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

2020 Three-Year Review of the Prescribed Persons and Prescribed Entities

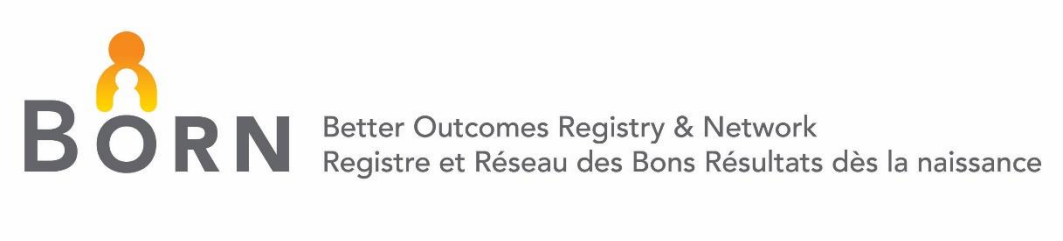


Table of Contents

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 (the "**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. Two versions of the Plan are referred to and described in this document. Version 2.0 of the Plan is effective as of October 31, 2019 and substantively corresponds to the practices and procedures approved in the prior review period ending October 31, 2017 (the "**2.0 Plan**"). BORN will update the 2.0 Plan to version 3.0 (the "**3.0 Plan**") to effect policy changes related to the migration of the BORN information system (BIS) to Microsoft Azure (the "**Migration Project**'). The 3.0 Plan also incorporates governance updates and improvements as described below following a comprehensive governance review that BORN commenced in late 2018. The 3.0 Plan is to become effective on or before the Migration Project goes live in 2020.

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, 2019 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 has taken steps that are reasonable in the circumstances to ensure adherence 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 Entities (the "**Manual**") 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 the following non-compliance to report, as follows:

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

   Policy **P-19: Executing Agreements with Third Party Service Providers in Respect of Personal Health Information** of the 2.0 Plan requires that each agreement is based on a template designed to conform to the requirements of the Manual. At a minimum, relevant template content will be met and further context will be added as needed. In the revised 3.0 Plan BORN is amending the procedure so that each agreement is normally based on the approved template. Material variations to the template are to be approved by the Executive Director and the Children's Hospital of Eastern Ontario – Ottawa Children's Treatment Centre ("**CHEO**") legal department. This will mean that BORN will have more latitude to alter the terms in which BORN, through CHEO, contracts with third party service providers in regard to industry standards, the material requirements of the Manual, and BORN's compliance requirements under the *Personal Health Information Protection Act*, S.O. 2004 ("**PHIPA**") and its regulation.

   Specific non-compliance:
   In March 2018 BORN agreed to terms that incorporated service provider terms with Microsoft Corporation in respect of the Migration Project. Those terms do not meet all of the express requirements of the policy and procedures for executing agreements with third party service providers set out in the Manual. For example, the agreement does not describe the status of BORN under PHIPA and the duties and responsibilities arising from this status.

   In proceeding with the Migration Project, BORN is implementing best industrial-grade cyber defenses to protect its data (or the data of stakeholders) in a cost-effective manner, upon terms that are reasonable in the circumstances in regard to industry standards and BORN's compliance requirements. By design, Microsoft will not have any access to personal health information as a result of the extensive use of encryption and controls implemented in respect of the encryption keys used. Additionally, data is hosted on servers located in Canada. In such circumstances, although the agreement does not describe the status of BORN under PHIPA and the duties and responsibilities arising from this status, BORN is of

the view that the agreement is still reasonable in the circumstances in regard to industry standards, BORN's compliance requirements under PHIPA and the material requirements of the Manual. In such circumstances, the fact that the agreement does not describe the status of BORN under PHIPA (and the duties and responsibilities arising from this status) is not seen a material concern provided that **P-19: Executing Agreements with Third Party Service Providers in Respect of Personal Health Information** is amended to allow for an assessment of contract terms and circumstances in regard to materiality. Accordingly, the 3.0 Plan will be amended so that each agreement is normally based on the approved template. Material variations to the template are to be approved of by the Director and the CHEO legal department, in regard to industry standards, BORN's compliance requirements under PHIPA and its regulation, and the material requirements of the Manual. This will mean that BORN will have more latitude to alter the terms in which it contracts with service providers in regard to industry standards and the material requirements of the Manual, while at the same time meeting its requirements under PHIPA and its regulation.

The policy will also expressly set out the following example: "By way of illustration, this means that in circumstances where personal health information that is hosted in Canada by a service provider who does not have access to the data by virtue of encryption, the fact that the agreement lacks a description of the status of BORN under PHIPA (and the duties and responsibilities arising from this status) is not considered a material concern in the circumstances. This change will be implemented with the revised 3.0 Plan.

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 – Ottawa Children's Treatment Centre is a prescribed person in respect of the Better Outcomes Registry and Network ("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. [1] 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[2], who report to the BORN Leadership Team on all related privacy and security matters. [3]

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[4] 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[5]
    - Disclosure of Personal Health Information Review Committee[6]

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.

---

[1] In the 3.0 Plan, the accountability framework is updated to reflect new changes and improvements in BORN's governance – please see Figure 1 (below), in Appendix C: Privacy, Security and Other Indicators, Part 1: Privacy Indicators. CHEO's CEO has delegated day to day responsibility for ensuring compliance with PHIPA and its regulation to BORN's Executive Director, and committees are established to provide support to BORN's Executive Director on matters of privacy, security and the collection, quality and disclosure of personal health information. The Executive Director also receives guidance from two management teams – the BORN Executive Team and the BORN Leadership Team - the role of these two teams are set out in **O-03: Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program** of the 3.0 Plan.

[2] In the 3.0 Plan, all references to Manager of Heath Informatics have been replaced with Information Security Officer to reflect organizational changes.

[3] In the 3.0 Plan, such reporting is to BORN's Executive Director on matters of privacy, security and the collection, quality and disclosure of personal health information (i.e., rather than reporting to the Leadership Team).

[4] The role of Scientific Manager is changed in the 3.0 Plan to refer to the Data Request and Research Coordinators except for those instances where a committee is used in place of the Scientific Manager.

[5] In the 3.0 Plan, the Data Collection Review Committee is now called the Data Holding Committee.

[6] In the 3.0 Plan, the Disclosure of Personal Health Information Review Committee is now called the PHI Disclosure Committee.

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:[7]

- 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

[7] In the 3.0 Plan, BORN makes it clear it uses the Personal Health Information that it collects for the purposes of facilitating or improving the provision of Health Care. The policy also indicates that such activities may encompass these examples described here. Additionally, the 3.0 Plan makes it clear that BORN may use Personal Health Information to conduct Research only when the strict requirements of PHIPA are adhered to, including review by a Research Ethics Board as per p.10: Use of Personal Health Information for Research.

- Creating reports that can be used to provide the Ministry of Health and Long-Term Care, Local Health Integration Networks (LHIN)[8] and Public Heath Units with comprehensive and timely information to support effective planning and management of health care delivery for mothers, babies and children in the province

Information provided in reports to the Ministry, Local Health Information Networks and Public Health does not contain personal health information or identify individuals; reports present an overview of aggregated health care data. These reports are produced following policies that are set out in the Plan that require that the data be aggregated and/or de-identified data; accordingly, the reports are carefully reviewed prior to disclosure to ensure there is no risk of re-identification through small cell counts or other forms of possible residual disclosure as per policy **P-24: De-Identification and Aggregation**. The reports are made available through the BORN website at www.BORNOntario.ca.

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

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

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.

[8] References to Local Health Integration Networks (LHIN) are removed in the 3.0 Plan.

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[9] initiates a review of privacy and security policies and procedures annually[10], or:

[9] In the 3.0 Plan, reviews are initiated by both the Privacy Officer and the Information Security Officer. This Policy is also changed to reflect that on-going review is appropriate having regard to the nature of ongoing risks, organizational changes, or technology changes. The decision-making process is revised to reflect that the Executive Director has ultimate authority over the Privacy and Security Review Committee, including final approvals over any changes to the policies and procedures. Record keeping and document retention is revised to include records of decisions of the PSRC, any relevant correspondence, and no longer includes documents not relevant to the review and revision process.

[10] In the revised 3.0 Plan, rather than annual this policy has been changed to reflect that it will be reviewed at least once prior to each scheduled review by the IPC pursuant to subsection 13(2) of the Regulation under the Act.

- 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 Confidentially 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. [11]

The Plan 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 Plan 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 (DCRC). [12] The DCHRC 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. [13]

[11] The 3.0 Plan provides that the purposes are to be expressly set out in P-07: Statements of Purpose for Data Holdings Containing Personal Health Information when new statements of purpose have been identified. Accordingly, the policy sets out that the DHC will ensure any new statements of purpose that have been approved are reflected in an update to P-07: Statements of Purpose for Data Holdings Containing Personal Health Information. In determining the any new statements of purpose to be considered, the policy sets out that Data Holdings Committee may consult with health information custodians and key experts in the field of maternal, infant and child health and other experts as warranted. Once changes are approved, the policy also sets out that the DHC will inform the Communications Lead in order to update the website with any changes to the statement of purpose. The Privacy Officer is to ensure that updates P-07: Statements of Purpose for Data Holdings Containing Personal Health Information that include new statement of purpose are communicated to Agents and any new statements of purpose are incorporated into data sharing agreements with the health information custodians or other persons or organizations from whom the personal health information in the data holding is collected.
[12] In the 3.0 Plan, the policy clarifies that the DCRC has been renamed to the "Data Holding Committee".
[13] In the 3.0 Plan, the functioning of the Data Holdings Committee (DHC) is very similar to the DCRC in the 2.0 Plan. The DHC will meet approximately every two months. Additional meetings will be scheduled as required.

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[14] and identifies the criteria that must be considered in determining whether to approve the collection of personal health information which includes[15]:

At the first meeting of the fiscal year, the DHC will develop its work plan and schedule for the year. The DHC will review any requests for new statements of purpose that may improve or facilitate the provision of health care, to provide proposed changes to its procedures to improve operational efficiencies, and to review BORN's data holdings to ensure their statements of purpose are still relevant and necessary for the identified purposes including: the purpose of the data holding, the PHI contained in the data holding, the source(s) of the PHI, and the need for PHI in relation to the identified purpose. It will also ensure that a summary list of BORN's data holdings of PHI are publicly communicated through BORN's website and it will also determine when the data collected by BORN is no longer needed to fulfill its purposes as a prescribed registry and collection of that particular data must be discontinued, and existing data must be de-identified or destroyed. Finally, it will also review and advise on the addition of new data elements and review and approve proposed enhancements to existing BORN data elements to improve accuracy, clinical relevancy, usability and/or reliability.

.

[14] In the 3.0 Plan, to reduce administrative inefficiencies the Data Holding Committee will no longer report to the Privacy and Security Review Committee; rather, it will report to the Executive Director.

[15] In the 3.0 Plan, the policy sets out that the DHC considers as part of its review whether: (a) The collection is permitted by PHIPA and its regulation, (b) Whether other information, namely de-identified and/or aggregate information, will serve the purpose of the Registry, (c) Whether no more Personal Health Information is being requested than is reasonably necessary to meet the purpose of the Registry, (d) Whether the rationale or statements of purpose for each data holding can be linked to the need for the data in relation to the identified purpose of the Registry, (e) Any risks identified in privacy impact assessments undertaken by BORN regarding new data holding (where applicable), (f) Any conditions that must be satisfied prior to collection, and (g) Whether appropriate data sharing agreements are in place or pending.

- 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[16]
- 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 securely maintained in identifiable form within the transactional database for 28 years[17] 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.

[16] In the 3.0 Plan, new statements of purpose will be added to **P-07: Statements of Purpose for Data Holdings Containing Personal Health Information** which will be included at the website. To the extent not reflected in any pre-exiting data sharing agreements that expressly list approved purposes, any new purposes will be incorporated as each agreement is amended or restated.

[17] In the 3.0 Plan, this will remain the case unless an earlier date is decided by the Data Holdings Committee.

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:[18]

#	Data Holding	Description
1	BORN Information System (BIS)	A single data holding comprised of Personal Health Information collected from the following health information custodians: • Prenatal and Newborn screening providers • Hospitals • Midwives • Outpatient clinics • Fertility clinics • Family Health Teams/Primary Care Providers • Birth Centres • Autism Treatment Centres • Public Health Units
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.

[18] In the 3.0 Plan this policy is updated to include historical data from CANImmunize from public health units that participated in a pilot which has since ended.

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[19]. The policy indicates that the BORN Data Dictionary maps data collected by BORN to one or more of these statements of purpose. The six approved statements of purpose are:

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

[19] In P-04: Collection of Personal Health Information and P-06: Statements of Purpose for Data Holdings Containing Personal Health Information of the 3.0 Plan, the policy sets out that for each holding containing personal health information the Data Holdings Committee determines the list of data elements and the associated statements of purpose, together with the proposed list of health information custodians from whom the data elements or data holdings will be collected.

