into DSAs with the midwifery program at the Ministry of Health and Long Term Care (MOHLTC) as BORN does not disclose PHI to the MOHLTC
- Clarified that Privacy Officer has a designate
- Clarified that the date of destruction is not flagged by a document management system but by reviewing the Log 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. No changes to IPC requirements

#### **P-19: Executing Agreements with Third Party Service Providers in Respect of Personal Health Information**

- Clarified that dates of destruction are monitored by the Privacy Officer in P-21: Log of Agreements with Third Party Service Providers for follow-up
- Clarified that method of secure disposal, where applicable, is consistent with the Personal Health Information Protection Act, 2004 and its regulation, with orders issued by the Information and Privacy Commissioner of Ontario, including Order HO-001 and Order HO-006, and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario including Fact Sheet 10. The secure method of disposal has always been compliant to this standard and now the wording is reflected in the procedure
- Added the following note: Each Agreement is based on the template; at a minimum, template content will be met and further content and context will be added as needed

#### **P-22: Linkage of Records of Personal Health Information**

- Reviewed to ensure all types of linkages are addressed (confirmed that probabilistic and deterministic linking are already included in procedure)

**P-24: De-Identification and Aggregation**

- Clearly separated the procedure into two sections: 1) de-identified data 2) aggregate data  
Clarified that BORN mandates the use of PARAT software for de-identification on all record-level datasets
- Removed any reference to CHEO's electronic health information laboratory as BORN bought a license for PARAT tool to use in-house
- Note that risk thresholds are under review; BORN working with Privacy Analytics on the detailed implementation of PARAT in the BORN environment to ensure most effective installation of the tool is in place. Thresholds will be lowered (in practice they already are)
- Clarified that in the case of aggregate data the Scientific Manager may allow an exception to suppressing all cell sizes less than six ( $n < 6$ ) where 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

**P-25: Privacy Impact Assessments**

- Updated the timeframe of review of the Log of Privacy Impact Assessments Initiated/Completed and the Log of Privacy Impact Assessments Not Undertaken from monthly to quarterly

**P-29 Privacy Breach Management**

- Recommendations resulting from a breach investigation are approved by the Privacy and Security Review Committee (not the Leadership Team)
- Updated formal breach communication/updates from the Privacy Officer to the Leadership Team from monthly to quarterly. This does not replace on-going communications during a breach but rather on-going follow up

**P-31: Privacy Complaints**

- Clarified the methods by which and to whom a complaint may be made, as follows:
  - BORN website contains full contact details for the BORN Privacy Officer, a link to the BORN Complaint Form, and information on contacting the Information and Privacy Commissioner regarding compliance to PHIPA
  - BORN brochures contain a link to the BORN website (where the Privacy section of the website is very apparent) as well as an e-mail address for BORN Privacy
- Longer print publications include full contact details for the BORN Privacy Officer and the website address for the privacy section of the BORN website

**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:***

An updated draft of the BORN Privacy and Security Management Plan was e-mailed to all BORN Agents by the Privacy Officer on October 28, 2016.

***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:***

No external communications or updates have been made as a result of this review. The privacy policies on the BORN website will be updated within one month of approval of the BORN Privacy and Security Management Plan.

**Collection**

***Indicator:***

The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.

***BORN Response:***

Eight (8) 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:***

There have been no new statements of purpose developed for data holdings containing personal health information since the prior review by the Information and Privacy Commissioner of Ontario.

BORN maintains the six original (existing) statements of purpose that were approved when BORN received prescribed registry status in 2011. These six statements of purpose continue to meet the needs of BORN.

***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:***

The following six (6) statements of purpose for data holdings containing personal health information were reviewed formally on October 19, 2016 and informally on an on-going basis (discussion of statements of purpose are regular at BORN, to ensure BORN is always operating within its mandate):

- A. Identifying where appropriate care has not been received and facilitating access to care and treatment for mothers, infants and children. For example: identifying false negative screens and informing the relevant health care provider in order to enable them to offer parents appropriate care for their baby.

- B. Facilitating continuous improvement of health care delivery tools to minimize adverse outcomes. For example: improvement of screening algorithm and cut-offs to minimize missed screens.
- C. 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.
- D. Enabling health care providers to improve care by providing them the information and tools to compare themselves with peers and/or benchmarks.
- E. 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.
- F. Creating reports that can be used to provide the Ministry of Health and Long-Term Care, LHINs 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.

**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:**

33 agents were approved to access and use personal health information in the BORN Information System for purposes other than research, between November 1, 2013 and October 31, 2016.

12 of these agents no longer have this access as they are no longer employees of BORN.

57 agents are approved to access and use personal health information on the BORN PHI Drive for purposes other than research.

**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:**

11 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:**

11 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:**

18 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, as follows:

- 7 requests from Public Health Units in Ontario for access to the BORN Public Health Analytics Cube
- 9 requests from Public Health Units in Ontario for access to the Healthy Babies Healthy Children Screen
- 1 request from a Prescribed Entity (under PHIPA reg 329/04 s.18)
- 1 request from a First Nations Health Authority (pending)

**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:**

17 requests granted for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario, as follows:

- 7 requests from Public Health Units in Ontario for access to the BORN Public Health Analytics Cube
- 9 requests from Public Health Units in Ontario for access to the Healthy Babies Healthy Children Screen
- 1 request from a Prescribed Entity (under PHIPA reg 329/04 s.18)
- 1 request under review (from First Nations Health Authority)

**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:**

Two (2) 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:**

No requests were granted.  
Two (2) requests were 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:**

No Research Agreement for the disclosure of personal health information was executed.

**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:**

409 requests received since the prior review by the Information and Privacy Commissioner of Ontario, as follows:

- 14 requests for the disclosure of de-identified information for research purposes
- Two (2) requests for the disclosure of de-identified information for purposes other than research
- 393 requests for the disclosure of aggregate information for research and other purposes

**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:**

The following agreements and acknowledgements were executed or received since the prior review by the Information and Privacy Commissioner of Ontario:

- Nine (9) research agreements executed for the disclosure of de-identified information
- Five (5) research agreements in progress for the disclosure of de-identified information
- Two (2) data sharing agreements executed for the disclosure of de-identified information for purposes other than research
- 213 acknowledgements received for the disclosure of aggregate information for research and other purposes
- 18 acknowledgements pending for the disclosure of aggregate information for research and other purposes
- 32 requests denied/unfulfilled for the disclosure of aggregate information for research and other purposes; requests denied/unfulfilled for reasons including but not limited to:
  - Request was an inquiry that was not formalized
  - Request has been deferred
  - Data quality did not meet needs of requestor
  - Timeline could not be met
- 130 acknowledgements not received; these aggregate data requests were granted but acknowledgement was not tracked; in 2016 BORN assigned new resources to the tracking of acknowledgements of all data requests to ensure follow up

## 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:**

226 collection data sharing agreements executed for the collection of personal health information since the prior review by the Information and Privacy Commissioner of Ontario. Of these data sharing agreements:

- 31 are new agreements with health information custodians from whom BORN began collecting personal health information
- 195 are renewed or amended agreements executed with health information custodians in order to continue collecting personal health information

### **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:**

17 data sharing agreements executed for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario.

## 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 since the prior review by the Information and Privacy Commissioner of Ontario.

## 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:**

16 data linkages approved as follows:

1. BORN – CIHI: Epidemiology, risk factors, and characterization of neonatal visits to Ontario emergency departments
2. BORN – CIHI: A population based comparison of obstetrical practices between France and Ontario
3. BORN – CIHI: Perinatal Health Indicators and Canadian Perinatal Surveillance System (CPSS) Labour algorithm validation

4. BORN – CIHI: Ontario Birth Centre Evaluation – indicators of morbidity not present in the BORN Information System
5. BORN – CIHI: BIS-CIHI record linkage for: validation of congenital anomalies data and live births
6. BORN – CIHI: Stillbirth rates, neonatal death and very preterm infant survival rates: a Canadian validation study
7. BORN – CIHI: Maternal morbidity in Ontario: A data quality validation exercise
8. BORN – CIHI: Risk of Perinatal Death in Singleton Pregnancies by Pre-Pregnancy Body Mass Index (BMI)
9. BORN – CIHI: BORN Data Quality Assurance Report (comparison of number of stillbirths and live births)
10. BORN – CIHI: Comparison of congenital anomaly rates between BORN Information System and CIHI
11. BORN – CIHI: Number of neural tube defects (excluding anencephaly) in Ontario and proportion that terminate
12. BORN – CIHI: Preterm Labour Diagnosis investigation
13. Neonatal Death Rates in Level of Care 2 Ontario Hospitals
14. BIS-NIPT: The introduction of non-invasive prenatal testing to the Ontario prenatal screening landscape: evaluating true test performance in the general population setting
15. BIS-cytogenetics/cytogenetics-non-invasive prenatal testing: Quality Assurance for prenatal screening and Enhancing of congenital anomalies capture
16. On-going linkage of the BORN Information System (BIS): the BORN Information System links records collected from various health information custodians to create a longitudinal profile