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[20], and states that access to personal health information by BORN agents is based on the "need to know" principle that is controlled via role-based access.

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

The 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

[20] In the 3.0 Plan, the policy no longer defines agent to mean employee or consultant, contractor or seconded employee to BORN Ontario who has authority to provide services to or on behalf of BORN Ontario (i.e., the definition in the 2.0 Plan). Rather, "Agent" is a defined term throughout the plan based on the usage of that term in PHIPA; i.e., a person that, with the authorization of BORN, acts for or on behalf of BORN in respect of PHI for BORN purposes, and not the agent's own purposes, whether or not that agent has the authority to bind BORN and whether or not that agent is employed by BORN and whether or not the agent is being remunerated by BORN.

- 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[21] 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

[21] BORN permits the storage of PHI in two environments, the BORN Information System and the BORN PHI Drive. Two different Agent Data Access Forms are reflected in the 3.0 Plan (i.e., one form for each environment).

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 Data Request and Research Coordinators are the only 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[22] 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

[22] In the 3.0 Plan, "BORN Director" is replaced with the "BORN Executive Director".

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 Plan 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**.[23] The Plan 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 **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 Confidentially 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 automatically set to one year unless subject to shorter timeframe (if less than one year specify timeframe)[24]

[23] In the 3.0 revised Plan, P-27: Privacy Audits sets out that audits are conducted on a monthly basis for a selection of agents designed each month to ensure that every agent with access to Personal Health Information is selected at least once every 12 months.

[24] The log explicitly sets out that the timeframe in the log is automatically set to one year unless a shorter timeframe has been determined for an individual agent. For those agents whose access is still active, the log specifically identifies which agents are subject to a shorter timeframe and what that timeframe is.

- 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[25].

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 Plan 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 Plan 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[26] 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[27]

Review and Approval Process

[25] In the 3.0 Plan, the term "Research" is defined to be consistent with PHIPA.
[26] In the 3.0 Plan, this test is revised to explicitly reference that research means a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research.
[27] In the 3.0 Plan, "Does not create new knowledge" is added to this test for consistency with other policies within the Plan.

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[28] approving the research.

The BORN policy further identifies the following review steps be undertaken by the Scientific Manager[29] 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 and its regulation*[30]
- 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.

[28] The 3.0 Plan is revised to reflect that REB approval may be pending rather than available at the time of the request, but in all cases, it is ultimately required before any request is fulfilled.

[29] In the 3.0 Plan, the review and approval of all use for research purposes is conducted by the Research Review Committee (rather than any one individual such as Scientific Manager in the 2.0 Plan), using the same criteria and information as in the 2.0 Plan.

[30] The revised 3.0 Plan expressly sets out a research plan must be in writing and must set out, (a) the affiliation of each person involved in the research; (b) the nature and objectives of the research and the public or scientific benefit of the research that the researcher anticipates; and (c) all other prescribed matters related to the research, e.g., (1) A description of the research proposed to be conducted and the duration of the research. (2) A description of the personal health information required and the potential sources, (3) A description of how the personal health information will be used in the research, and if it will be linked to other information, a description of the other information as well as how the linkage will be done, (4) An explanation as to why the research cannot reasonably be accomplished without the personal health information and, if it is to be linked to other information, an explanation as to why this linkage is required, (5) An explanation as to why consent to the disclosure of the personal health information is not being sought from the individuals to whom the information relates, (6) A description of the reasonably foreseeable harms and benefits that may arise from the use of the personal health information and how the researchers intend to address those harms, (7) A description of all persons who will have access to the information, why their access is necessary, their roles in relation to the research, and their related qualifications, (8) The safeguards that the researcher will impose to protect the confidentiality and security of the personal health information, including an estimate of how long information will be retained in an identifiable form and why, (9) Information as to how and when the personal health information will be disposed of or returned to the health information custodian, (10) The funding source of the research, (11) Whether the researcher has applied for the approval of another research ethics board and, if so the response to or status of the application, (12) Whether the researcher's interest in the disclosure of the personal health information or the performance of the research would likely result in an actual or perceived conflict of interest with other duties of the researcher.

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[31]. 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 Plan 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
The policy states 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

[31] In the 3.0 Plan, the Research Review Committee reports to the Executive Director and as such its decisions are not reviewed by the Privacy and Security Review Committee.

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[32]
- 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)[33] 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

[32] In the 2.0 Plan one individual (i.e., the Scientific Manager) reviewed and approved the use of de-identified or aggregate information for Research without the need approval by the Privacy and Security Review Committee (PSRC). In the 3.0 Plan, this has changed so that the review and approval of any use for research purposes is conducted by the new Research Review Committee (RRC), using the same criteria as in the 2.0 Plan. Additionally, the PSRC is no longer involved in the review or approval of research requests (because these functions are performed by the RRC) and the RRC reports directly to the Executive Director.
[33] In the 3.0 Plan, other de-identification software tools (besides PARAT) are also included, including successor and replacement products. A suitable definition is thus used throughout the Plan for "De-identification Tools".

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 Plan:
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 Confidentially 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 section13(5) of the *Personal Health Information Protection Act, 2004*
4. To a health data institute under section 13(5) and section 47 of the *Personal Health Information Protection Act, 2004*

Review and Approval Process

The policy clearly defines the agent(s) responsible for receiving and reviewing requests for the disclosure of personal health information. The Scientific Manager receives all requests and reviews them with the Manager of Health Informatics and the Privacy Officer. The policy further defines that approvals are the responsibility of the Disclosure of Personal Health Information Review Committee[34]. 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[35]:

- 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

[34] In the 3.0 Plan, the Data Disclosure Review Committee (DCRC) has been renamed to the PHI Disclosure Committee (PDC). The same procedure is substantively followed in the 3.0 Plan.

[35] The terms of reference for the PHI Disclosure Committee (PDC) require the PDC to consider: (i) the legal authority of the prospective disclosure request with reference to PHIPA; (ii) the background of the project including how it aligns with BORN purposes (or other considerations pertaining improving or facilitating the provision of Health Care – in this respect, the PDC may refer requests that require consideration of a new or revised purpose to the Data Holdings Committee); (iii) advice or recommendations provided by the Data Request and Research Coordinator, BORN Privacy Officer and other BORN staff or outside consultants or experts; (v) whether more data is being requested than is necessary for the purpose; (vi) the list of agreed-upon data elements and whether there are opportunities to de-identify any data; (vii) contractual restrictions under data sharing agreements that might restrict the disclosure; (vii) the location/jurisdiction of the recipient and its data security and privacy practices; (ix) the legal terms that would apply to the disclosure and protection of PHI during its intended use and subsequent destruction; and (x) any other relevant privacy, security, or legal considerations that might warrant refusing the requests.

- 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, the Scientific Manager 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 policy sets out that 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 policy sets out that the Privacy Officer monitors disposal dates **in P-18: Log of Data Sharing Agreements** for follow-up. The policy sets out that 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.

The policy sets out that 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)[36] 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 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 states that the Scientific Manager[37] 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

[36] In The 3.0 Plan, references to PARAT have been changed to the De-identification Tools because BORN now uses successor products that perform a similar function.
[37] In the 3.0 Plan, the disclosure of record level (i.e., non-aggregated) de-identified data is reviewed and approved by the PHI Disclosure Committee rather than a single person.

- 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 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 Plan:

- 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* and its regulation
- 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[38] 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 Scientific Manager prepares an official letter of approval which sets out:

- Purpose of the research

[38] In the 3.0 Plan, the review of all research data requests is conducted by the Research Review Committee (RRC) rather than a single person. The RRC may approve requests that involve de-identified or aggregate data disclosures but all other requests (i.e., disclosure of record level PHI for research purposes) will require the additional approval of the PHI Disclosure Committee.

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

Secure Return or Disposal

In accordance with the policy, the Research Agreement 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 policy requires the Privacy Officer or designate monitors disposal dates in **P-15: Log of Research Agreements** for follow-up. The policy provides 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.

The policy provides 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 policy provides 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 set out in **S-07: 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.

The template research agreement requires the Recipient to complete and submit to the BORN Privacy Officer within 7 days of the secure destruction the certificate of destruction setting out the personal health records destroyed, date, time, location and precise method of secure destruction employed, and bearing the name and signature of the person who performed the secure destruction

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[39]:

- 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:

[39] In the 3.0 Plan, these fields are:

- Name of research study
- Principal researcher last name
- Principal researcher first name
- Date of written application received
- Date of written research protocol received
- Date of Research Ethics Board written decision approving plan
- Dataset de-identified (Y/N)
- If NO to de-identification provide explanation
- Date Research Agreement executed
- Date of approval to disclose Personal Health Information or de-identified data for research was granted (by BORN Research Review Committee)
- Date Personal Health Information or de-identified data was disclosed
- Nature of Personal Health Information or de-identified data (data source description)
- PHI or de-identified data
- Retention period as per Research Ethics Board
- Secure disposal due date
- Date certificate of destruction was received
- Any Research Agreement amendments

- 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 (**P-22: 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.[40]

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.

[40] In the 3.0 Plan, policy **P-19: Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information** will provide that each Agreement is normally based on an approved template designed to conform to the requirements of the Manual. Material variations to the template are to be approved of by the Director and CHEO legal, in regard to industry standards, BORN's compliance requirements under PHIPA and its regulation and the material requirements of the Manual. This will mean that BORN will have more latitude to alter the terms in which it contracts with service providers in regard to industry standards and the material requirements of the Manual, while at the same time meeting its requirements under PHIPA and its regulation. The revised 3.0 policy expressly sets out the following example: "By way of illustration, this means that in circumstances where personal health information that is hosted in Canada by a service provider who does not have access to the data by virtue of encryption, the fact that the agreement lacks a description of the status of BORN under PHIPA (and the duties and responsibilities arising from this status) is not considered a material concern in the circumstances."

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 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 Confidentially 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 of personal health information related to BORN.

Where the third-party service provider is an Electronic Service Provider as described in subsection 10(4) of the *Personal Health Information Protection Act*, such 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. The agreement states that "disposed of in a secure manner" requires destruction in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstances. The agreement includes and incorporates a policy setting out the technical guidelines.[41] 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

[41] Such are designed to be consistent with PHIPA and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information; and S-8: Policy and Procedures for Secure Disposal of Records of Personal Health Information.

- 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

Secure Disposal as a Contracted Service
BORN does not enter into arrangements where the disposal of records of personal health information is the primary service provided to BORN.

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.[42]

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.

[42] In P-19: Executing Agreements with Third Party Service Providers in Respect of Personal Health Information the revised 3.0 Plan, a statement has been added that indicates that in circumstances where personal health information is hosted in Canada by a service provider who does not have access to the data by virtue of encryption, the fact that the agreement lacks advanced notice of intention to subcontract and lacks a requirement to deliver actual terms is not considered a material concern in the circumstances.

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[43]

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:

[43] The revised 3.0 Plan expressly provides that all linkages require review and approval according to the following process that is also set out in the policy. In the case of a research project, the approval for the linkage rests with the Research Review Committee who review, approve and log the linkage by confirming that it is described in the research plan and the REB approval; the policy also provides that they confirm it is allowed by any applicable in-bound data sharing agreements. For BORN's internal work pursuant to facilitation or improvement of health care (e.g. linkage with CIHI or Stats Canada data), the need for linkage is outlined by a specific group (data quality, a clinical program, or technical group) and is documented in a project memorandum and approved by the BORN management group (i.e., the Executive Director and BORN Managers) who review, approve (or deny) such decision by email, and log the linkage. Approval is granted where such linkage is necessary for the purposes of improving and/or facilitating care, it is permitted under the applicable data sharing agreement, any applicable REB approvals and research plans, and it is in compliance with PHIPA and its regulation. In all cases, approved linkages are logged in the Log of Approved Linkages of Records of Personal Health Information by the Manager of Health Outcomes or designate. Decisions are communicated to the original requestor by email by the Manager of Health Outcomes (or designate). If there are any conditions to the approval these are noted in the approval.

- 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.[44] 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

[44] As the BORN Information System (BIS) is an aggregation of various health care encounters during pregnancy and the early newborn period, BORN needed a mechanism to link the PHI from these encounters. During the development of the BIS, BORN developed a linking and matching strategy to ensure the PHI and clinical data from the same individuals and their child (children) would be aggregated appropriately. This mechanism is largely based on a weighting algorithm and allows BORN to have confidence in ensuring the information is assigned appropriately. The revised 3.0 Plan accordingly sets out and describes three categories in its policy:
(i) BORN Information System – Link Queue: 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 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 Agent (linking and matching resource) has responsibility for managing the queue of potential linked records.
(ii) BORN Information System – External Link Queue: The BORN Information System contains a function that allows a designated Agent to load an external dataset into its linking and matching engine. A report is then produced listing automatic, potential, and non-matched patients. This report is used by BORN agents to facilitate data requests that require external datasets.
(iii) Third Party Datasets or other Holdings Not Forming Part of the BIS: BORN Agents use statistical analysis software (e.g. SAS and R) to link other datasets with data extracted from the BIS. Linkage occurs to bring together separate datasets, usually to improve the ascertainment of cases, exposures or outcomes. At BORN, this usually involves linking a dataset held outside the BIS with data held inside the BIS for research or internal needs.

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.[45]

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.

[45] In the revised 3.0 Plan, exceptions to this policy requires consideration of Data Sharing Agreements, Research Agreements and written research plans pursuant to which the personal health information was collected by BORN. Additionally, consideration must go to whether the risk is remote in the circumstances that it (i.e., the small cell sized data of five (5) or less) could be used alone or in combination with other information to identify an individual. The policy establishes that the PHI Disclosure Committee will make these determinations on a case-by-case basis in consideration of the foregoing constraints.

- **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. This restriction is contained in all Research Agreements and Data Sharing Agreements.

As stated in the policy, BORN uses the Privacy Analytics Re-Identification Risk Assessment and De-identification Tool (PARAT) [46] 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**

[46] As noted above, in the 3.0 Plan this is now updated to the "De-identification Tools"; i.e., the software tools and related services, if any, used for the De-identification of data including (in the case of products marketed by Privacy Analytics or their successors) the products referred to as Eclipse and PARAT and any successor products used by BORN. The policy is otherwise unchanged except that BORN has created a standard operating procedure for Dataset De-identification Process that is incorporated by reference into the 3.0 Plan in order to help standardize methods of using the De-identification Tools.

The Plan 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 Confidentially 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 Confidentially 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[47] 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

[47] In the 3.0 Plan, audit reporting is to Privacy and Security Review Committee and the Executive Director.

- 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. [48]

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

[48] The revised 3.0 Plan provides that this same policy also applies to suspected privacy breaches (where indicated).

- 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.[49]

If the Privacy Officer determines that the breach involves theft or impacts personal safety, the Privacy Officer:[50]

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

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

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

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

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

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

[49] In the 3.0 Plan, as soon as reasonably possible, the Executive Director will advise the CHEO VP and a description of any further efforts at containment. The Privacy Officer will advise the CHEO Chief Privacy Officer.
[50] In the 3.0 Plan, it is to be noted that steps involving consideration of any legal requirements to provide notification are incorporated including guidance's issued by the Information and Privacy Commissioner.

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 its recommendation to proceed with implementation of the recommendation.[51]

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 Confidentially 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.

[51] In the 3.0 Plan, the governance is changed to reflect that the Privacy and Security Review Committee (PSRC) reports to the BORN Executive Director, who ultimately has the authority to approve or deny any recommendations made by the PSRC – please see Figure 1 (below), in Appendix C: Privacy, Security and Other Indicators, Part 1: Privacy Indicators.

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 if required, the complainant will be contacted
- Sets out the timeframe for completion of the investigation
- Sets out the nature of the documentation that will be provided upon completion of the investigation

The BORN Privacy Officer is responsible for conducting privacy complaint investigation as per the procedure, which also sets out that the Privacy Officer seeks to substantiate the facts surrounding the complaint by undertaking reviews of relevant documents, conducting interviews with the complainant, BORN agents and third parties, health information custodians, and researchers, as appropriate, and carrying out site visits and inspections, as appropriate.

The investigation and documentation of the findings are completed by the Privacy Officer within 30 days of receipt of the complaint form. The report is forwarded to the BORN Director, who in turn forwards it to the Leadership Team[52]. 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.

[52] In the 3.0 Plan, the review and approval vests with the BORN Executive Director rather than the Leadership Team – please see Figure 1 (below), in Appendix C: Privacy, Security and Other Indicators, Part 1: Privacy Indicators.

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 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 Confidentially 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 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 Confidentially 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[53]. 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

[53] In the 3.0 Plan, PART 2: Information Security Policy is updated to reflect changes to physical and information security based on BORN's move to Microsoft Azure. The updated policy identifies the BORN Information Security Officer (rather than the Manager of Health Informatics) as responsible for ensuring compliance with all BORN security policies and procedures. Administrative safeguards have been updated to focus on security, delegating the privacy safeguards to the Privacy Officer. Technical safeguards have been updated to remove specific reference to RSA two-factor authentication and replace it with a generic statement that two-factor authentication will now be required for all Registry users. This prevents BORN from being locked into a specific technology and allows it to adapt to new security technologies on an as needed basis. Furthermore, the addition of a requirement for independent reviews and assessments to be performed at least annually, or at planned intervals, to ensure that the organization addresses any nonconformities of established policies, procedures, and known contractual, statutory, or regulatory compliance obligations.

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[54] 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.

[54] In the 3.0 Plan, **S-02: Ongoing Review of Security Policies and Procedures** is updated to identify the BORN Information Security Officer rather than the Privacy Officer as responsible for the policy.

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

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

The policy sets out that 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.

The policy defines two types (levels) of access[55]:

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**.

The policy requires that 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.

---

[55] In the 3.0 Plan, Ensuring Physical Security of Personal Health Information, is updated to reflect BORN's move to Microsoft Azure. Responsibility will be shared by the Information Security Officer and Privacy Officer. Physical access will be defined as: (1) Any secure CHEO building protected by two levels of secure access and/or a BORN employee's personal residence (i.e. teleworkers) and where no personal health information is retained on these premises. **Policies S-01: Information Security Policy**, **S-09: Passwords and Multi-Factor Authentication**, **S-14: Acceptable Use of Technology**, and **P-08: Limiting Agent Access to and Use of Personal Health Information** address the physical security of devices used by teleworkers. (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 will be managed by the Hosting Service Provider (i.e. Microsoft).

The update will further detail access to the BORN premises where CHEO employees work (i.e. procedures on the provisioning of identification/access cards and office keys). It will also detail physical safeguards and access to the Microsoft Azure data centre. Other updates will include added detail on: (a) The procedures for handling theft, loss and misplacement of identification cards, access cards and keys; and (b) the policy for termination of the employment, contractual or other relationship

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 Confidentially 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
The policy provides that 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). The policy provides that 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

The policy provides that 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 policy provides that 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
The policy provides that 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**

The policy provides that 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**

The policy provides that 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

The policy provides that 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 policy provides that 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.

Policy, Procedures and Practices with Respect to Notification When Access is No Longer Required

As per **P-8: Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information**, all approved accesses and uses of personal health information are subject to an automatic expiry after one year or sooner based on the Agent Data Access Form. [56] The policy provides that Agents and their supervisors request approval for access (when necessary) on an annual basis one year from the date approval is granted.

Additionally, the policy provides that BORN Agents and their supervisors must adhere to HR-10 Termination and Cessation of Employment when a decision is taken to terminate the Agent's role. Agents and their supervisors are required to notify the Executive 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:

- Name of Agent
- Termination date
- Reasons for termination

The policy also provides that within three days, the Executive Director, or delegate, forwards the name of the Agent and the termination date to:

- Security for termination of access to the building
- Information Security Officer who arranges for the withdrawal of access to Personal Health Information on termination date and updates **P-09: Log of Agents Granted Approval to Access/Use/Disclose Personal Health Information**.

The policy also provides that the Executive Director, or delegate, reminds the Agent of the confidentiality requirements contained in the signed Confidentiality Agreement.

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

[56] For situations where access cannot be set to automatically expire by virtue of limitations in the technology, the BORN privacy officer maintains a reminder system to manually disable access on the same basis through a request to the IT Department. This change is reflected in the revised 3.0 Plan.

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

The policy sets out that Visitors to the BORN Data Centre are required to sign in and record their name, date and time of arrival, time of departure and the name of the Agent(s) with whom the visitors are meeting. Visitors must be accompanied by the BORN System Hosting Provider at all times. [57]

The policy requires that all documentation related to the identification, screening and supervision of visitors to the Data Centre is retained by the BORN System Hosting Provider.

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

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

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

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

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

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

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

BORN has in place a policy to ensure the secure retention of records of personal health information in 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

[57] In the revised 3.0 Plan, visitors must wear identification issued by the BORN Information Security Officer; the Information Security Officer ensures the identification is returned prior to departure; and the Information Security Officer ensures that the visitors complete the appropriate documentation upon arrival and departure.

collection data sharing agreements. As per BORN policy **P-04: Collection of Personal Health Information**, the data is then converted to de-identified format.

With respect to records of personal health information 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[58].

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

[58] In the 3.0 Plan, **S-05: Retention of Records of Personal Health Information** is updated to reflect that responsibility will be shared by the Information Security Officer and Privacy Officer. In order to facilitate the day to day operations of BORN, the use of temporary data storage is required. Temporary data storage is required for, but not limited to: the collection of Personal Health Information; testing of Disaster Recovery Procedures; testing of data backups; and migration of data to BORN's Microsoft Azure environment. Data residing in temporary locations will only be for the amount of time required to import the data into the BORN Information System and/or storing the data on the BORN PHI drive after which time it will be deleted. A section is added detailing the policy on the temporary storage of PHI specifically related to the BORN secure FTP server and the BORN SQL server file systems (for backup and restore files).

- 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".

Prior to BORN's migration to Azure, BORN did not contract a third party service provider to retain records of personal health information. By design, Microsoft will not have any access to personal health information in unencrypted form. BORN's service provider Dapasoft does not retain records of PHI on behalf of BORN.

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 Confidentially 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[59]. 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[60].

[59] In the 3.0 Plan, the policy around agent access via the internet will be the responsibility of the Information Security Officer who ensures that: staff are trained to use strong unique passwords that are a mixture of alphabetic characters, special characters, digits, minimum of six characters in length; remote access can only be achieved through single secure portal logon page; 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; mobile devices use full disk encryption are encrypted with a minimum standard of AES-256; and staff compliance is monitored using the **S-06A: Agreement for the Use of Mobile Devices/Remote Access**.

[60] In the 3.0 Plan, **S-08: Secure Transfer of Records of Personal Health Information** is updated to identify the BORN Information Security Officer rather than the Manager of Health Informatics as responsible for the policy. Furthermore, references to the Scientific Manager is updated to Data Request and Research Coordinator. Secure transfer of data into BORN will be detailed, specifically the methods of data transfer allowed will be in one of the following ways:

1. Direct connection to the BORN portal by:
    a. using a browser with industry standard SSL encryption, or
    b. HL7 feed directly from hospital systems using a secure VPN connection
2. BORN Hosting Provider
3. Secure FTP
4. BORN Secure Web Service
    a. Users on the public Internet must establish a SSL connection to the BORN Secure Web Service; this requires token-based dual authentication
5. Ontario Health's Connected Backbone (Health Information Access Layer or HIAL)

The policy requires the following:

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

Transfer Out of BORN

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

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

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

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

When receipt has been confirmed, the Scientific Manager 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-crypt the data set.

a. Organizations on the public Internet require ONE ID certificate authentication to access the HIAL Health Information Network Provider (HINP) to transfer Personal Health Information to BORN

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 secure 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 Personal Health Information Disposed Of/Destroyed
- Confirmation of the secure disposal of the records of personal health information
- 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[61] 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

[61] In the 3.0 Plan, **S-09: Passwords and Multi-Factor Authentication** is updated to identify the BORN Information Security Officer rather than the Privacy Officer as responsible for the policy. Furthermore, a new section on the use of multi-factor authentication is added which details the new requirements for all BORN Information System users. Specifically, multi-factor authentication (MFA) will be required for all BORN Information System users.

Two options for MFA will be available to users: for users in organizations that cannot have access to a smart phone or direct phone number a PIN and for users in organizations that have access to a smart phone a one-time use code.

1) For users in organizations that cannot have access to a smart phone or direct phone number
   - The public IP address of the site will be registered in the BIS.
   - Any attempt to access the BIS from an unlisted site by a user who is setup for this option will result in denied access to the BIS.
   - A user logging in from a registered site must enter an alphanumeric PIN which will be setup during the user registration process
   - The PIN will be 6-8 characters in length and contain at least one number and one letter.
2) For users in organizations that have access to a smart phone there will be two methods for this option: Send a one-time use code via a SMS message or receive a call with a one-time use code over the phone.
   - A valid phone number will be registered with a user's account, which is setup during the user registration process.
   - The user will be able to select which method they wish to be contacted at the time of login.

   The one-time use code must be successfully entered in order to complete authentication.

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[62]. 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

[62] In the 3.0 Plan, **S-10: System Control and Audit Logs** is updated to reflect that responsibility is shared by the Information Security Officer and Privacy Officer. Furthermore, a new requirement is added such that at the request of the Privacy Officer, the Information Security Officer will produce the following ad-hoc reports (this is undertaken if there is a suspected breach or other system anomaly):

- What did a user change during a period of time – report of the records created, modified and or deleted by a specific user during a specified date range;
- What is the revision history for a patient during a period of time – report of the complete revision history of who created, modified and/or deleted details of patient demographics and encounter details for selected patients and date range;
- What did a particular user access within the system during a period of time – report of patient IDs, record details and record IDs accessed by that user during the specified date range;
- Who looked and/or changed a particular patient during a period of time – report of the complete access history of who viewed, created, modified and/or deleted details for selected patient ID and date range.