### 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 assessment completed on January 9, 2014.

The privacy impact assessment evaluated the following projects:

- Collection of PHI related to the Ontario 18-month well baby visit, an autism assessment tool, and fertility clinics
- Disclosure of pregnancy outcomes to fertility clinics (with patient consent)
- Protocol for follow-up testing for gestational diabetes
- Tracking number of unaccommodated midwifery clients
- Secure messaging within the BORN Information System
- Procurement of a provider registry by BORN



A brief description of each recommendation	The date and the manner in which each recommendation was addressed or is proposed to be addressed
1. BORN and CHEO should establish a mechanism through which the CHEO privacy function receives ongoing reporting regarding BORN, such as the implementation of the Privacy and Security Review Committee.	BORN Privacy Officer and CHEO Chief Privacy Officer have met three times informally and discussed the involvement of the CHEO CPO. CHEO CPO does not have responsibility for the BORN privacy program (an incorrect premise on which this PIA finding was based). The involvement of the CHEO CPO (frequency of attendance at meetings, etc) to be reviewed by the BORN Privacy and Security Review Committee (2017).
2. BORN should draft and execute agreement provisions for its disclosure of birth outcomes data to the CARTR Plus Fertility Clinics; these provisions should be included in an amendment to the DSA that BORN has executed with each clinic for collection of clinic data.	Amendments to the fertility data sharing agreements addressing this consented disclosure to be drafted and executed in 2017.
3. BORN should update its agreement with ABS to include appropriate privacy provisions that address its access to and handling of PHI, even if this access is only incidental.	Report to be moved from the MIS to the BORN Information System in 2017. MIS agreement contains sufficient protection for PHI although none was intended to be housed in it.
4. BORN should ensure that the procurement of provider data as part of a Provider registry product or service is governed by a data sharing agreement.	BORN will enter into a data sharing or information sharing agreement as appropriate prior to receiving a provider registry.
5. BORN should establish a plan to complete the revision and implementation of its privacy policies and procedures within the organization, using a risk-based approach to prioritize key areas of privacy risk that the privacy program can address, while also maintaining flexibility with regard to business needs.	The BORN Privacy Officer and Manager of Health Informatics work under the guidance of the policies and procedures and amend as necessary and as appropriate. Implementation of policies and procedures at the time of this PIA was as expected (in progress) and this PIA recommendation requires no further discussion. BORN's compliance and adherence to its many privacy and security policies is reviewed by the IPC every three years.
6. In its revisions to the privacy policies, BORN should ensure that it provides the appropriate level of detail in its procedures that address the use and disclosure of PHI under PHIPA s.49(1)(a).	BORN policy <i>P-12: Disclosure of Personal Health Information for Purposes Other Than Research</i> to be updated with more detail on the review, approval, and execution of a data sharing agreement in all cases where BORN discloses PHI to facilitate and improve the provision of health care. BORN was in the process of making this policy update during this PIA. Updated version of this policy followed in 2014. Draft internal policy available and followed from 2014.
7. BORN should update the application service provider privacy training so that it addresses the role as a service provider and the privacy obligations that are specific to that role.	The application service provider is a third-party service provider and BORN legal began drafting a new agreement in Feb 2016. As per policies, BORN is expected to have in place a third-party service provider agreement that follows an IPC approved template; the agreement in place with application service provider is stronger than the BORN template and legal is reviewing both, and working on a hybrid (due 2017). The need to provide privacy training is transferred to the application

	service provider under the agreement. BORN Privacy Officer has been to the application service provider twice to delivery privacy training in person.
8. BORN should investigate options for delivering self-administered privacy training to BIS users, to ensure that they are aware of their privacy obligations related to the use of the BIS.	BORN has addressed privacy expectations and responsibilities (outside of this finding) as follows: <ul style="list-style-type: none"> <li>• Every collection DSA clearly outlines the responsibility of the organization in choosing a local administrator for their instance of the BIS and outlines that their own privacy policies apply to their use of the BIS</li> <li>• Click-through agreement for BIS end users underway (started in Feb 2016; due in 2017)</li> <li>• BORN staff are in touch with sites and provide training with many privacy tips</li> <li>• BIS local admin user guide includes privacy suggestions</li> </ul>
9. BORN should use its research and business design activities to inform the revision of its policy on disclosures for purposes other than research; the policy should provide clarity regarding the conditions under which BORN will disclose to health care providers, and the procedures to be used in making the disclosure.	This type of disclosure is covered under PHIPA section 49.1.a in finding 6 above. Any disclosure of this type that BORN undertakes has to go through management, leadership, the Disclosure of PHI Committee, and is covered by a disclosure data sharing agreement. It also has to align with BORN purposes, which are approved by the IPC. BORN considers this recommendation already addressed.
10. In the event that BORN uses a provider registry product or service to process and enrich provider data in its data holdings, it should develop policies and procedures to ensure that the processing of the data does not lead to inaccuracies in the provider information.	This type of disclosure is covered under PHIPA section 49.1.a in finding 6 above. Any disclosure of this type that BORN undertakes has to go through management, leadership, the Disclosure of PHI Committee, and is covered by a disclosure data sharing agreement. It also has to align with BORN purposes, which are approved by the IPC. BORN considers this recommendation already addressed.
11. BORN should establish a retention and disposal schedule for the messages received and sent through the BIS messaging system.	Recommendation assigned to Manager of Health Informatics, Sr Technical Architect and BIS Systems Administrator on October 4, 2016. Decision to be taken by June 2017.
12. BORN should add a provision to its Privacy Inquiries policy indicating that while it will not fulfill access requests made by individuals, it will provide support to individuals in following up with their providers that have disclosed PHI to BORN.	BORN privacy training sets out that the BORN Privacy Officer can confirm to an enquirer that BORN holds their PHI and can let the enquirer know which HIC disclosed it to BORN. There is no IPC requirement in the policy on Privacy Inquiries that mandates these steps to be included. BORN considers this recommendation closed.
13. BORN should ensure that all breaches of PHI due to user error have been recorded as breaches in the BORN Privacy Breach Log so that they can be reviewed by the Privacy Officer to detect patterns of inadvertent or intentional breach.	BORN met with IPC March 7, 2013 to clarify that user errors are not tracked as breaches, as they represent anticipated human-machine interface issues. BORN tracks these incidents and reviews them periodically. This is also a documented risk on the BORN risk register. Incidents are reviewed and monitored.
14. The Privacy Officer should ensure that the recently completed Annual Auditing Plan is fully implemented as soon as possible.	Privacy Officer included details of privacy and security auditing in 2014 IPC triennial review of BORN as a prescribed registry.

15. BORN should enhance policies and procedures with control indicators and metrics that can be used to determine if they are effective and being followed.	Automation of many of BORN's privacy and security logs, including metrics, would be very beneficial to the Privacy Officer, as well as the Privacy and Security Review Committee. While automating some of this work has been discussed several times, and a tool has been investigated, there have been other priorities to address. This recommendation will remain open to be discussed periodically.
16. BORN should arrange for quarterly backup tapes to be archived off-site to a secure third-party storage facility.	Storage is offsite. Privacy Officer to update backup and restore policy (2017).
17. BORN/CHEO should implement specialist software and/or appliances (or use 3rd party monitoring services) that are able to perform complex log-analysis, event correlation, and detect the presence of Advanced Persistent Threats.	Committee feedback is that because the BIS resides on the private eHealth network, a dedicated intrusion detection system would provide limited benefit at high cost, at the moment. Along with the appliance you need someone to interpret the findings which can be a full time job. Committee suggests making this an evergreen item to be reviewed annually.

**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 privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner of Ontario.

Proposed date of completion: 2017

The scope of this privacy impact assessment includes:

- Ontario Perinatal Record changes
- Immunization “app”
- Pre-population of fields in the BORN Information System: data quality and burden of data entry
- Data cubes (for analytics)

**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 determined that the following two data collections did not require privacy impact assessments:

1. Capture of new prenatal screening test: Non-Invasive Prenatal Test (NIPT)

- BORN’s existing mandate includes the collection of prenatal screening data in Ontario. With the introduction of NIPT, existing pathways of care may change as women who screen positive through maternal multiple marker screening (MMMS) now have the option of NIPT prior to invasive prenatal diagnosis (e.g. amniocentesis). Capturing NIPT-related data in the BIS can dramatically increase the information available to providers and patients about the true value of this type of testing.
  - Collection data sharing agreements were put in place with health information custodians for the collection of this data into BORN and all applicable privacy policies and reviews were followed and/or conducted. This included approval by BORN’s Data Collection Review Committee, which undertook a review of all data elements (most of which are already approved for collection into BORN via the existing prenatal screening testing in Ontario) and the decision that a privacy impact assessment was not required.
2. Capture of cytogenetics data from prenatal screening labs in Ontario
- BORN has in place collection data sharing agreements with all prenatal screening labs in Ontario, in keeping with its mandate related to provincial prenatal screening quality assurance. These data sharing agreements were amended to expand the data collection to include cytogenetics data. BORN already had approval to collect most of the data elements; the change was with respect to collecting from prenatal screening labs, and the expansion of the collection by three new data elements (specimen number, date of sample, tissue type). This data is important for quality assurance of prenatal testing in Ontario, especially with the introduction of NIPT as noted above.
  - All applicable privacy policies and reviews were followed and/or conducted. This included approval by BORN’s Data Collection Review Committee, which undertook a review of the new data elements and the decision that a privacy impact assessment was not required.

**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:**

One (1) privacy impact assessment reviewed on October 7, 2016. This was the privacy impact assessment that was completed on January 9, 2014 (details in indicators above).

**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:**

Dates of audits of agents granted approval to access and use PHI since prior review by IPC	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
February 19, 2014	Verify audit logs of system activity by BORN System Administrator. No recommendations. All activity in line with expectations of BORN System Administrator role.
February 19, 2014	Verify BIS audit logs of system activity by BORN employee with access to PHI. No recommendations. All activity in line with expectations of BORN employee (agent) with access to PHI.
February 19, 2014	Re-verify access to maternal and newborn records of high profile birth mother and baby (original audit Oct. 2, 2013). No recommendations. No inappropriate access detected.
February 19, 2014	Re-verify access to maternal and newborn records of BORN employee (original audit Oct. 28, 2013). No recommendations. No inappropriate access detected.
February 19, 2014	Re-verify access to maternal and newborn records of BORN employee (original audit Oct. 28, 2013). No recommendations. No inappropriate access detected.
March 26, 2015	Verify that agent access to PHI was revoked when she left BORN. No recommendations from this audit as access had been correctly removed.
March 26, 2015	Verify that a BORN Agent's access to PHI was revoked when he left BORN. No recommendations from this audit as access had been correctly removed.
March 26, 2015	Verify that a contractor's reporting (back end) view-only access was revoked when she left BORN. No recommendations from this audit as access had been correctly removed.
March 26, 2015	Verify that a contractor's reporting (back end) view-only access was revoked when he left BORN. No recommendations from this audit as access had been correctly removed.
March 26, 2015	Verify that 2 previous BORN Agents' temporary access was revoked when they ceased to be BORN agents (enabled as agents, including privacy training, for testing). No recommendations from this audit as access had been correctly removed.
March 26, 2015	Verify that a BORN Agent's BIS access revoked when she left BORN. No recommendations from this audit as access had been correctly removed.
March 26, 2015	View audit logs of a BORN Agent (former employee) to ensure all BIS access was in line with expectations. No recommendations. All activity in line with expectations.
August 27, 2015	Verify BIS (live) audit logs of system activity by BORN coordinator (verify June 1, 2016 and August 27, 2016). No recommendations. All activity in line with expected access.
September 29, 2016	Verify access to maternal and newborn records of BORN employee. No recommendations. No inappropriate access detected.
September 30, 2016	Verify BIS (live) audit logs of system activity by BORN data analyst (verify June 30 - September 30, 2016). No recommendations. No inappropriate access detected.
September 30, 2016	Verify BIS (staging) audit logs of system activity by BORN data analyst (verify June 30 - September 30, 2016). No recommendations. All activity in line with expected access.
September 30, 2016	Verify BIS (live) audit logs of system activity by BORN Sr. Technical Analyst (verify Jan 30 - September 30, 2016). No recommendations.

September 30, 2016	Verify BIS (staging) audit logs of system activity by BORN Sr. Technical Analyst (verify Feb 24 - September 30, 2016). No recommendations.
September 30, 2016	Verify BIS (live) audit logs of system activity by BORN System Administrator (verify June 30 - September 30, 2016). No recommendations.
September 30, 2016	Verify BIS (staging) audit logs of system activity by BORN System Administrator (verify June 30 - September 30, 2016). No recommendations.

**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:**

20 other privacy audits were completed as follows:

The number and a list of all other privacy audits completed since the prior review by the Information and Privacy Commissioner of Ontario; date of completion of each audit		A description of the nature and type of 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
1	2014 IPC triennial review: Comparison of all BORN Policies and Procedures to IPC requirements as part of BORN's triennial review as a prescribed registry.	<p><b>Recommendation 1:</b> BORN to complete business continuity and disaster recovery plan and confirm this to IPC by June 1, 2015.</p> <p><b>Addressed:</b> BORN confirmed via e-mail to the IPC on June 15, 2015 that its plan was formally documented and implemented.</p> <p><b>Recommendation 2:</b> BORN to complete the revisions of its Policy and Procedure for Secure Disposal of Records of PHI in order that it comply with IPC requirements, as set out in the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities, on or before Oct 31, 2016.</p> <p><b>Addressed:</b> BORN re-reviewed policy which was more compliant to IPC requirements than initially noted; BORN added a timeline to receive certificate of destruction to policy; BORN updated compliance evidence in this document (see section III, Compliance to Appendix B).</p>
4	January 31, 2014 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.	No recommendations. Agreements were in place.

2	February 6, 2014 Audit a cross-section of collection data sharing agreements (71 agreements) to ensure all appear in P-18: Log of Data sharing Agreements	All agreements were correctly logged. <b>Recommendation:</b> use consistent terminology for data elements across all organizations and data sharing agreements. <b>Addressed:</b> throughout 2015 and 2016 when BORN renewed all collection data sharing agreements.
3	February 6, 2014 Audit a cross-section of collection data sharing agreements (71 agreements) to ensure PHI listed in agreement matches PHI coming into the BORN Information System.	Discrepancies noted in three agreements. <b>Recommendation:</b> review all DSA "schedules of PHI" when agreements are renewed to ensure consistency. <b>Addressed:</b> throughout 2015 and 2016 when BORN renewed all collection data sharing agreements.
5	February 28, 2014 Verify that three organizations contributing data to the BORN System are implementing sensitive user roles correctly.	<b>Recommendation:</b> work with one organization to decrease the number of sensitive user roles they had implemented. <b>Addressed:</b> number decreased from 41 users to seven users as of March 21, 2014.
6	February 19, 2014 Verify understanding of "super user" account by third party service provider that builds the BORN Information System (application service provider).	No recommendations. ASP verified and acknowledged use of account in line with BORN expectations.
7	2015 Review of the BORN collection data sharing agreement template prior to renewing agreements with all hospitals and midwifery practice groups. Review intended to ensure all parties aware of breach/liability responsibilities with respect to access to/use of BORN Information System.	<b>Recommendation:</b> add new articles to agreement to clarify data provider roles and responsibilities with respect to access to/use of BORN Information System. <b>Addressed:</b> in BORN 2015-16 DSA renewal exercise.
8	January 28, 2016 Verify audit logs for high-profile birth mother to ensure no snooping. Verified date range Dec 28, 2013 - Jan 28, 2016.	No recommendations. No inappropriate access detected.
9	January 28, 2016 Verify audit logs to birth records of a BORN employee to ensure no snooping. Verified date range Dec 28, 2013 - Jan 28, 2016.	No recommendations. No inappropriate access detected.
10	January 28, 2016 Verify access to newborn records of BORN employee. Verified date range Dec 28, 2013 - Jan 28, 2016.	No recommendations. No inappropriate access detected.
11	January 28, 2016 Verify access to maternal and newborn records of BORN employee (to ensure no snooping). Viewed history from Dec 28, 2013 - Jan 28, 2016.	No recommendations. No inappropriate access detected.