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[63].

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.[64]

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

[63] In the 3.0 Plan, **S-11: Patch Management** is updated to identify the BORN Information Security Officer (rather than the Privacy Officer) as responsible for the policy.

[64] In the revised 3.0 Plan, the policy requires that the Information Security Officer document the implementation of patches in a patch log that contains: the description of the patch; the date that the patch became available; the severity level and priority of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; the date that the patch was implemented; the agent(s) responsible for implementing the patch; the date, if any, when the patch was tested; the agent(s) responsible for testing; and whether or not the testing was successful.

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 Confidentially 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[65] (where BORN's operational environment is the BORN Information System).

[65] In the 3.0 Plan, **S-12: Change Management** is updated to identify the BORN Information Security Officer and the BORN System Administrator rather than the Manager of Health Informatics will share responsibility for the policy. Furthermore, reference to the Manager of Health Informatics will be replaced with BORN System Administrator or BORN Information Security Officer as appropriate. Change requests will be divided into two sections: the BORN Information System and the BORN operational environment (i.e. BORN's Azure environment). The sections will identify the different sources of change requests and detail the information required and request submission procedures. The BORN System Administrator and the Information Security Officer will receive, review and approve or deny all requests.

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 the 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:
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 Confidentially 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. This includes documentation that must be completed; the agent(s) responsible for completing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

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[66] as per S-05: Retention of Records of Personal Health Information.

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

[66] In the 3.0 Plan, **S-13: Back-up and Recovery of Records of Personal Health Information** is updated to reflect that backups are stored on servers hosted by Microsoft in Toronto, Ontario in encrypted format using the Azure Backup Service. Copies of the backups are also stored at BORN's disaster recovery site hosted by Microsoft in Quebec. Furthermore, full details of the BORN Backup plan will be contained in the BORN Disaster Recovery Plan.

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[67].

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

[67] In the 3.0 Plan, **S-14: Acceptable Use of Technology** is updated to reflect responsibility is shared by the Information Security Officer and Privacy Officer.

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[68]. 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

[68] In the 3.0 Plan, **S-15: Security Audits** is updated to reflect the BORN Information Security Officer rather than the Manager of Health Informatics as responsible for the policy.

- 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[69].

The policy defines a security breach[70] 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

[69] In the 3.0 Plan, **S-17: Security Breach Management** is updated to reflect responsibility will be shared by the Information Security Officer and Privacy Officer. Furthermore, the BORN Information Security Officer will now be 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.

[70] The revised 3.0 Plan provides that this same policy also applies to suspected information security breaches (where indicated).

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

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

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

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

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

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

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

The written notification will include:

- Date of the security breach
- A general description of the extent of the breach

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

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

- The BORN Leadership Team is notified by the BORN Director (who forwards the Privacy Officer's e-mail and a description of any further efforts at containment) as soon as is reasonably possible.
- The Information and Privacy Commissioner may be notified; the decision to notify made between the Privacy Officer and the BORN Director and, if deemed necessary, results in an e-mail from the Privacy Officer to the office of the Information and Privacy Commissioner indicating that:
    - A security breach has occurred
    - A brief description of the nature and extent of the security breach, including what information has been breached
    - Actions taken by the agent reporting the security breach and the Privacy Officer to contain the breach
    - The police have been notified and why (if applicable)
- BORN staff, the Leadership Team and the CHEO Chief Privacy Officer receive e-mail updates from the Privacy Officer on a regular basis. [71]

Investigation

When the breach has been contained and the BORN Director informed, the Privacy Officer[72] 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

[71] In the 3.0 Plan, the Privacy Officer e-mails updates to the CHEO Chief Privacy Officer. The Information Security Officer updates the Privacy and Security Review Committee and the Executive Director and the CHEO VP on a regular basis.

[72] In the 3.0 Plan, the Information Security Officer is also involved in this function.

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[73] 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

[73] In the 3.0 Plan, the review and approval vests with the BORN Executive Director rather than the Leadership Team – please see Figure 1 (below), in Appendix C: Privacy, Security and Other Indicators, Part 1: Privacy Indicators.

- 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.

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

BORN has in place policy **HR-05 Execution of Confidentiality Agreements by Agents** to ensure all agents are aware of and confirm their obligations to protect the privacy and confidentiality of the personal health information for which BORN is responsible. As per this policy, BORN agents execute

Confidentiality Agreements (as per policy **HR-06: Template Confidentiality Agreement with Agents**) at the commencement of their employment, contractual or other relationship with BORN and prior to being given access to personal health information. Confidentiality Agreements are renewed annually on completion of annual privacy and security training.

The BORN policy identifies that the Privacy Officer is responsible for ensuring that a Confidentially Agreement is signed with each agent of BORN at the commencement of the employment as well as re-signed or re-acknowledged annually.

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

3.6 Template Confidentiality Agreement with Agents

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

General Provisions

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

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

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

The Confidentiality Agreement is executed at the end of the initial privacy and security orientation, at which point each agent is also provided with the BORN Privacy and Security Management Plan, which contains all privacy and security policies and procedures. As agents have not yet had time to read this book, the Confidentiality Agreement does not satisfy the following IPC required statement:

> *Agents must also be required to acknowledge that they have read, understood and agree to comply with the privacy and security policies, procedures and practices implemented by the prescribed person or prescribed entity and to comply with any privacy and security policies, procedures and practices as may be implemented or amended from time to time following the execution of the Confidentiality Agreement*.

Rather, each agent is required to reply to an e-mail from the privacy officer, after they have undergone privacy training and have read through all BORN privacy and security policies and procedures, to confirm the following:

> *I have read, understood and agree to comply with the privacy and security policies and procedures implemented by BORN and I will comply with any privacy and security policies and procedures that may be implemented or amended from time to time.*

Obligations with Respect to Collection, Use and Disclosure of Personal Health Information

The BORN Confidentiality Agreement clearly identifies the purpose for which BORN is permitted to collect, use and disclose personal health information (for the purposes of facilitating and improving the provision of health care to mothers, infants and children). The agreement further sets out that any personal health information collected, used or disclosed must be in accordance with the Act and its regulation, the provisions of the Confidentiality Agreement, the BORN privacy and security policies and procedures, or as required by law. This agreement further includes the following obligations:

> *Agents agree they will not access or use personal health information if other information will serve the purpose and will not access and use more personal health information than is reasonably necessary to meet the purpose.*

Termination of the Contractual, Employment or Other Relationship

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

Notification

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

security policy or procedure as per policy **S-17: Policy and Procedures for Information Security Breach Management**.

Consequences of Breach and Monitoring Compliance

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

3.7 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.

3.8 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[74]:

- 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

[74] In March 2019 BORN's privacy officer commenced reporting into the CHEO Chief Privacy Officer and the BORN Executive Director. The privacy officer is also a lawyer and in such capacity commenced reporting to the CHEO General Counsel and the BORN Executive Director in March 2019. The current BORN Privacy Officer and Counsel also serves as the chair of the Privacy and Security Review Committee.

- 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

3.9 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.

3.10 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.

3.11 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[75]

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

[75] In version 3 of the Plan, the new framework identifies the BORN Executive Director as responsible for ensuring compliance with PHIPA and its regulation (rather than the Leadership Team). All committees are established to provide guidance and advice to BORN's Executive Director on matters of privacy, security and the collection, quality and disclosure of data - please see figure 1 (below), in Appendix C: Privacy, Security and Other Indicators, Part 1: Privacy Indicators. The Executive Director also receives guidance from two management teams – the BORN Executive Team and the BORN Leadership Team.

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.[76] 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 quarterly 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

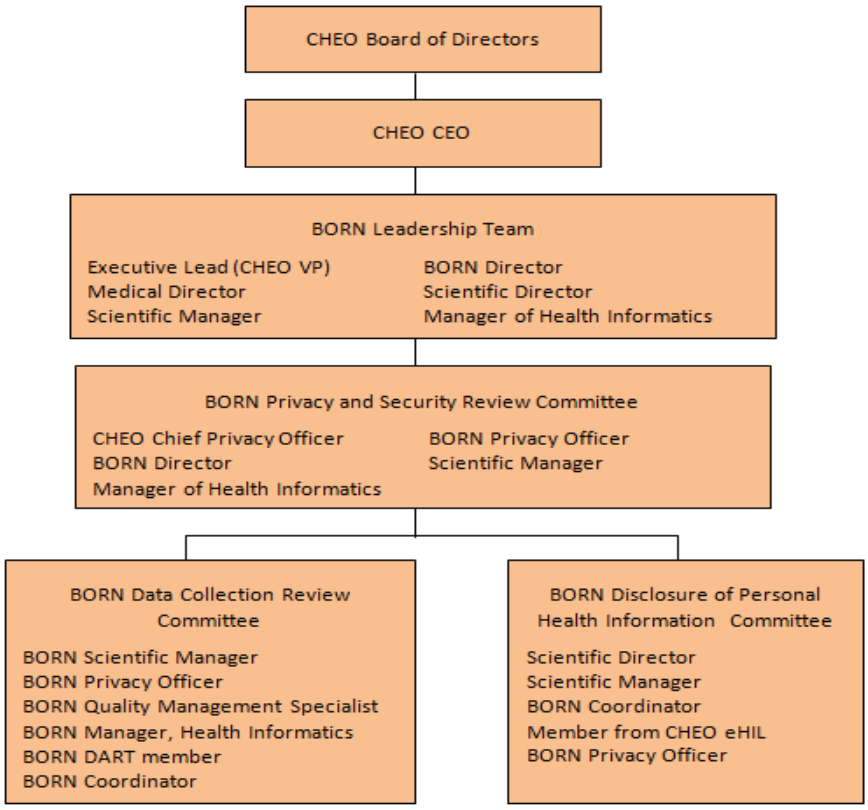
- Privacy inquiries and complaints and their resolution
- Privacy and security breaches, if any, related recommendations and the status of their implementation.
- Any other privacy and security related issues, as applicable

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

[76] In the 3.0 Plan, the policy indicates that the Privacy Officer and Information Security Officer will prepare an annual report to be reviewed by the PSRC for approval by the Executive Director. Based on this report, each year the Vice President of Provincial Programs and CIO will be supplied with a written report by the Executive Director addressing the initiatives undertaken by the privacy and security programs including training, development of policies, procedures, audits undertaken, privacy impact assessments, threat risk assessments, privacy and security breaches, privacy complaints that were investigated, and the status of any recommendations that were made from the investigations. The Vice President of Provincial Programs and CIO will present such findings to a committee of the CHEO Board of Directors on an annual basis.

The BORN policy on **Privacy and Security Governance and Accountability Framework** includes a privacy and security governance organization chart[77]:



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[78] 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

[77] In the 3.0 Plan, this chart is replaced with the chart shown at figure 1 (below), in Appendix C: Privacy, Security and Other Indicators, Part 1: Privacy Indicators.

[78] In the 3.0 Plan, the policies incorporate the terms of reference for BORN Privacy and Security Review Committee, the BORN Data Collection Committee, BORN Data Disclosure Review Committee, the Research Review Committee, and the Data Quality 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
- Reports generated by the Committee[79]

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 are the agents 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 #

[79] The terms of reference in respect of the 3.0 Plan set out the reports produced, reviewed or approved. For the PSRC these include quarterly audit reports, audit plans, privacy impact assessments, threat risk assessments, business continuity and recovery plans, penetration tests. For the PHI Disclosure Committee, these include establishing precedents for acceptable levels of de-identification, including recommending changes to P-24 of the Privacy and Security Management Plan as appropriate. Documenting such decisions and identifying changes required to any existing agreements or BORN practices. For the Data Holding Committee, this includes review BORN's data holdings to ensure their statements of purpose are still relevant and retaining them is necessary for the identified purposes.

    - 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[80] 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.

[80] In the 3.0 Plan, the Information Security Officer is also responsible for the administration of this policy throughout as it pertains to security.

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 privacy and security policies were reviewed on an on-going basis from 2016 until 2018. That "on-going review" was intended to verify implementation of all policies and procedures and make any amendments necessary. A comprehensive governance review process was commenced in August 2018 to improve the operation of BORN's committees and the implementation of the policies and procedures. All committees reviewed their terms of references and elements of the privacy policies pertinent to each committee. In January 2019 additional work was commenced on security policy development which was focused on BORN's plan to migrate the BIS from a CHEO hosted solution to a solution hosted by Microsoft Azure. The policy work of both groups (i.e., the work related to the governance review and the work related to the Migration Project) was combined in September 2019 and was reviewed at the Privacy and Security Review Committee meetings in September and October. The resulting plan is referred to as "3.0 Plan" and is anticipated to become effective at or before the time of the Migration Project goes live (currently anticipated for December 2019) following approval by the Executive Director.