12	August 18, 2016 Audit of 36 disclosure data sharing agreements that require a signed Confidentiality Agreement for each user with access to BORN data covered under the agreement. E-mail audit requested review of users and confirmation that Confidentiality Agreements match list of data users.	No recommendations. All recipients reviewed list of users and removed access for those users no longer requiring access.
13	September 8, 2016 Audit of agreement log (P-18) to cross check that each logged entry has a printed agreement.	Noted one hospital agreement has lapsed. <b>Recommendation:</b> execute new collection data sharing agreement. <b>Addressed:</b> agreement in place Oct 5, 2016.
14	September 30, 2016 Audit report verified by all managers to review BORN agent roles/access to BIS and confirm on-going access/remove or edit access.	<b>Recommendation:</b> remove access for three agents and one third-party service provider; adjust access for five agents. <b>Addressed:</b> date implemented: Oct 11, 2016 by Sr. Technical Architect.
15	October 15, 2016 Review of all HR logs to ensure adherence to policies, procedures and business process. Review period: spring 2016 to fall 2016.	Audit identified that all HR logs (HR-02-04 Log of Attendance at Privacy/Security Training and HR-07 - Log of Executed Confidentiality Agreements) tracked appropriately, but with room for improvement. <b>Recommendation:</b> Improve communication between BORN privacy and BORN HR to ensure HR privacy activities documented in real time, eliminating need to "catch up". <b>Addressed:</b> October 15, 2016.
16	October 18, 2016 Ensure access to PHI systems terminated for two former BORN agents.	Three (3) recommendations resulted from this audit: 1) Managers to advise BORN HR when an employee is leaving 2) BORN HR to copy the privacy officer on all termination steps 3) BORN HR to monitor termination dates of contract employees Addressed in two ways: 1) All three (3) recommendations will be addressed during a meeting on November 7, 2016 with BORN Privacy team, HR and the Manager of Health Informatics. 2) Reminder of notice of termination process e-mailed to all managers, with required acknowledgement, on October 19, 2016 (all managers acknowledged).
17	October 24, 2016 Audit conducted to ensure Agent Data Access form in place for all BORN Agents with BIS access.	No recommendations. All agents with access to PHI had appropriate approved documentation in place.
18	October 25, 2016 Report verified by all managers to review BORN agent access to BORN PHI Drive and confirm on-going access/remove or edit access.	<b>Recommendation 1:</b> remove access for five agents. <b>Addressed:</b> Oct 26, 2016. <b>Recommendation 2:</b> review audit logs of access to BORN PHI Drive to ensure no inappropriate access. <b>Addressed:</b> Oct 26, 2016 (no inappropriate access). <b>Recommendation 3:</b> review steps for IS department to add members to BORN PHI drive. <b>Addressed:</b> Oct 26, 2016 via e-mail reminder to IS staff. <b>Recommendation 4:</b> further investigate control of enabling



		access to BORN PHI drive. <b>To be addressed:</b> Nov 18, 2016 meeting.
19	October 28, 2016 Verify audit report/list of all Family Health Teams contributing data to the BIS to ensure all have agreements in place and all agreements are tracked in DSA log (P-18).	No recommendations. All agreements in place and logged appropriately.
20	2014 - 2016 Audit all policies and procedures in the BORN Privacy and Security Management Plan to review effective implementation; amend as appropriate.	Audit resulted in the "Policy and Procedure Notes and Recommendations" that appears below this table.

### **Audit 20: Policy and Procedure Notes and Recommendations**

#### **General updates**

- The role of the CHEO Chief Privacy Officer as set out in BORN policies is under review. While the CHEO CPO is a noted member of the BORN Privacy and Security Review Committee, this is not followed in practice. The BORN Privacy Officer and the CHEO Chief Privacy Officer meet annually and will use the next annual meeting to discuss with BORN Privacy and Security Review Committee the committee mandate, governance structure at BORN, breach management protocol, privacy reports (with a view to redefining where the CHEO CPO's input and expertise fits within BORN).
- The BORN Privacy and Security Governance model will be updated to reflect current management at BORN (to ensure appropriate committee representation).

#### **P-02 and S-02: Ongoing Review of Privacy and Security Policies and Procedures**

- Policy calls for reviews annually or more frequently if necessary. BORN policies have been continually under review for more than two years as BORN continues to fully operationalize all aspects of its very detailed policies. Annual review, as set out in the policy, will begin in 2017.
- The precise steps for Leadership Team approval may be amended to note that the Privacy and Security Review Committee approves updates and Leadership Team is kept aware of changes.
- Procedure calls for a three-month review period; this time period may be adjusted.

#### **P-02 A: Annual and Quarterly Reports on Privacy and Security**

- BORN policy on privacy reports calls for quarterly and annual reports. This reporting timetable has been followed on an informal basis. BORN is currently finalizing three formal annual reports on privacy and security, and will update the mandated framework/content of the quarterly report (not all elements necessary on a quarterly basis).

**P-03: Transparency of Privacy Policies and Procedures**

- Reviewing mandated information for brochures (current list of elements to be included on brochures is too long).
- BORN does not currently publish to its website IPC review results and Privacy Impact Assessment summaries; these items to be updated on the website.

**P-04: Collection of Personal Health Information and P-06 Statements of Purpose for Data Holdings Containing Personal Health Information**

- Precise flow of decision points and approvals once the Privacy and Security Review Committee has approved a decision is under review. The policy sets out very specific steps for communication from and between Data Collection Review Committee, Privacy and Security Review Committee, and Leadership Team. All members of these committees are involved in approvals in practice and the precise order and flow of approvals to be updated as needed.
- Method by which Communications Lead is made aware of any necessary website changes is under review.

**P-08: Limiting Agent Access to and Use of Personal Health Information**

- Work underway to ensure policy and procedure reflect the BORN PHI drive (not just the BORN Information System).
- Review of the following procedure statement:  
All approved accesses and uses of Personal Health Information are subject to an expiry after one year or sooner based on request.  
The auto expiry feature in the BORN Information System is not universally set up. Currently reviewing need for policy update or enabling auto expiry.

**P-08 A: BORN PHI Access Request Form**

- Work underway to ensure the BORN PHI Drive is represented on this form.

**P-09: Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information**

- Work underway to ensure the BORN PHI Drive is represented by this log (BORN PHI Drive access tracked in another log to date).
- Work underway to update log fields to better reflect new roles and permissions set out in updated P-08: Limiting Agent Access to and Use of PHI.

**P-10: Use of Personal Health Information for Research**

- BORN has in place a research review committee that does much of the work assigned to the Privacy and Security Review Committee as described in the policy. Updates to be made as appropriate.
- Steps describing the Scientific Manager's formal approval letter to be updated. Scientific Manager provides approval but policy does not precisely reflect the method by which this approval is granted.

**P-25: Privacy Impact Assessments**

- Reviewing steps for formal and written approval by the BORN Leadership Team; likely to move to the Privacy and Security Review Committee with the Leadership Team informed of progress. Implementation of this is being looked at as BORN formalizes the privacy and security review committee.

- Privacy Impact Assessment summaries have not been posted to the BORN website to date, although it is BORN's intent to do this (where appropriate).

#### **P-27: Privacy Audits**

- Steps setting out the formal approval by Privacy and Security Review Committee and Leadership team to be updated to reflect certain levels and types of audits that do not require advanced approval.
- Timeline for reporting to Privacy and Security Review Committee and Leadership Team to be updated/increased depending on type or audit or finding.
- Formal annual advanced audit plans have not been prepared to date; no policy update expected as formal planning underway.

#### **P-29: Privacy Breach Management**

- The following line to be removed as it is not necessary:  
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.
- Policy steps and notification timelines to be updated with respect to the types of breaches BORN defines in its policy. Contravention of a privacy policy does not necessarily need the same level of communication timelines as a breach of personal health information, as an example of expected updates.

#### **P-31: Privacy Complaints**

- Work underway to provide more flexibility on requirement to provide monthly updates to BORN Director, Communications Lead, Leadership Team and BORN staff on any in-progress recommendations resulting from a complaint (may not always be necessary).

#### **S-03: Ensuring Physical Security of Personal Health Information**

- BORN has not verified implementation of the following step:  
CHEO security provides a list of agents with authorized access (audit list) and a list of all associated badge in/out activity (log) to the BORN System Hosting Provider Director annually. 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.
- This audit is schedule for February 16, 2017.

#### **S-07: Secure Transfer of Records of Personal Health Information**

- BORN has in place a third-party service provider agreement with the Ministry of Health and Long Term Care for use of the e-Health Ontario Health Information Access Layer (HIAL) to transfer secure personal health information from Family Health Teams to the BORN Information System. This successful transfer mechanism to be reflected in BORN's policy S-07: Secure Transfer of Records of PHI.

#### **S-10: System Control and Audit Logs**

- BORN is not formally compliant to the following line in this procedure: The Manager of Health Informatics is responsible for monitoring the logs on a monthly basis.

- BORN monitors/uses audit logs on a regular basis, sometimes more than monthly, and the formality of this step is being reviewed (to add more flexibility).
- This policy reflects the auditing capability of the BORN Information System and changes are underway to reflect the auditing capabilities of the BORN PHI Drive.

#### **S-15: Security Audits**

- Note that ethical hacking, vulnerability testing, and penetration testing are under review. While the policy and procedure is compliant to IPC requirements, these types of security auditing have not been implemented in an on-going way at BORN and are under review. There is much industry movement towards vulnerability assessments as an effective tool and decision point regarding the need for ethical hacking and penetration testing. These tests are complex and should be undertaken when they are expected to produce reliable results to inform security practices and decision making.

#### **S-17: Security Breach Management**

- Policy steps and notification timelines to be updated with respect to the types of breaches BORN defines in its policy. Contravention of a security policy does not necessarily need the same level of communication timelines as a breach that affects the confidentiality of information in BORN's custody and control.

#### **HR-01 and HR-03: Privacy and Security Training and Awareness**

- BORN delivers annual privacy and security training to all BORN Agents via an in-person training session. BORN Human Resources schedules training in advance of the session. Where a BORN Agent is unable to attend the in-person training session, the BORN Privacy Officer or designate ensures annual training is completed either via webinar or e-mail. This scheduling, and follow up for BORN Agents who are unable to attend training in person, will be reflected in a future version of the training policy. This will replace current detailed steps in the procedure stating that the BORN Privacy Officer provides two weeks' notice prior to training, and follows up with supervisors when an employee misses privacy training. BORN does not follow these steps.

#### **HR-05: Execution of Confidentiality Agreement by Agents**

- The policy sets out that Confidentiality Agreements are renewed annually on completion of annual privacy and security training. BORN provided verbal review and re-acknowledgement of the Confidentiality Agreement for two years, at annual privacy and security training, and conducted an e-mail review to track re-acknowledgement of the Confidentiality Agreement in another year. BORN has decided to continue with the e-mail re-acknowledgement of the Confidentiality Agreement for all BORN Agents and will update the procedure to reflect this.

#### **O-01 and O-02: Privacy and Security Governance and Accountability Framework**

- The BORN Privacy and Security Governance model will be updated to reflect current management at BORN (to ensure appropriate committee representation).
- Current policy calls for quarterly and annual reports on privacy and security, and that the annual report be published on the BORN website. BORN has informally approached quarterly reports to date. Annual reports have been prepared but not formally reviewed; three annual reports will be reviewed in the first quarter of 2017. BORN is moving to meet policy guidelines for quarterly reports and will evaluate this frequency and amend the policy if necessary. BORN intends to publish summaries of the annual reports on its website.

### **O-03: Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program**

- Committee Terms of Reference under review to ensure committee membership has appropriate cross-BORN representation.
- Privacy and Security Review Committee: BORN introduced formal meetings of the Privacy and Security Review Committee in September 2016. Committee met informally prior to this.
- Data Collection Review Committee will begin rotating annual review of currently collected data elements in 2017.

### **O-04: Corporate Risk Management Framework**

- Formal, regularly-scheduled meetings for risk management were introduced in May 2016. Risk management meetings were held informally prior to this and BORN is now fully implementing its policy and procedure on risk management. Steps for risk register approval likely to be amended.

### **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:***

No privacy breaches since the prior review by the Information and Privacy Commissioner of Ontario.

### **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 policy P-02 and S-02: Ongoing review of Privacy and Security Policies and Procedures notes that BORN undertakes a review of policies annually or more frequently, as follows:*

BORN Ontario undertakes a review of its privacy and security policies and procedures on an annual basis or more frequently if required. The purpose of a review is to determine whether amendments are needed or whether new policies and procedures are required to ensure that BORN Ontario meets or exceeds industry standards and best practices.

*To date, BORN has performed reviews of its policies and procedures more frequently than a single annual review.* BORN security policies have been reviewed (all policies) on an on-going basis since 2014. The goal of this review is to verify implementation of all policies and procedures and make any amendments necessary.

The review process was conducted as follows:

*Summer 2013 – Fall 2016*

All policies and procedures in the BORN Privacy and Security Management Plan were reviewed by subject matter experts and by end users. This on-going review was to solidify the operationalization of BORN policies and procedures, monitor their implementation and make any further updates on an on-going basis. BORN has been fine-tuning policy and procedure details since it first implemented all policies and procedures in 2012, when the BORN Information System was introduced. Review results and updates were captured in sequential drafts of the BORN Privacy and Security Management during

this time. The result of this review will enable BORN to move to an efficient annual review of policies and procedures.

Members of BORN's Privacy and Security Review Committee were involved in many of the individual policy reviews and updates. On October 24, 2016, the BORN Privacy Officer sent a detailed publication history recapping all changes to policies and procedures to members of this committee. All changes were accepted.

**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 and description of security policy amendments as a result of the on-going review:

**S-01: Information Security Policy**

- Added the word "unauthorized" to section prohibiting copying, modification and disposal. Updated "most responsible person" for policy from Privacy Officer to Privacy Officer and Manager of Health Informatics
- Clarified that the Manager of Health Informatics is responsible for oversight of the information security program
- Reviewed and updated policy references to better reflect related policies
- Clarified that second-factor authentication is mandatory for system administrators (removed specificity that RSA tokens are used as the goal is to mandate second factor authentication rather than brand)

**S-03: Ensuring Physical Security of Personal Health Information**

- Updated the levels of secure access to the main data centre from three to four and described fourth
- Edited/rearranged content of procedure for clarity. Organized content into physical security for access to main BORN offices, access to the main data centre, access by visitors, added a visitor log for main BORN premises, removed the need for the visitor log to BORN main offices based on further procedural review (visitors to the BORN premises are supervised; BORN does not issue temporary badges)
- Clarified that visitors to the BORN data centre must sign a log and be supervised at all times by the BORN System Hosting Provider
- Clarified roles: BORN HR manages process for badges to main building, CHEO IT resource manages access to server room; clarified different processes for loss of badge for main BORN building, key to office in main BORN building, and badge to data centre
- Updated the HR steps and HR responsibility for retrieving badges and keys upon termination (original policy placed responsibility for badges and keys on Privacy Officer)
- Added a step to "whom to notify if you lose your badge"
- Clarified that de-activating a badge to the BORN main premises (if it is lost) involves notice to both CHEO and The Ottawa Hospital as BORN rents space from The Ottawa Hospital and full deactivation requires notice to both organizations
- Changed all references from "swipe" cards to "HID" (different technology; better security)

**S-04: Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity**

- Removed columns for temporary badges (granted and returned) as BORN does not grant temporary badges
- Removed "nature of access" as this applies to a building with various levels of security. BORN work premises do not contain any Personal Health Information on site. There are separate logs for BORN work premises (no PHI) and the BORN data centre (all PHI)

#### **S-05: Secure Retention of Records of Personal Health Information**

- Ensured all references to paper records of PHI removed (BORN prohibits paper records of PHI)
- Updated "most responsible person" for policy from Privacy Officer to Privacy Officer and Manager of Health Informatics
- Clarified that the standard data retention period of 28 years is noted in all BORN collection data sharing agreements
- Removed section on third party service provider that included the BORN System Hosting Provider (BORN does not contract hosting of data to a third party; the BORN System Hosting Provider is a BORN Agent and not a third-party service provider)
- Reflected in list of safeguards that all BIS data is collected pursuant to a data sharing agreement as per policy P-16: Data Sharing Agreements
- Added the BORN PHI Drive to the procedure, including a list of what types of data are retained on this drive, and what safeguards are in place

#### **S-06: Secure Retention of Records of Personal Health Information on Mobile Devices**

- Added that retention of records of PHI on mobile devices may be granted for research or facilitating and improving the provision of health care (previously noted that mobile use was only for research)
- Removed the reference to "when records are being disclosed" because records of PHI are never disclosed on mobile data
- Updated reference to secure passwords (six characters not eight)
- 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-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)
- Added direct statement that BORN agents are not permitted to transfer PHI by e-mail
- Removed note that where secure FTP is not possible BORN will use an encrypted hard drive
- Re-organized procedure into clear sections on: secure transfer out of BORN; secure transfer of aggregate data out of BORN and acknowledging receipt of data; secure transfer into BORN; secure transfer between prescribed registry and prescribed entity
- Clarified that steps outlining mandatory use of BORN's secure FTP to transfer data out of BORN apply to de-identified data
- Clarified that transferring aggregate data out of BORN may be done by e-mail, with password protection as applicable, and that all transfers of this type must be logged on the Data Tracking Log, include mandatory acknowledgement by the recipient, and that the e-mail must contain the following boiler plate information:

*This message, including any attachments, contains confidential information and is for the sole*



*use of the intended recipient(s). Any unauthorized use, disclosure or distribution is prohibited. If you are not the intended recipient, please notify the sender immediately and destroy the original message. The intended recipient of this message will not use the information, either alone or with other information, to attempt to identify or re-identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.*

#### **S-08: Secure Disposal of Records of Personal Health Information**

- Added more detail regarding when records of PHI may need to be destroyed, contacting the Privacy Officer regarding secure destruction
- Updated to clarify that paper records of PHI are not permitted and what steps should be taken if a paper record of PHI were found
- Clarified that BORN agents must contact the privacy officer re secure destruction of data for direction
- Clarified steps on mandatory certificates of destruction
- Edited (to improve clarity) steps for destruction of electronic records of PHI and PHI on mobile media

#### **S-08B: Certificate of Destruction of Personal Health Information**

- Updated the definition of secure destruction to be consistent with definition in Research Agreement (definitions were similar but not the same)
- Added clarification that certificates of destruction must be produced within a month of the actual destruction