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 in the 3.0 Plan:

General updates:

The 3.0 Plan is amended to ensure that words used in the policies throughout the plan are defined to be the same as the Act. This helps to ensure better adherence to PHIPA and consistency throughout. Substantively, this impacts:

- The Definition of Agent now means "In relation to BORN, a person that, with the authorization of BORN, acts for or on behalf of BORN in respect of PHI for BORN purposes, and not the agent's own purposes, whether or not that agent has the authority to bind BORN and whether or not that agent is employed by BORN and whether or not the agent is being remunerated by BORN."
- The meaning of "Health Care" to cross reference s. 2 of the Act (instead of not being defined in the Plan).
- The meaning of "Service Provider" as an organization who provides goods or services under Section 10(4) of PHIPA and related provisions.

Other general updates are as follows:

- The role of Director is replaced with Executive Director.

- The role of Communications Lead was identified as the CHEO employee designated as such by the Executive Director and who is delegated certain responsibilities for implementing changes to web site materials and printed as described in this Plan.
- The role of Requestor is changed to Data Requestor and means a person requesting access to Personal Health Information or data created using Personal Health Information (such as aggregated data or De-identified Data).
- The role of Scientific Manager from the 2.0 Plan is changed to generally refer to the Data Request and Research Coordinators (except for those instances where a committee is used in place of the Scientific Manager). The Data Request and Research Coordinator(s) are delegated certain responsibilities for implementing activities related to use and scientific analysis of BORN information and disclosure requests (including de-identified and aggregated disclosure requests) as described in the Plan.
- The term De-identification is defined to mean the process of removing or obscuring personal information from a record or data set to the extent necessary so that it is no longer reasonably foreseeable in the circumstances that it could be used, either alone or in combination with other information, to identify an individual.
- The phrase De-identification Tools is defined to mean the software tools and related services, if any, used for the De-identification of data including (in the case of products marketed by Privacy Analytics or their successors) the products referred to as Eclipse and PARAT and any successor products used by BORN.
- The role of Information Security Officer is created to describe the employee delegated certain responsibilities for implementing activities related to technology and information security as described in the Plan. This role was formerly held by the Manager of Health Informatics.
- Words that no longer have any application such as "Legacy System Hosting Provider", LHIN (local health integration networks), OPSS (Ontario Perinatal Surveillance System) were removed
- The role of Privacy Officer is described to mean the employee who is delegated certain responsibilities for implementing activities related to privacy as described in the Plan.
- To improve readability, excessive repetition is removed from the document.

P-01: PRIVACY POLICY IN RESPECT OF CHEO'S STATUS AS A PRESCRIBED PERSON

This policy is substantively updated in the 3.0 Plan to reflect the current resourcing while at the same time ensuring that BORN has a privacy and security accountability framework to implement its status and overall responsibility as a prescribed person under PHIPA.

The policy is updated to describe that BORN Ontario is a Provincial Program, funded through the Children's Hospital of Eastern Ontario (CHEO) and as such, has direct accountability through CHEO's accountability structure. The policy goes on to describe that there are a number of committees that have been established to support BORN's Executive Director on matters of privacy, security and the collection, quality and disclosure of data, and those committees are specifically described.

The following figure reflects the new governance framework:

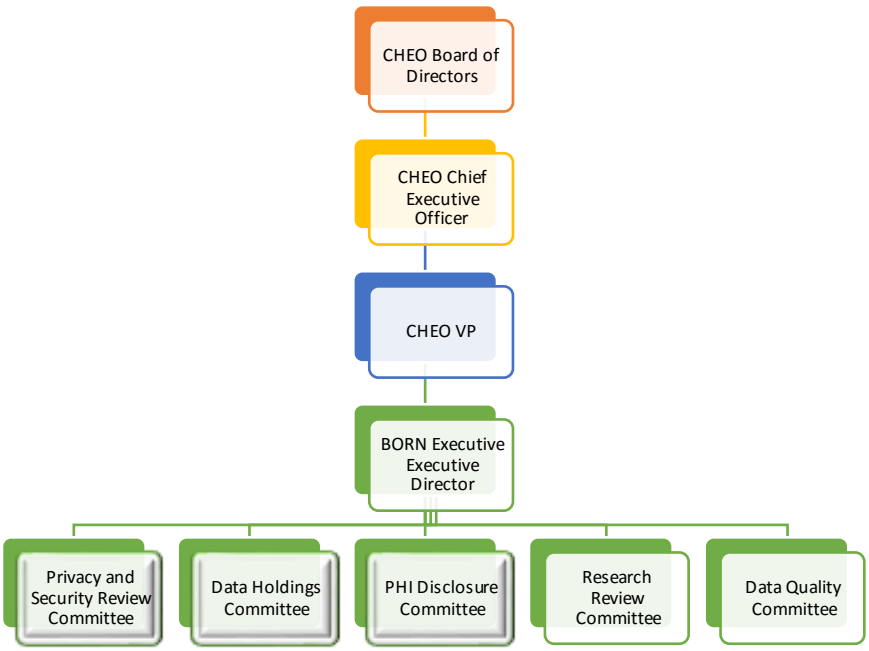


Figure 1: Accountability Structure

The policy describes that, as illustrated in figure 1, BORN's accountability is through CHEO. CHEO's CEO has delegated the day to day responsibility for ensuring compliance with PHIPA and its regulation to BORN's Executive Director. The policy explains that there are a number of committees that have been established to provide guidance and advice to BORN's Executive Director on matters of privacy, security and the collection, quality and disclosure of data. It also explains that the Executive Director receives guidance from two management teams – the BORN Executive Team and the BORN Leadership Team.

BORN reviewed and revised the terms of reference for each committee in connection with the development of the 3.0 Plan. The policy **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** in the 3.0 Plan describes the role of each of the committees in accordance with the following.

Privacy and Security Review Committee (PSRC)

The PSRC has the mandate to review and approve the necessary elements of BORN's privacy and security framework that are required for compliance with the Personal Health Information Protection Act, 2004 and its regulation as well as with guidelines for registries issued by the Information and Privacy Commissioner (IPC). Identifying and managing risk is part of the culture and day to day responsibility of all BORN staff. The PSRC is the escalation authority for significant privacy and security risks faced by BORN.

Data Holdings Committee (DHC)

The DHC ensures that the data that BORN collects is aligned with BORN's purposes, that BORN collects only the Personal Health Information than is reasonably necessary to meet those purposes and that a current listing and brief description of BORN's data holdings is developed and maintained. This includes identifying new statements of purpose that may improve or facilitate the provision of Health Care using BORN data holdings.

PHI Disclosure Committee (PDC)

The PHI Disclosure Committee (PDC) is responsible for reviewing and approving all requests for the disclosure of Personal Health Information pursuant to PHIPA and its regulation. The PDC also reviews and approves record level (i.e., non-aggregated) De-identified data disclosure requests. The PHI Disclosure Committee is also responsible for reviewing any changes to the methods used to De-identify Personal Health Information under **P-24: De-identification and Aggregation**.

Research Review Committee (RRC)

This is a new committee in the 3.0 Plan. The RRC is responsible for reviewing, approving and/or denying requests for the use of Personal Health Information for research purposes. The RRC is responsible for reviewing requests for the disclosure of Personal Health Information for research purposes which are ultimately referred to the PHI Disclosure Committee for approval.

Data Quality Committee (DQC)

This is a new committee in the 3.0 Plan. The policy describes that BORN is an authoritative source of accurate, trusted, and timely data used to monitor, evaluate, and plan for the best possible beginnings for lifelong health. The policy describes the purpose of the DQC as facilitating the implementation and refinement of BORN's data quality framework, including overseeing and assessing the quality of BORN's data and developing and implementing plans, processes and tools to enhance data quality.

Additional Roles and Responsibilities - Privacy Officer, Security Officer, and Data Request and Research Coordinator(s)

The policy is revised in the 3.0 plan to better clarify the responsibilities of the Privacy Officer, the Information Security Officer, and the Data Request and Research Coordinators. In this regard, the policy describes that the Executive Director has delegated responsibility for:

- Day to day management of privacy matters to the Privacy Officer.
- Day to day management of information security matters to the Information Security Officer.
- Day to day management of Research and other aggregated and/or De-identified disclosure requests for the purposes of improving or facilitating Health Care to the Data Request and Research Coordinator(s).

The policy in the 3.0 Plan is modified to state that the Privacy Officer, Information Security Officer and the Data Request and Research Coordinator(s) can delegate work to other BORN employees. It is also revised so that the Privacy Officer is not responsible for management of the security program or

execution of security training. Rather, these are now delegated by the Executive Director to the Information Security Officer, who also has responsibility for:

- Management of the security program, including monitoring compliance, conducting regular audits and providing reports to senior management and recommendations for changes to policy or procedures
- Execution and oversight of threat and risk assessments
- Execution and oversight of vulnerability assessments
- Any and all related security oversight
- The technology used to collect and securely store the Personal Heath Information used by BORN

The role of Data Request and Research Coordinator has been created in the 3.0 Plan as a partial replacement to the Scientific Manager. The policy describes that the Data Request and Research Coordinators have responsibility for coordinating the review of all use and disclosure requests with the PHI Disclosure Committee and/or the Research Review Committee to ensure that they comply with the requirements of PHIPA and its regulation. The Data Request and Research Coordinators are also responsible for ensuring that de-identification is conducted in accordance with the 3.0 Plan.

Changes to Section Describing Collection of Personal Health Information

The Data Collection Review Committee has been replaced by the Data Holdings Committee. The new policy in the 3.0 Plan sets out that BORN collects only those data elements that have been identified through the rigorous review process undertaken by the Data Holdings Committee. The Policy indicates that the Data Holdings Committee has been delegated responsibility for:

- reviewing new proposed BORN data holdings;
- reviewing new statements of purpose that may improve or facilitate the provision of Health Care;
- reviewing BORN's data existing holdings to ensure their statements of purpose are still relevant and necessary for the identified purposes including: the purpose of the data holding, the PHI contained in the data holding, the source(s) of the PHI, and the need for PHI in relation to the identified purpose.

Changes to Section Describing Disclosure of Personal Health Information

The policy is revised in the 3.0 Plan to describe that the PDC has responsibility for reviewing and approving all requests for record level disclosure of Personal Health Information. In the case of disclosure of Personal Health Information for research purposes, the RRC helps with that review process by first providing its recommendations to the PDC.

Changes to Section on Disclosure of De-identified and/or Aggregate Personal Health Information

The 3.0 Plan describes that De-identified and aggregated data generated from Personal Health Information may be disclosed to third parties. For example, these might include:

- Public Health Units to facilitate the appropriate planning, monitoring and provision of Health Care
- Researchers for Research purposes

- Ministry of Health to inform policy and planning

P-02 AND S-02: ONGOING REVIEW OF PRIVACY AND SECURITY POLICIES AND PROCEDURES

In the 3.0 Plan, this policy is changed to incorporate the role of the Information Security Officer in conducting the review (in addition to the Privacy Officer). This Policy is also changed to reflect that more frequent than annual is appropriate having regard to the nature of ongoing risks, organizational changes, or technology changes. The decision making process is revised to reflect the fact that the Executive Director has ultimate authority to approve the changes. Record keeping and document retention is revised to include records of decisions of the PSRC, any relevant correspondence, and no longer includes documents not relevant to the review and revision process.

In 3.0 of the Plan, the policy is changed to indicate that the Privacy Officer and Information Security Officer will prepare an annual report to be reviewed by the PSRC for approval by the Executive Director. Based on this report, each year the Vice President of Provincial Programs and CIO will be supplied with a written report by the Executive Director addressing the initiatives undertaken by the privacy and security programs including training, development of policies, procedures, audits undertaken, privacy impact assessments, threat risk assessments, privacy and security breaches, privacy complaints that were investigated, and the status of any recommendations that were made from the investigations.

The Plan's Privacy and Security Governance and Accountability Framework sets out that the Vice President of Provincial Programs and the CIO will present such findings to a committee of the CHEO Board of Directors. In this regard, briefings in respect of BORN are supplied to the Connected Care Committee which oversees provincial programs operating within CHEO. The Audit and Finance Committee is also briefed in regard to data security matters. The governance and accountability framework will be communicated to agents of BORN each year by the Privacy Officer at the annual training session.

P-04: COLLECTION OF PERSONAL HEALTH INFORMATION AND P-06 STATEMENTS OF PURPOSE FOR DATA HOLDINGS CONTAINING PERSONAL HEALTH INFORMATION

In the previous plan, the policy described the role of the Data Collection Review Committee (DRC) as having responsibility in reviewing each data element and data holding being collected, for any new data elements to be added to the data holding, to review existing statements of purpose and to review any requests for new statements of purpose. This included responsibility for determining the nature of the PHI required to enable BORN to fulfill its mandate, the list of data elements and data holdings to be collected and any sub elements as applicable, the health information custodians from whom the data elements will be collected, and the statements of purpose (rationale) for each data element in relation to the identified purpose of the registry.