#### **S-09: Passwords**

- Updated the minimum password length from eight characters to six characters, which correctly reflects the BORN System
- Clarified that request for a BIS password is sent to the BORN System Administrator by the Privacy Officer (not the Manager of Health Informatics)
- Updated references to include P-08A: BORN PHI Access Request Form, and that the Privacy Officer and Manager of Health Informatics follow this policy in association with P-08: Limiting Agent Access to and Use of Personal Health Information, P-08A: BORN PHI Access Request Form, and P-09: Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information
- Significant review, edit and updates after an in-depth review by Privacy Officer, Manager of Health Informatics and Senior Technical Architect. All IPC requirements continue to be met and procedure better reflects practices in place

#### **S-10: System Control and Audit Logs**

- Updated "most responsible person" for policy from Privacy Officer to Privacy Officer and Manager of Health Informatics
- Removed "Source Network Address" from list of fields in a system control audit report
- Edited terminology of audit events for accuracy: changed "date and time of disconnection and nature of disconnection" to "Date and time of user sign off or system automatic disconnect at 15 minutes of inactivity"

#### **S-11: Patch Management**

- Updated "most responsible person" for policy as follows:  
Removed Privacy Officer, added Manager of Health Informatics and Senior Technical Architect

- Edited and revised significantly by Privacy Officer, Manager of Health Informatics, BORN System Hosting Provider, Senior Technical Architect, BORN System Administrator to ensure alignment between IPC requirements and BORN operations
- Included an in-depth review of S-12 Change Management to ensure a clear division (no overlap) between the two policies; review updates include:
  - Clarification that S-11 Patch Management is restricted to operating system patches and other hosting system upgrades, and S-12 Change Management addresses patches from Application Service Providers for custom-developed solutions
  - Reviewed and revised all phases of patch lifecycle: notice of patches, determination that a patch should be applied, procedure for testing, roles and responsibilities and communication between them, testing, documentation

#### **S-12: Change Management**

- Updated "most responsible person" for policy from Privacy Officer to Privacy Officer and Manager of Health Informatics
- Edited and revised significantly by Privacy Officer and Manager of Health Informatics to ensure alignment between IPC requirements and BORN operations
- Included an in-depth review of S-11 Patch Management to ensure a clear division (no overlap) between the two policies; review updates include:
  - Clarification that S-11 Patch Management is restricted to operating system patches and other hosting system upgrades, and S-12 Change Management addresses patches from Application Service Providers for custom-developed solutions
  - Removed all reference to S-12A Log of Change Requests and S-12B Change Request Form as these are not used and/or needed. BORN uses the change management system of the Application Service Provider to manage, review, and approve all aspects of change management with respect to the BORN Information System
  - Reviewed and revised all phases of change management lifecycle: Submitting a Change Request, Review of Change Requests, Implementing a Change Request, Testing a Change Request, Deploying a Change Request to the Live System

#### **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
- Updated policy to note that systematic backup and recovery of back up tapes includes testing
- Updated frequency of testing from monthly to "as necessary, minimally twice per year"
- Removed names of some specific tools and replaced with generic tool types (backup system rather than the tool BORN has selected)

#### **S-14: Acceptable Use of Technology**

- Updated roles and responsibilities to both Privacy Officer and Manager of Health Informatics
- Clarified that remote access to applications and resources is initiated via the CHEO remote access control

#### **S-15: Security Audits**

- Updated roles and responsibilities to reflect appropriate involvement of both Privacy Officer and Manager of Health Informatics
- Added to the list of "types of security audits" that BORN audits compliance to security policies and procedures

- Note that ethical hacking, vulnerability testing, and penetration testing are under review. While the policy and procedure are compliant to IPC requirements, these types of security auditing have not been implemented in an on-going way at BORN and are under review. There is much industry movement towards vulnerability assessments as an effective tool and decision point regarding the need for ethical hacking and penetration testing. These tests are complex and should be undertaken when they are expected to produce reliable results to inform security practices and decision making
- Updated frequency of the Log of Security Audits being forwarded to the Privacy and Security Review Committee from monthly to quarterly

#### **S-17: Security Breach Management**

- Updated roles and responsibilities to reflect appropriate involvement of both Privacy Officer and Manager of Health Informatics
- Removed references to breaches being tracked in the CHEO IS Vector form. BORN tracks breaches on S-19 Log of Information Security Breaches and provides updates in Privacy and Security Reports including any breach-related recommendations and the status of their implementation
- Updated contact information for Manager of Health Informatics

#### **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:**

An updated draft of the BORN Privacy and Security Management Plan was e-mailed to all BORN Agents by the Privacy Officer on October 28, 2016.

#### **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:**

No external communications or updates have been made as a result of this review. The privacy policies on the BORN website will be updated within one month of approval of the BORN Privacy and Security Management Plan.

### **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, September 30, 2016

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:*

No recommendations.

*The date each recommendation was addressed or is proposed to be addressed.*

No recommendations.

*The manner in which each recommendation was addressed or is proposed to be addressed:*

No recommendations.

**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:**

The dates of the review of system control and audit logs since the prior review by the Information and Privacy Commissioner of Ontario	A general description of the findings, if any, arising from the review of system control and audit logs
February 19, 2014 Verify use of super user account used by third party service provider that builds the BORN system. View six month period of user activity.	No recommendations. All activity in line with expected use of this account.
February 19, 2014 Verify BIS audit logs of system activity by BORN System Administrator.	No recommendations. All activity in line with expected use of this account.
February 19, 2014 Verify BIS audit logs of system activity by BORN employee with access to PHI.	No recommendations. All activity in line with expected use of this account.
February 19, 2014 Re-verify access to maternal and newborn records of high profile birth mother and baby (original audit Oct. 2, 2013).	No recommendations. All activity in line with expected use of this account.

February 19, 2014 Re-verify access to maternal and newborn records of BORN employee (original audit Oct. 28, 2013).	No recommendations. All activity in line with expected use of this account.
February 19, 2014 Re-verify access to maternal and newborn records of BORN employee (original audit Oct. 28, 2013).	No recommendations. All activity in line with expected use of this account.
March 26, 2015 Verify that agent access to PHI was revoked when she left BORN.	No recommendations.
March 26, 2015 Verify that a BORN Agent's access to PHI was revoked when he left BORN.	No recommendations.
March 26, 2015 Verify that a contractor's reporting (back end) view only access was revoked when she left BORN.	No recommendations.
March 26, 2015 Verify that a contractor's reporting (back end) view only access was revoked when he left BORN.	No recommendations.
March 26, 2015 Verify that 2 previous BORN Agent's temporary access was revoked when they ceased to be BORN agents (enabled as agents, including privacy training, for testing).	No recommendations.
March 26, 2015 Verify that a BORN Agent's BIS access revoked when she left BORN.	No recommendations.
March 26, 2015 View audit logs of a BORN Agent (former employee) to ensure all BIS access was in line with expectations.	No recommendations.
August 27, 2015 Verify BIS (live) audit logs of system activity by BORN coordinator (verify June 1, 2016 and August 27, 2016).	No recommendations.
September 29, 2016 Verify access to maternal and newborn records of BORN employee.	No recommendations. No inappropriate access detected.
September 30, 2016 Verify BIS (live) audit logs of system activity by BORN data analyst (verify June 30 - September 30, 2016).	No recommendations. No inappropriate access detected.
September 30, 2016 Verify BIS (staging) audit logs of system activity by BORN data analyst (verify June 30 - September 30, 2016).	No recommendations. All activity in line with expected access.
September 30, 2016 Verify BIS (live) audit logs of system activity by BORN Sr. Technical Analyst (verify Jan 30 - September 30, 2016).	No recommendations.
September 30, 2016 Verify BIS (staging) audit logs of system activity by BORN Sr. Technical Analyst (verify Feb 24 - September 30, 2016).	No recommendations.

September 30, 2016 Verify BIS (live) audit logs of system activity by BORN System Administrator (verify June 30 - September 30, 2016).	No recommendations.
September 30, 2016 Verify BIS (staging) audit logs of system activity by BORN System Administrator (verify June 30 - September 30, 2016).	No recommendations.
September 30, 2016 Verify BIS (staging) audit logs of system activity by BORN employee with access to PHI (verify June 30 - September 30, 2016).	No recommendations.
October 18, 2016 Ensure access to PHI terminated for two former BORN agents.	Three (3) recommendations resulted from this audit: 1) Managers need to advise BORN HR when an employee is leaving 2) BORN HR needs to copy the privacy officer on all termination steps 3) BORN HR needs to better track employees All three (3) recommendations will be addressed during a meeting on Oct 28, 2016 with the Privacy team, the BORN admin staff who are responsible for HR activities and the Manager at BORN who is responsible for HR. Reminder of notice of termination process e-mailed to all managers, with required acknowledgement, on October 19, 2016.
October 25, 2016 Verify BORN PHI Drive audit logs of system access by three users (viewed access between October 12 - 27, 2016).	Recommendation: no findings; view longer history. Meeting November 18, 2016.