As part of BORN's policy review process, the Committee reviewed its scope and purpose and revised its mandate and procedures. The revised policy sets out that the DHC will meet approximately every two months. Additional meetings will be scheduled as required. At the first meeting of the fiscal year, the DHC will develop its work plan and schedule for the year. The revised policy sets out that the DHC has responsibility for the following:

Statements of Purpose and BORN data holdings:

- Identify and consider any requests for new statements of purpose that may improve or facilitate the provision of health care using BORN data holdings.
- Identify the requirement for a Privacy Impact Assessment (PIA) of new holdings of data or PHI from data contributors in Ontario and review relevant PIAs, considering risks and mitigation strategies.
- Review any proposed new data holdings or any changes to existing data holdings, confirming the fit with BORN's purposes and recommending the approval, change, or rejection of the collection of these data holdings.
- On an annual basis, review BORN's data holdings to ensure their statements of purpose are still relevant and retaining them is necessary for the identified purposes.
- Revise documentation, as necessary, that includes the following for each data holding:
  - purpose of the data holding
  - PHI contained in the data holding
  - source(s) of the PHI including the health information custodians from whom the data will be collected
  - need for PHI in relation to the identified purpose
- Ensure that a summary list of BORN's data holdings of PHI are publicly communicated through BORN's website.

Disposal

Determine when the data collected by BORN is no longer needed to fulfill its purposes as a prescribed registry and collection of that particular data must be discontinued, and existing data must be de-identified or destroyed.

Data Elements and Enhancements

Review and advise on the addition of new data elements and review and approve proposed enhancements to existing BORN data elements to improve accuracy, clinical relevancy, usability and/or reliability considering whether:

- the data collection is permitted by the Personal Health Information Protection Act (PHIPA) and its regulation;
- any and all conditions or restrictions set out in PHIPA and its regulation have been satisfied;
- other information (i.e. de-identified and/or aggregate information) will serve BORN's purposes; and,
- no more PHI is being collected than is reasonably necessary to serve BORN's purposes.

The revised Policy sets out that the DHC will establish the necessary working groups to review proposed enhancements and BORN data elements in more detail for all of BORN's data holdings. Such working groups will address minor enhancements but all changes of substance will be reviewed and approved by DHC.

The revised Policy sets out that the review process should involve the following.

1. In determining the data holdings and data elements therein to be collected, and any new statements of purpose to be considered, the Data Holdings Committee may consult with health information custodians and key experts in the field of maternal, infant and child health and other experts as warranted.
2. In determining the data holdings and elements to be collected and their statements of purpose, the Data Holdings Committee considers whether:
    - The collection is permitted by PHIPA and its regulation
    - Whether other information, namely de-identified and/or aggregate information, will serve the purpose of the Registry,
    - Whether no more Personal Health Information is being requested than is reasonably necessary to meet the purpose of the Registry
    - Whether the rationale or statements of purpose for each data holding can be linked to the need for the data in relation to the identified purpose of the Registry
    - Any risks identified in privacy impact assessments undertaken by BORN regarding new data holding (where applicable)
    - Any conditions that must be satisfied prior to collection
    - Whether appropriate data sharing agreements are in place or pending.
3. In respect of any new data holdings or statements of purpose, the Data Holdings Committee will record in its record of decisions including:
    - The proposed list of data elements and/or data holdings and the associated statements of purpose
    - The proposed list of health information custodians from whom the data elements or data holdings will be collected
    - Any newly proposed statements of purpose that have been approved
    - Any changes to the content of policy **P-07: Statements of Purpose for Data Holdings Containing Personal Health Information** that are recommended as a result of new proposed statements of purpose
4. The DHC is accountable to and reports to the BORN Executive Director. Where significant changes to BORN's data holdings are proposed the DHC will inform the Executive Director. On an annual basis, the DHC will provide an update on BORN's data holdings, data elements, and enhancements to BORN's Executive Director.
5. The Privacy Officer has responsibility for ensuring that a signed data sharing agreement is executed before data are collected. Where there are revisions made to data holdings, a revised data sharing agreement must be completed before collection of data proceeds. See P-16: Data Sharing Agreements. All BORN statements of purpose are outlined in data sharing agreements. The Privacy Officer will ensure that, to the extent not reflected in any pre-exiting data sharing agreements that expressly list approved purposes, any new purposes will be incorporated as each agreement is amended or restated.

6. The DHC will ensure any new statements of purpose that have been approved are reflected in an update to **P-07: Statements of Purpose for Data Holdings Containing Personal Health Information**.
7. The DHC will inform Service Providers (as appropriate) and ensures that any conditions or restrictions that must be satisfied prior to the collection of Personal Health Information have been satisfied.
8. The DHC will inform the Communications Lead in order to update the website with any changes to the data holdings, the Personal Health Information contained in each data holding, the source of the Personal Health Information and/or the statement of purpose for each data holding in relation to the identified purpose of the Registry. Changes to collections and statements of purpose are made public in accordance with **P-03: Transparency of Privacy Policies and Procedures**.
9. The Privacy Officer is to ensure that updates **P-07: Statements of Purpose for Data Holdings Containing Personal Health Information** that include new statement of purpose are communicated to Agents.

P-05: LIST OF DATA HOLDINGS CONTAINING PERSONAL HEALTH INFORMATION

In the 3.0 Plan policy **P-05: List Of Data Holdings Containing Personal Health Information** is amended to reflect that the Genetics/MFM Encounter is formed by the merger of encounters for prenatal screening follow-up and antenatal specialty for fetal anomalies information.

P-08: LIMITING AGENT ACCESS TO AND USE OF PERSONAL HEALTH INFORMATION

In 3.0 of the Plan, policy **P-08: Limiting Agent Access to and Use of Personal Health Information** now establishes that all agents must be approved for access to and use of Personal Health Information by completing one or both of the following:

1. P-08A: BORN PHI Access Request Form: BORN Information System (BIS)
2. P-08B: BORN PHI Access Request Form: BORN PHI Drive

In respect of "P-08B: BORN PHI Access Request Form: BORN PHI Drive", the policy now sets out:

A copy of the Standard Operating Procedure (SOP) for access to the BORN PHI Drive is stored on the Departmental Drive (\General\Standard Operating Procedure (SOP)).

P-10: USE OF PERSONAL HEALTH INFORMATION FOR RESEARCH

This policy is amended in the 3.0 Plan to provide that agents interested in a prospective research project should first consult with the appropriate subject matter expert within BORN. This facilitates identification of potential redundancy in research or opportunities for collaboration.

This policy is also amended to specifically define what is meant by "Research" to ensure that proper tests are applied in alignment with the requirements of the Act; i.e., the policy reiterates that in the context of PHIPA, "research" means a systematic investigation designed to develop or establish

principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research.

This policy is also amended to specify what material the Research Review Committee should review in making its determinations; i.e., the Data Request Form, the Research plan, a copy of the decision of a Research Ethics Board that approved the research plan (unless such approval is still pending), any relevant electronic correspondence with the Agent regarding the research request (where such information has not been otherwise supplied or summarized), and the list of the proposed data elements.

P-11 A: DATA TRACKING LOG

The fields to the data tracking log are updated in the 3.0 Plan to include description of data request.

P-12: DISCLOSURE OF PERSONAL HEALTH INFORMATION FOR PURPOSES OTHER THAN RESEARCH

In 3.0 of the Plan, this policy is changed to reflect that any decisions made by the PHI Disclosure Committee to disclose personal health information will be referred to and must involve the Executive Director and be approved by the Executive Director.

P-12 A: DATA REQUEST FORMS

This policy is changed in the 3.0 Plan to indicate that all forms are available at the BORN website.

P-13: DISCLOSURE OF PERSONAL HEALTH INFORMATION FOR RESEARCH PURPOSES AND THE EXECUTION OF RESEARCH AGREEMENTS

This policy is changed in the 3.0 Plan to reflect that the Research Review Committee and the Data Request and Research Coordinator have now taken on the roles that were delegated to the Scientific Manager in the 2.0 plan. The disclosure of personal health information that has not undergone de-identification (or de-identification through aggregation) is reviewed and approved by the PHI Disclosure Committee (rather than the Privacy and Security Review Committee).

The terms of reference for the PHI Disclosure Committee require the PDC to consider (i) the legal authority of the prospective disclosure request with reference to PHIPA; (ii) the background of the project including how it aligns with BORN purposes (or other considerations pertaining improving or facilitating the provision of Health Care – in this respect, the PDC may refer requests that require consideration of a new or revised purpose to the Data Holdings Committee); (iii) advice or recommendations provided by the Data Request and Research Coordinator, BORN Privacy Officer and other BORN staff or outside consultants or experts; (v) whether more data is being requested than is necessary for the purpose; (vi) the list of agreed-upon data elements and whether there are opportunities to de-identify any data; (vii) contractual restrictions under data sharing agreements that

might restrict the disclosure; (viii) the location/jurisdiction of the recipient and its data security and privacy practices; (ix) the legal terms that would apply to the disclosure and protection of PHI during its intended use and subsequent destruction; and (x) any other relevant privacy, security, or legal considerations that might warrant refusing the requests.

P-15: LOG OF RESEARCH AGREEMENTS

This policy was updated to reflect the following fields for capture in the Log of Research Agreements:

- Name of research study
- Principal researcher last name
- Principal researcher first name
- Date of written application received
- Date of written research protocol received
- Date of Research Ethics Board written decision approving plan
- Dataset de-identified (Y/N)
- If NO to de-identification provide explanation
- Date Research Agreement executed
- Date of approval to disclose personal health information or de-identified data for research was granted (by BORN Research Review Committee)
- Date personal health information or de-identified data was disclosed
- Nature of personal health information or de-identified data (data source description)
- PHI or de-identified data
- Retention period as per Research Ethics Board
- Secure disposal due date
- Date certificate of destruction was received
- Any Research Agreement amendments

P-17A: TEMPLATE DATA SHARING AGREEMENT: COLLECTION OF PERSONAL HEALTH INFORMATION WAS UPDATED TO REFLECT THE FOLLOWING CHANGES:

The following reflects the changes made:

Date	Change

Fall 2016/Winter 2017	Reference to authorized user in 8.2 b changed/corrected; incorrectly referred to 8.3 and now corrected to refer to 2.4
March 1, 2017	Schedule A – List of PHI was changed to more accurately reflect that changes to data elements on the BORN website would be pursuant to the BORN data element review process
April 2019	As per PIA recommendation, paragraph 5.1 revised to forbid third-party service providers from using PHI for their own purposes and identify that any access to PHI in the custody of BORN is a use of PHI by BORN and not a disclosure of PHI to the service provider.

P-19: EXECUTING AGREEMENTS WITH THIRD PARTY SERVICE PROVIDERS IN RESPECT OF PERSONAL HEALTH INFORMATION

This policy is updated in the 3.0 Plan to provide that each Agreement is normally based on the template. Material variations to the template are to be approved by the Executive Director and CHEO legal. This means that BORN will have more latitude to alter the terms in which it contracts with service providers in regard to industry standards.

P-24: DE-IDENTIFICATION AND AGGREGATION

This policy in the 3.0 plan is updated to incorporate a standard procedure using the De-identification Software. This SOP was created in response to a substantial upgrade to the software tool used by BORN to perform de-identification to improve use of the software.

P-29 PRIVACY BREACH MANAGEMENT

This policy is amended in the 3.0 Plan to ensure that the Executive Director and the Privacy Officer factor in legal requirements and IPC guidance's to provide notification under PHIPA, in addition to all other factors listed in the 2.0 plan. A provision that made use of a CHEO Incident Report using the AEMS System is removed.

Indicator:
The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.

BORN Response:

The 2.0 Plan was made available at the BORN website in July 2018 (replacing the prior version) and a draft was communicated to agents in October 2016 through email.

The Policy was not updated since the prior review although a comprehensive update (i.e., the 3.0 Plan) is planned to become effective in December 2019.

Specifically, Version 3.0 of the BORN Privacy and Security Management Plan will be e-mailed to all BORN Agents by the Privacy Officer as soon as it has been approved by the BORN Executive Director. In this respect, the 3.0 Plan includes revisions designed for operation of the BIS in Microsoft Azure, together with updated governance changes as described herein. Because it encompasses changes for Microsoft Azure, it will be approved and communicated to Agents before the go-live date of the Migration Project (this is currently anticipated to be in December 2019).

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.

In August 2019 the BORN website was updated to include summaries of privacy impact assessments and a description of data security, all as part of a complete web-site redesign.

The 3.0 Plan will be made available on the BORN Website within 7 days of it becoming effective.

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. These are six original (existing) statements of purpose that were approved when BORN received registry status in 2011.

Indicator:

The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the Information and Privacy Commissioner of Ontario.

BORN Response:
The following (6) statements of purpose for data holdings containing personal health information are reviewed 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 Heath Units with comprehensive and timely information to support effective planning and management of health care delivery for mothers, babies and children in the province.

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. It is anticipated that BORN's statements of purpose will be amended to include a new purpose for pre-population of important data elements within the circle of care of a pregnancy, to improve the accuracy or completeness of data and reduce the burden of re-entry.

It is anticipated that this will be considered and addressed by the Data Holdings Committee by April 1, 2020. The rationale is to collect the data closer to the time when care occurs (compared to retrospective entry after the event), primarily to improve the accuracy and completeness of data and secondarily to reduce the burden of data entry on clinicians. A specific example relates to the collection and use of data provided by midwifery practice groups in instances where a woman under midwifery care plans to

deliver or unexpectedly delivers at a hospital. BORN prepopulates data entered in the BORN Information System by midwifery practice groups (at the point of, and within the circle of care) directly into the appropriate birthing hospital encounter in the BORN Information System thereby improving the accuracy and completeness of data which may be important to facilitating subsequent health care for the woman and baby and also reducing the burden of data entry when the hospital's BORN record is normally created after the birth. This also helps to reduce patient safety risks caused by incomplete or inaccurate data. As well, busy clinicians are more available for patient care when a percentage of the data that is normally collected after a birth is already in the Born Information System and available for future care planning. The procedure for adding new purposes has been clarified in the 3.0 Plan. In **P-04: Collection of Personal Health Information and P-06: Statements of Purpose for Data Holdings Containing Personal Health Information**, the Data Holdings Committee may review and approve new statements of purpose and amend **P-07: Statements of Purpose for Data Holdings Containing Personal Health Information** accordingly.

Use

Indicator:
The number of agents granted approval to access and use personal health information for purposes other than research.

BORN Response:
44 agents were approved to access and use personal health information in the BORN Information System for purposes other than research, between November 1, 2016 and October 31, 2019.

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

49 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:
18 requests received. Note: This number is as of Oct 24, 2019

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:
18 requests granted; 0 denied. Note: This number is as of Oct 24, 2019

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:
27 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:

- 25 requests from Public Health Units in Ontario for access to the Healthy Babies Healthy Children Screen
- 2 request from a Prescribed Entity (under PHIPA reg. 329/07 s.18)

Note: These numbers are as of Oct 24, 2019

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:
27 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:

- 25 requests from Public Health Units in Ontario for access to the Healthy Babies Healthy Children Screen
- 2 request from a Prescribed Entity (under PHIPA reg. 329/07 s.18)

Note: These numbers are as of Oct 24, 2019

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:
No 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
No requests were denied
Note: This information is as of Oct 24, 2019

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. Note: This information is as of Oct 24, 2019

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

- 15 requests for the disclosure of de-identified information for research purposes
- 90 requests for the disclosure of aggregate information for research purposes
- 438 requests for the disclosure of aggregate information for non research purposes

Note: These numbers are as of Oct 24, 2019

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:

- 5 research agreements executed for the disclosure of de-identified information
- 1 data sharing agreement executed for the disclosure of aggregate information for purposes other than research
- 333 acknowledgements received for the disclosure of aggregate information for research and other purposes
- 142 acknowledgements not received; these data requests were granted but acknowledgement are still outstanding;

Note: These numbers are as of Oct 24, 2019

As a corrective measure, BORN is implementing a change to its procedures to ensure that all acknowledgments are obtained and recorded automatically in advance using our electronic forms. This procedure change is part of our redesigned DART process and the new forms will be implemented on or before October 31, 2020. The revised 3.0 Plan expressly includes this requirement

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:

80 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:

- 26 are new agreements with health information custodians from whom BORN began collecting personal health information
- 54 are amended agreements executed with health information custodians in collect additional 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:
25 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:
11 data linkages approved as follows:

1. BIS-CIHI: Investigating the relationship between prenatal screening results and adverse pregnancy and birth outcomes

2. BIS-CIHI: Identifying modifiable factors to improve access to and perinatal outcomes of assisted conception in Ontario
3. BIS – CIHI: Maternal socioeconomic disparities and risk of congenital heart diseases: A population-based study in Ontario
4. BIS-CIHI: Adverse outcome indicators (AOI) by grouped pre-existing maternal health conditions for pregnancies in Ontario
5. BIS-CIHI: Gestational weight loss in obese women and risk for adverse perinatal outcomes
6. BIS-CIHI: Timing of Delivery in Women with Pre-existing Hypertension
7. BIS-CIHI: Advanced maternal age in twins in women with and without DOH
8. BIS-CIHI: Has redefining preeclampsia influenced rates of indicated preterm birth and associated adverse pregnancy outcomes?
9. BORN-CIHI: ED visits in Ontario neonates preliminary results the abstract for BORN Conference
10. BORN-CIHI: ED visits in Ontario neonates
11. On-going linkages of the BORN Information System (BIS: the BORN Information System links records collected from various health information custodians to create a longitudinal profile

Note: These numbers and information are as of Oct 24, 2019

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:

Three (3) privacy impact assessment were completed as follows.

1. BIS Migration to Cloud – Completed March 31, 2018. Migration of the BORN Information System (BIS) from the CHEO-OCTC Information Technology Shared Services Department (IT SSD) hosting infrastructure into the Microsoft Azure Cloud using the services of Dapasoft, a Microsoft partner and the developer of the BORN Information System (BIS).

A brief description of each recommendation	The date and the manner in which each recommendation was addressed or is proposed to be addressed
1. Clarify services, contractual relationships, PHIPA roles, and privacy obligations for the BIS-to-Cloud project.	A substantial revision to BORN's agreement with its service provider has been prepared. Such amendment will be signed before the migration goes live.

2. Identify and conduct any updates to privacy and security policies and procedures that are needed to support privacy in the BIS-to-Cloud project (where required to align with updates to security policies, procedures, and standards, including IPC requirements) (See also TRA for further guidance on security policies and procedures for the cloud)	This is addressed with the 3.0 Plan. This will become effective before the migration goes live.
3. Ensure access controls for BORN, Dapasoft (and Dapasoft's subcontractor, Microsoft), and CHEO IT support limits on staff access to PHI because of the BIS-to-Cloud project, namely through: • Access control matrices; • Job descriptions; • Provisioning and de-provisioning practices; and • Lists of staff with access to PHI.	To be completed before the migration goes live. In the 3.0 Plan role-based access controls will be described in changes to the security policies that pertain to Azure and key management - Policy S-21: Roles Based Access Controls for the Azure Environment. These will also be incorporated into the Dapasoft Agreement. Role descriptions for the management of Azure will be described in the 3.0 Plan and the Dapasoft Agreement for those specific staff who have access to encryption keys or access to PHI for development purposes (if any). Details pertaining to provisioning and de-provisioning practices for the role-based descriptions are built into the security policies for Dapasoft employees.
4. Set retention schedules for temporary or duplicate copies of PHI where they are not yet established, or they need to be updated for the migration of the BIS to the cloud and the ongoing management of PHI in the cloud.	S-05: Retention of Records of Personal Health Information - Temporary Storage section details retention period for temporary or duplicate copies of PHI. In the Dapasoft Agreement, Dapasoft is required to retain records of PHI in a secure manner that includes encryption, audit trails, intrusion and alteration alert systems, all in accordance with the above policy. In particular, Dapasoft is required to take steps that are reasonable in the circumstances to ensure that any PHI to which it has access to or that it has in its custody in the course of providing the services is protected against theft, loss and unauthorized use or disclosure and is protected against unauthorized copying, modification or disposal.

	Dapasoft is required to implement password protections, encryption, role-based access, and audit systems for records of personal health information retained in electronic media.
5. Set secure storage requirements for temporary, duplicate, or backup copies of PHI where they are not yet established for the migration of the BIS to the cloud and the ongoing management of PHI in the cloud. (See TRA for further guidance on secure storage)	To be completed before the migration goes live. These requirements are established in **S-05: Retention of Records of Personal Health Information** - Temporary Storage section details retention period for temporary or duplicate copies of PHI. Backup copies are maintained as per policy "**S-13: Back-up and Recovery of Records of Personal Health Information**". Retention schedules are detailed in the BORN-Azure Environment Disaster Recovery Plan.
6. Set secure disposal requirements for temporary, duplicate, or backup copies of PHI where they are not yet established for the migration of the BIS to the cloud and the ongoing management of PHI in the cloud. (See TRA for further guidance on secure disposal)	To be completed before the migration goes live. Policy "S-08: Secure Disposal of Records of Personal Health Information" details the disposal of all PHI. At the end of the agreement and upon written request of BORN, Dapasoft is required to ensure that all PHI that are described in such written request and that Dapasoft has in its custody will be disposed of in a secure manner within thirty (30) days of such termination or written request. In particular, all PHI will be disposed of in accordance with the BORN's Policies. A certificate of destruction setting out the data, date, time, location and method of secure destruction employed, and bearing the name and signature of the person who performed the secure destruction will be issued to the BORN Privacy Officer within seven (7) days of the destruction. BORN may witness the secure disposal.

2. Various Programs – Completed November 9, 2018 - privacy impact assessment on three BORN program initiatives as follows:
   - Sending completed Healthy Babies Healthy Children (HBHC) screens from hospitals to public health units (PHUs) and sending missed screening alerts to PHUs where a HBHC screen has not been completed in the hospitals;
   - Sending missed immunization alerts to PHUs where babies and children have not been immunized; and

- Collecting additional data about a child's growth parameters (height and weight) and lifestyle from primary care to facilitate the province's Health Growth Initiative (HGI).

A brief description of each recommendation	The date and the manner in which each recommendation was addressed or is proposed to be addressed
1. Discuss with primary care how PHIPA relationships in the primary care setting are defined in agreements to: • Support both parties in having confidence that the appropriate person is signing the DSA with BORN; and • Identify technical requirements for the EMR and the BIS to support the authorized disclosure of PHI to BORN i.e., limit disclosures of PHI to only authorized physician(s) if the physician(s) shares an EMR with other providers that do not disclose PHI to BORN.	Recommendation addressed May 2018 • Intake process strengthened to include thorough discussions with site to ensure appropriate signing authority for DSA execution process • Intake process strengthened to include thorough discussions with site to ensure PHI only accessed by authorized persons as per DSA

3. Prenatal Screening Program – November 20, 2018
   1. Ascertain the privacy risks associated with operationalizing the Prenatal Screening Program under the Registry, including the individual provider-related Quality Assurance activities.
   2. Examine a new registry collection of antenatal and pediatric microarray results from Ontario's cytogenetics laboratories.
   3. Examine Health Information Network Provider (HINP) status related to prenatal screening results

A brief description of each recommendation	The date and the manner in which each recommendation was addressed or is proposed to be addressed
1. Revise the data sharing agreement (DSA) template to forbid third-party service providers from using PHI for their own purposes and identify that any access to PHI in the custody of BORN is a use of PHI by BORN and not a disclosure of PHI to the service provider.	The Data Sharing Agreement template was revised on May 16, 2019
2. Revise the Privacy Requirements for BORN Projects and New Collections form with similar considerations for the disclosure of PHI to any person including health care providers.	A Privacy Requirements for Disclosure of PHI form is under development and anticipated to be fully implemented by end of 2019 or early 2020
3. Ensure the PSP website has a plain language description of BORN's role in operating the PSP and	The new PSP website was launched on August 18, 2019 and includes a plain language description of

links to the BORN plain language notice on its organizational website.	BORN's role in operating the PSP along with links to the BORN website.

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:
There were no privacy impact assessment undertaken but not completed.

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:
None.

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:
The DCRC and PSRC considered the merger of the Prenatal Screening Follow-Up (PSFU) encounter with the Antenatal Specialty (AS) encounter to form the Genetics/MFM encounter. This merger reduced the amount of data collected from 80 data elements (in the AS encounter) and 47 data elements (in the PSOFU encounter) to 19 data elements in total. The determination that a PIA was not required was made by the Privacy and Security Review Committee because fewer data elements would be collected as a result of the merger of the two encounters, resulting in net reduction in personal health information being collected as a result of the change.

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:
Three (3) privacy impact assessment reviewed in 2018 all of which are described in detail above.

1. Migration to Microsoft Azure
2. Various programs
3. Prenatal Screening Program

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 24, 2017	Verify BIS audit logs of system activity by two (2) BORN employees with access to PHI. One from Oct 12/16 to Feb 23/17 and the other from Jan 1/17 to Feb 23/17. No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI.
April 27, 2017	Verify BIS audit logs of system activity by two (2) BORN employees with access to PHI from Jan 1/17 to Apr 27/17. No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI.
May 26, 2017	Verify BIS audit logs of system activity by four (4) BORN employees with access to PHI as follows: One (1) from Apr 27/17 to May 26/17 Two (2) from Jan 1/17 to May 26/17 One (1) from Sep 1/16 to May 26/17 No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI.
June 15, 2017	Verify BIS audit logs of system activity by three (3) BORN employees with access to PHI from May 15, 2017 to June 15, 2017. No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI. Audited a recent family member birth of a BORN Agent. Audit revealed that there was no unauthorized access. No recommendations. All activity in line with expectations.
July 31, 2017	Verify BIS audit logs of system activity by five (5) BORN employees with access to PHI from Jun 1/17 to July 31/17. No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI.
October 26, 2017	Verify BIS audit logs of system activity by eight (8) BORN employees with access to PHI from Sep 1/17 to Sep 30/17. No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI.