**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:**

	The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario	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
1	February 2014 Audit BORN log: S-06B Log of Agent use of mobile Devices/Remote Access	No recommendation. Log up to date.
2	February 2014 Threat and risk assessment on: Using e-Health Ontario's Health Information Access Layer to transmit PHI from primary care EMRs to BORN). Reviewing transfer of PHI via "app"	<p><b>Recommendation:</b> ensure 3rd party vendors perform due diligence on supplied code. <b>Addressed:</b> to be explicitly included in list of project deliverables on all future projects.</p> <p><b>Recommendation:</b> BORN should identify the impact associated with ingestion of false or erroneous information and adopt a suitable strategy to address such information. <b>Addressed:</b> periodic evaluations look at data quality. The next version of the application requires public health units to vet the data before it is moved into BORN.</p> <p><b>Recommendation:</b> BORN should train users on best practices in security. <b>Addressed:</b> a new BORN Information System acceptable use policy will reminds users to consult local applicable policies regarding access to and use of PHI (2017). BORN has also strengthened its DSAs to clarify responsibilities of end users and their organizations re access to the BIS. DSAs in place in 2015 and 2016.</p> <p><b>Recommendation:</b> review public facing training materials to ensure no security insights are present. <b>Addressed:</b> the materials have been reviewed and do not contain any security information.</p> <p><b>Recommendation:</b> audit security technical configuration for internet connected devices. <b>Addressed:</b> the next version of agreement with Hosting Service Provider will contain explicit audit requirements (2018 contract).</p> <p><b>Recommendation:</b> develop a consistent method to enforce user password resets. <b>Addressed:</b> a new VPN solution has been procured and installation is expected by end of 2016 to ensure VPN</p>

		<p>users passwords reset the same way eHealth network users do.</p>
		<p><b>Recommendation:</b> perform Penetration test on application's internet facing components.  <b>Addressed:</b> while the BORN policy and procedure is compliant to IPC requirements and includes penetration testing, these types of security audits are not implemented in an on-going way at BORN and are under review. There is much industry movement towards vulnerability assessments as an effective tool and decision point regarding the need for ethical hacking and penetration testing. These tests are complex and should be undertaken when they are expected to produce reliable results to inform security practices and decision making.</p> <p><b>Recommendation:</b> validate data before importing into BIS.  <b>Addressed:</b> periodic evaluations look at data quality. The next version of the application requires public health units to vet the data before it is moved into BORN.</p> <p><b>Recommendation:</b> develop a strategy to test for exploitable vulnerabilities associated with all application components.  <b>Addressed:</b> if a decision is made to take the application out of pilot, a strategy will be developed for VA testing prior to provincial/national rollout.</p> <p><b>Recommendation:</b> input data should be validated before being transmitted to prevent potential exploits.  <b>Addressed:</b> if a decision is made to take Immunize out of pilot, a strategy will be developed for data input validation testing standards prior to provincial/national rollout.</p> <p><b>Recommendation:</b> develop a risk register to document relevant risks, vulnerabilities and associated recommendations.  <b>Addressed:</b> Risk Management policy and procedure and risk register have been formalized and all historical audits are being reviewed and added as applicable.</p>



		<p><b>Recommendation:</b> BORN needs to ensure that app maker is aware that:</p> <p>1) they are solely responsible for security related breaches arising from use of their software; and</p> <p>2) they needs to conduct appropriate security due diligence exercises (e.g. TRA, vulnerability testing, etc) on their software.</p> <p><b>Addressed/comment:</b> This is not BORN's responsibility. Agreements with maker of the application detail responsibilities. No finding.</p>
3	November 2015 Threat and risk assessment on Healthy Babies Healthy Children screening tool.	A draft of this audit has been submitted and will be reviewed in January 2017 along with a project evaluation. None of the recommendations have been finalized at this time.
4	September 30, 2016 Site visit to CHEO System Hosting Provider to audit compliance to BORN Security Policy S-03: Ensuring Physical Security of Personal Health Information.	No recommendations.
5	October 4, 2016 Audit of Log S-04 to ensure agents granted access to the premises have a documented HR status with BORN and an on-going need for a badge to the premises.	<p><b>Recommendation:</b> update log rather than track log contents in various files.</p> <p><b>Addressed:</b> Oct 17, 2016.</p>

**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:**

No security breaches since the prior review by the Information and Privacy Commissioner of Ontario.

**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:**

- 56 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:**

*2013-14 ongoing organizational privacy/security training*

- There were 70 BORN agents in 2013-14:
  - 54 agents attended organizational privacy/security training
  - 16 agents did not attend organizational privacy/security training. Of these 16 agents:
    - 3 agents joined BORN after date of annual training; all received initial privacy/security orientation
    - 2 agents were on maternity leave
    - 1 agent left BORN before the annual privacy/security training
    - 1 agent had received initial privacy and security orientation within the same year
    - 1 agent was on secondment to another organization
    - 7 agents are CHEO IS employees (also BORN agents for BORN Helpdesk services); CHEO IS employees attend mandatory CHEO privacy training every two years
    - 1 agent did not attend ongoing privacy/security training

*2014-15 ongoing organizational privacy/security training:*

- There were 75 BORN agents in 2014-15:
  - 60 agents attended organizational privacy/security training
  - 15 agents did not attend organizational privacy/security training. Of these 15 agents:
    - 3 agents joined BORN after the organizational training was delivered; all received initial privacy/security orientation
    - 3 agents did not attend annual privacy/security training
    - 9 agents left BORN before the ongoing organizational training was delivered; all received initial privacy/security orientation

*2015-2016 on-going organizational privacy/security training:*

- There were 78 BORN agents in 2015-16:
  - 61 agents attended or received organizational privacy/security training
  - 17 agents did not attend organizational privacy/security training. Of these 17 agents:
    - 13 agents joined BORN after the organizational training was delivered; all received initial privacy/security orientation
    - 1 agent was on maternity leave

- 3 agents left BORN before the ongoing organization training was delivered, but all received initial privacy/security orientation

**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:**

22 privacy communications by BORN to agents since the prior review by the Information and Privacy Commissioner of Ontario as follows:

1. 23-May-14  
As part of annual privacy and security training, the Privacy Officer gave additional updates:
  - Privacy skits performed by volunteer BORN Agents to demonstrate good privacy/security habits vs bad privacy/security habits
  - Review of BORN "Seven Habits of Highly Private People"
2. 3-Jul-14  
The Privacy Officer provided the team with an update on the BORN CASL subscription (in weekly BORN staff e-mail).
3. 24-Jul-14  
Privacy Officer provided the team with an update on the status of the IPC triennial review process (in weekly BORN staff e-mail).
4. 15-Jul-14  
Privacy Officer e-mailed a correction to all staff regarding a BORN BUZZ recommendation for an online password management tool; BORN has not evaluated and does not endorse this tool.
5. 1-Sep-14  
At a BORN staff conference, the Privacy Officer gave presentation on current status of privacy office, including an update on meeting with other privacy officers from prescribed registries and entities, and a review of BORN breach/suspected breach protocol and containment measures.
6. 5-Nov-14  
The BORN Director shared that the IPC triennial review was complete (in weekly BORN staff e-mail).
7. 13-Nov-14  
Privacy Officer provided the team with an update on work underway in the privacy department (at monthly staff meeting).
8. 15-Jan-15  
Privacy Officer posted the following articles on Yammer:
  - Tips on how to monetize health data (IAPP)
  - Hospital privacy violations that go unreported (Toronto Star)
9. 29-Jan-15  
Privacy Officer posted an update on CASL with links to more information on CASL (in weekly BORN staff e-mail).
10. 26-Mar-15  
Privacy Officer provided the team with an update on privacy infrastructure and privacy projects (at monthly staff meeting).
11. 1-Apr-15

- Privacy Officer posted a link to an article with respect to balancing privacy with access to health and health related data from the Council of Canadian Academies (in weekly BORN staff e-mail).
12. 7-Aug-15  
Privacy Officer posted a privacy update in the BORN BUZZ on the implementation of a new log for tracking internal use of PHI (in weekly BORN staff e-mail).
  13. 29-Oct-15  
In addition to annual privacy and security mandatory training Privacy Officer spent time on the "need to know" principle, the "limiting principle", a review of BORN statements of purpose.
  14. 3-Dec-15  
Privacy Officer provided a link to the results of a survey on data sharing, protection and analytics in the healthcare (in weekly BORN staff e-mail).
  15. 10-Dec-15  
Privacy Officer provided the team with a report on the 2015 PHIPA Privacy Summit as well as a reminder to lock workstations when they are unattended (in weekly BORN staff e-mail).
  16. 2-Mar-16  
Privacy Officer gave an update on privacy work underway at BORN (at monthly staff meeting).
  17. 6-Apr-16  
Privacy Officer gave an update on privacy work underway at BORN (at monthly staff meeting).
  18. 18-Aug-16  
Privacy Officer sent an e-mail communication to all BORN staff entitled "BORN Privacy Quick Reference for Handling PHI." Quick Reference handout highlighted key elements from privacy and security training as well as key reminders from commonly-used privacy and security policies, with an emphasis on secure retention, logging, privacy do's and don'ts.
  19. 5-Oct-16  
Update in the BORN Buzz weekly staff newsletter. Shared seven breach articles from newspapers and issued reminder to staff to follow all privacy and security policies and procedures and treat all registry data with respect (in weekly BORN staff e-mail).
  20. 17-Oct-16  
Privacy Officer sent an e-mail to all BORN staff thanking them for on-going help related to the IPC triennial review and a reminder that with two weeks left before the IPC report must be filed, all questions related to the IPC report should be prioritized.
  21. 19-Oct-16  
Privacy Officer e-mailed all managers to remind them of the need to notify BORN HR two weeks in advance of any termination dates. Included steps from BORN HR policy on termination and cessation.
  22. 28-Oct-16  
BORN Privacy Officer sent an updated DRAFT version of the BORN Privacy and Security Management Plan to all BORN Agents.

### **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:**

- 56 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:**

*2013-14 ongoing organizational privacy/security training*

- There were 70 BORN agents in 2013-14:
  - 54 agents attended organizational privacy/security training
  - 16 agents did not attend organizational privacy/security training. Of these 16 agents:
    - 3 agents joined BORN after date of annual training; all received initial privacy/security orientation
    - 2 agents were on maternity leave
    - 1 agent left BORN before the annual privacy/security training
    - 1 agent had received initial privacy and security orientation within the same year
    - 1 agent was on secondment to another organization
    - 7 agents are CHEO IS employees (also BORN agents for BORN Helpdesk services); CHEO IS employees attend mandatory CHEO privacy training every two years
    - 1 agent did not attend ongoing privacy/security training

*2014-15 ongoing organizational privacy/security training:*

- There were 75 BORN agents in 2014-15:
  - 60 agents attended organizational privacy/security training
  - 15 agents did not attend organizational privacy/security training. Of these 15 agents:
    - 3 agents joined BORN after the organizational training was delivered; all received initial privacy/security orientation
    - 3 agents did not attend annual privacy/security training
    - 9 agents left BORN before the ongoing organizational training was delivered; all received initial privacy/security orientation

*2015-2016 on-going organizational privacy/security training:*

- There were 78 BORN agents in 2015-16:
  - 61 agents attended or received organizational privacy/security training
  - 17 agents did not attend organizational privacy/security training. Of these 17 agents:

- 13 agents joined BORN after the organizational training was delivered; all received initial privacy/security orientation
- 1 agent was on maternity leave
- 3 agents left BORN before the ongoing organization training was delivered, but all received initial privacy/security orientation

**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:**

11 privacy communications by BORN to agents since the prior review by the Information and Privacy Commissioner of Ontario as follows:

1. 23-May-14  
As part of annual privacy and security training, the Privacy Officer gave additional updates:
  - Privacy skits performed by volunteer BORN Agents to demonstrate good privacy/security habits vs bad privacy/security habits
  - Review of BORN "Seven Habits of Highly Private People"
2. 15-Jul-14  
Privacy Officer e-mailed a correction to all staff regarding a BORN BUZZ recommendation for an online password management tool; BORN has not evaluated and does not endorse this tool.
3. 1-Sep-14  
At a BORN staff conference, the Privacy Officer gave presentation on current status of privacy office, including an update on meeting with other privacy officers from prescribed registries and entities, and a review of BORN breach/suspected breach protocol and containment measures.
4. 15-Jan-15  
Privacy Officer posted the following articles on Yammer:
  - Tips on how to monetize health data (IAPP)
  - Hospital privacy violations that go unreported (Toronto Star)
5. 1-Apr-15  
Privacy Officer posted a link to an article with respect to balancing privacy with access to health and health related data from the Council of Canadian Academies (in weekly BORN staff e-mail).
6. 29-Oct-15  
In addition to annual privacy and security mandatory training Privacy Officer spent time on the "need to know" principle, the "limiting principle", a review of BORN statements of purpose.
7. 10-Dec-15  
Privacy Officer provided the team with a report on the 2015 PHIPA Privacy Summit as well as a reminder to lock workstations when they are unattended (in weekly BORN staff e-mail).
8. 18-Aug-16  
Privacy Officer sent an e-mail communication to all BORN staff entitled "BORN Privacy Quick Reference for Handling PHI." Quick Reference handout highlighted key elements from privacy and security training as well as key reminders from commonly-used privacy and security policies, with an emphasis on secure retention, logging, privacy do's and don'ts.

9. 5-Oct-16  
Update in the BORN Buzz weekly staff newsletter. Shared seven breach articles from newspapers and issued reminder to staff to follow all privacy and security policies and procedures and treat all registry data with respect (in weekly BORN staff e-mail).
10. 19-Oct-16  
Privacy Officer e-mailed all managers to remind them of the need to notify BORN HR two weeks in advance of any termination dates. Included steps from BORN HR policy on termination and cessation.
11. 28-Oct-16  
BORN Privacy Officer sent an updated DRAFT version of the BORN Privacy and Security Management Plan to all BORN Agents.

### 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 and details were reported with the last IPC triennial review. Following this, BORN initiated a verbal re-acknowledgement of Confidentiality Agreements for two years, as follows:

- 2013 - 2014: BORN implemented verbal re-acknowledgement of Confidentiality Agreements as part of organizational privacy and security training
- 2014 - 2015: BORN implemented verbal re-acknowledgement of Confidentiality Agreements as part of organizational privacy and security training

In the 2015-2016 year, BORN returned to mandatory re-acknowledgement of the BORN Confidentiality Agreement via e-mail. Of the 76 BORN agents covering the period from Nov 1, 2015 to Oct 31, 2016 all agents have re-acknowledged their BORN Confidentiality Agreement.

#### **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:**

28 termination notices were received from full-time BORN agents who terminated their employment with BORN Ontario.

13 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 corporate risk register was reviewed on the following dates:

- 27-Mar-14
- 1-Jun-14
- 25-May-16
- 17-Aug-16
- 22-Sep-16
- 27-Sep-16
- 27-Sep-16
- 6-Oct-16

**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:**

The following discussions and/or amendments occurred at the review meetings:

- 27-Mar-14  
Meeting between Privacy Officer, Manager of Health Informatics and Scientific Manager to review BORN risk management policy, rating system, further formalizing BORN policy to risk management (BORN has in place a very strong policy that has been informally followed).
- 1-Jun-14  
Meeting to address some risk management items/vulnerabilities as a result of the Rouge Valley birth records breach in May/June 2014.
- 25-May-16  
Privacy Officer and Manager of Health Informatics met to review risk management at BORN; formalized schedule of meetings put in place.
- 17-Aug-16  
Privacy Officer and Manager of Health Informatics updated risks related to Internet browsers and user errors.
- 22-Sep-16  
Privacy Officer and Manager of Health Informatics updated risks related to power loss, communication loss, data integrity loss, data loss.



- 27-Sep-16  
Privacy Officer and Manager of Health Informatics updated risks related to abuse of access privilege by employees, natural disasters and computer viruses.
- 27-Sep-16  
Privacy Officer presented risk management updates to Privacy and Security Review Committee.
- 6-Oct-16  
Privacy Officer and Manager of Health Informatics updated risks related to system failure, theft or destruction of system assets, unauthorized system access by outsider (hacking).

### **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:**

The business continuity and disaster recovery plan was tested on the following dates (since the prior review by the Information and Privacy Commissioner of Ontario):

1. Backup and restore tapes tested on the following dates:
  - Apr 25, 2013
  - Jun 4, 2013
  - Sep 17, 2013
  - Nov 5, 2013
  - Jun 24, 2014
  - Aug 16, 2014
  - Dec 3, 2014
  - Feb 5, 2015
  - Apr 22, 2015
  - Jul 28, 2015
  - Dec 7, 2015
  - Jul 19, 2016
2. CHEO conducted a digital earthquake preparedness exercise on October 20, 2016.

Actual incidents occurred on January 2, 2014 and July 8, 2016.

**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:**

The following amendments were made to the CHEO IT Disaster Recovery Policy after the January 2, 2014 incident:

- Code Grey IS policy and process implemented, setting out new timelines and response checklists for severe outages to a mission critical IT system outage
- The glycol to water mixture ratio in the cooling loop was adjusted to withstand colder temperatures