November 24, 2017	Verify BIS audit logs of system activity by four (4) BORN employees with access to PHI from Nov 1/17 to Nov 30/17. No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI.
January 25, 2018	Verify BIS audit logs of system activity by four (4) BORN employees with access to PHI from Dec 1/17 to Jan 25/18 No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI.
February 22, 2018	Verify BIS audit logs of system activity by six (6) BORN employees with access to PHI from Jan 1/18 to Feb 22/18 No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI.
April 26, 2018	Verify BIS audit logs of system activity by four (4) BORN employees with access to PHI from Mar 26/18 to Apr 25/18. No recommendations. All activity in line with expectations
May 24, 2018	Verify BIS audit logs of system activity by four (4) BORN employees with access to PHI from Apr 24/18 to May 24/18. No recommendations. All activity in line with expectations
July 10, 2018	Verify BIS audit logs of system activity by three (3) BORN employees with access to PHI from Jun 1/18 to Jul 10/18. No recommendations. All activity in line with expectations
September 18, 2018	Verify BIS audit logs of system activity by eight (8) BORN employees with access to PHI from Aug 1/18 to Sep 18/18. No recommendations. All activity in line with expectations
October 26, 2018	Verify BIS audit logs of system activity by five (5) BORN employees with access to PHI from Sep 26/18 to Oct 26/18. No recommendations. All activity in line with expectations
November 13, 2018	Verify BIS audit logs of system activity by ten (10) BORN employees with access to PHI from Oct 1/18 to Nov 13/18. No recommendations. All activity in line with expectations
December 18, 2018	Verify BIS audit logs of system activity by six (6) BORN employees with access to PHI from Nov 18/18 to Dec 18/18. No recommendations. All activity in line with expectations
January 15, 2019	Verify BIS audit logs of system activity by seven (7) BORN employees with access to PHI from Dec 15/18 to Jan 15/19. No recommendations. All activity in line with expectations
February 26, 2019	Verify BIS audit logs of system activity by seven (7) BORN employees with access to PHI from Jan 26/19to Feb 26/19. No recommendations. All activity in line with expectations
March 19, 2019	Verify BIS audit logs of system activity by eight (8) BORN employees with access to PHI from Feb 19/19to Mar 19/19. No recommendations. All activity in line with expectations
April 16, 2019	Verify BIS audit logs of system activity by eight (8) BORN employees with access to PHI from Mar 16/19to Apr 16/19. No recommendations. All activity in line with expectations
May 22, 2019	Verify BIS audit logs of system activity by ten (10) BORN employees with access to PHI from Apr 22/19to May 22/19. No recommendations. All activity in line with expectations

June 7, 2019	Verify audit logs of system activity by BORN Senior Technical Architect. No recommendations. All activity in line with expectations of BORN System Administrator role.
June 20, 2019	Verify BIS audit logs of system activity by twelve (12) BORN employees with access to PHI from May 20/19to Jun 20/19. No recommendations. All activity in line with expectations
July 17, 2019	Verify BIS audit logs of system activity by ten (10) BORN employees with access to PHI from June 17/19 to July 17/19. No recommendations. All activity in line with expectations
Aug 20, 2019	Verify BIS audit logs of system activity by nine (9) BORN employees with access to PHI from July 20/19to Aug 20/19. No recommendations. All activity in line with expectations
Sep 17, 2019	Verify BIS audit logs of system activity by ten (10) BORN employees with access to PHI from Aug 17/19 to Sept 17/19. No recommendations. All activity in line with expectations
Oct 15, 2019	Verify BIS audit logs of system activity by eight (8) BORN employees with access to PHI from Sep 15/19 to Oct 15/19. No recommendations. All activity in line with expectations

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:
17 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	February 9, 2017 CIHI DSA Audit conducted to ensure that BORN is compliant with all conditions contained in the DSA	Findings: Audit revealed that the epidemiologist assigned to manage the deliverables in consultation with the Privacy Officer did not fully transition this role to the new epidemiologist when that employee left BORN. As a result of this audit the following recommendations were made: 1. Create a standing annual audit of the CIHI agreement to ensure full compliance with all terms 2. Data Access Request Team (DART) to identify a subject matter expert to manage reporting and usage of CIHI data 3. Usage Report will include the additional BORN-only columns to ensure appropriate monitoring of data destruction: All recommendations implemented October 25, 2017
2	February 14, 2017 Audit to ensure that there is a signed BORN Confidentiality Agreement in place for all BORN Agents	No recommendations. All documentation in line with expectations
3	February 15, 2017 Audit conducted to ensure Agent Data Access documentation in place for all BORN Agents with BORN Information System access.	No recommendations. All documentation in line with expectations
4	March 1, 2017 Audit of P-18 Log of Data Sharing Agreements to cross-check that each logged entry has a printed agreement.	No recommendations. All logged entries had a corresponding printed data sharing agreement in place
	June 15, 2017 Audited a recent family member birth of a BORN Agent to ensure no unauthorized access.	No recommendations. No unauthorized access found.
5	June 21, 2017 Audit of Third-party Service Agreement – Health Information Access Layer (HIAL) requesting confirmation of compliance with all provisions in the agreement	No recommendations. Confirmation of compliance with all terms in the agreement received on November 23, 2017
6	October 31, 2017 Renewal of Confidentiality Agreement of all BORN Agents – audit ensured that all BORN Agents re-confirmed their confidentiality pledges	No recommendations. All BORN Agents renewed their confidentiality pledge
7	November 7, 2017 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.	No recommendations. All recipients advised full compliance with the terms of the agreement.

8	September 29, 2017 Audit PHI Drive access of a BORN employee who left BORN to ensure that access was removed appropriately	No recommendations as System Administrator confirmed that access was removed appropriately.
9	October 10, 2017 Audit of a Disclosure agreement recipient BORN requested compliance with the agreement in general and specifically that only authorized agents have had access to the data provided under the agreement	No recommendations. Audit confirmed compliance with the agreement and that only authorized users had access to the data.
10	October 31, 2017 Compliance audit with two (2) Research Agreements recipients requesting confirmation of compliance with the agreement in general and specifically with respect to Disclosure, Terms of Use and Security	No recommendations. Audit confirmed that researchers were fully compliant with agreement terms.
11	November 14, 2017 Audit report verified by all managers to review BORN agent roles/access to the BORN Information System and confirm on-going access/remove or edit access.	Recommendation: adjust access for two (2) agents. Addressed: date implemented: November 14, 2017 by Sr. Technical Architect.
12	October 23, 2018 Renewal of Confidentiality Agreement of all BORN Agents – audit to ensure all BORN Agents re-confirmed their confidentiality pledge annually	No recommendations. All BORN Agents re-confirmed their confidentiality pledge
13	November 14, 2018 Audit BORN Confidentiality Agreement documentation retention to ensure that a signed agreement in place for all BORN Agents	No recommendations. All documentation in place and in good standing
14	December 3, 2018 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.
15	March 2019 Audit of agreement log (P-18) to ensure accuracy of all information in the log is correct and to ensure that the hard copy file matches the electronic files.	Minor corrections made to ensure all hard copy documentation matched electronic files. No recommendations
16	July 16, 2019 Audit of HR logs to ensure accuracy information pertaining to initial and ongoing privacy and security training	No recommendations. All documentation in place and in good standing

17	October 15, 2019 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 as well as confirmation of compliance with the data sharing agreement terms	No recommendations. All recipients reviewed list of users and removed access for those users no longer requiring access and provided a confirmation of compliance of all data sharing agreement terms

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 privacy and security policies were reviewed on an on-going basis from 2016 until 2018. That "on-going review" was intended to verify implementation of all policies and procedures and make any amendments necessary. A governance review process was commenced in August 2018 to improve the operation of BORN's committees. All committees reviewed their terms of references and elements of the privacy policies pertinent to each committee. In January 2019 additional work was commenced on security policy development, which was focused on BORN's plan to migrate the BIS from a CHEO hosted solution to a solution hosted by Microsoft Azure. The policy work of both groups was combined in September 2019 and was reviewed at the Privacy and Security Review Committee in September and October. The resulting plan is referred to as "3.0 Plan" and is anticipated to become effective at or before the time the Migration Project goes live (currently anticipated for December 2019).

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 general updates listed above in respect of Privacy Indicators also apply to this Section. The following is a list and description of security policy amendments reflected in the 3.0 Plan as a result of the on-going review:

S-01: INFORMATION SECURITY POLICY

Added multifactor authentication for all registry users (i.e., CHEO employees and agents).

Added a provision requiring that independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure that the organization addresses any nonconformities of established policies, procedures, and known contractual, statutory, or regulatory compliance obligations.

S-03: ENSURING PHYSICAL SECURITY OF PERSONAL HEALTH INFORMATION

Added to the policy that 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 Agents work and to secure locations within the premises where records of personal health information are retained. In the policy, two types of access are defined:

1. The BORN premises where CHEO 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 Hosting Service Provider.

References to security measures for the CHEO data center were removed since Microsoft will become the new supplier of hosting services (referred to below as the "Hosting Service Provider").

Added that the Hosting Service Provider data centers all receive SSAE16/ISAE 3402 Attestation and are ISO 27001 certified. Microsoft manages access to the Data Centre as follows:

- Datacenter entrances are guarded 24x7x365 by security personnel.
- Access to all Hosting Service Provider buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Data Centers.
- Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards.
- Staff must wear identity badges at all times, and are required to challenge or report individuals without badges.
- All guests are required to wear guest badges and be escorted by authorized Hosting Service Provider personnel.

- Azure Employees and contractors must have a business need to enter a Hosting Service Provider data center and have received prior approval.
- Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis.

S-05: SECURE RETENTION OF RECORDS OF PERSONAL HEALTH INFORMATION

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

Added a provision that data on the database servers is protected using native Transparent Data Encryption (TDE). For all other data at rest, encryption is enabled per-volume for disks, and per-container (or container) for blob storage. This applies both to data stored on disks/volumes, as well as data stored in object storage. BLOB storage has server-side encryption implemented.

Added a provision that record-level data files are retained on the BORN PHI drive. Such data may be 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.

Added that the following additional safeguards are in place for records of personal health information retained on the BORN PHI drive:

- Personal health information is collected via secure FTP as **per 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 an Agent.
- Data Request and Research Coordinator 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 premises is controlled as per **S-03: Ensuring Physical Security of Personal Health Information**.

The policy also describes BORN Temporary Storage and its safeguards.

In order to facilitate the day to day operations of BORN, the use of temporary data storage is required. Temporary data storage is required for, but not limited to: the collection of personal health information; testing of Disaster Recovery Procedures; testing of data backups; and migration of data to BORN's cloud environment. Data residing in temporary locations will only be for the amount of time required to import the data into the BORN Information System and/or storing the data on the BORN PHI drive after which time it will be deleted.

Temporary locations are:

- The BORN secure FTP server

- BORN SQL server file systems (for backup and restore files)

S-06: SECURE RETENTION OF RECORDS OF PERSONAL HEALTH INFORMATION ON MOBILE DEVICES

Removed reference to use of VPN connection to the e-Health Ontario (eHO) ONE network, since this is no longer applicable post migration.

Added requirement for multifactor authentication.

S-07: SECURE TRANSFER OF RECORDS OF PERSONAL HEALTH INFORMATION

Added Secure Transfer in to BORN:

1. Personal Health Information collected electronically from Health Information Custodians is transferred in one of the following ways:

    a. Direct connection to the BORN portal by:

        i. using a browser with industry standard SSL encryption, or

        ii. HL7 feed directly from hospital systems using a secure VPN connection

    b. BORN Hosting Provider

2. Secure FTP

3. BORN Secure Web Service

    a. Users on the public Internet must establish a SSL connection to the BORN Secure Web Service; this requires token-based dual authentication

4. Ontario Health's Connected Backbone (Health Information Access Layer or HIAL)

    a. Organizations on the public Internet require ONE ID certificate authentication to access the HIAL Health Information Network Provider (HINP) to transfer Personal Health Information to BORN

BORN applications have idle timeouts implemented to safeguard the data.

S-09: PASSWORDS

Added that Multi-Factor Authentication (MFA) is required for all BORN Information System users. There are currently 2 options for MFA: For users in organizations that cannot have access to a smart phone or direct phone number (PIN) and for users in organizations that have access to a smart phone (One-time use code)

For users in organizations that cannot have access to a smart phone or direct phone number

- The public IP address of the site must be registered in the BIS.
- Any attempt to access the BIS from an unlisted site by a user who is setup for this option must result in denied access to the BIS.

- A user logging in from a registered site must enter an alphanumeric PIN which is setup during the user registration process.
- The PIN must be 6-8 characters in length and contain at least one number and one letter.

For users in organizations that have access to a smart phone

There are currently two methods for this option: Send a one-time use code via a SMS message or receive a call with a one-time use code over the phone.

- A valid phone number must be registered with a user's account, which is setup during the user registration process.
- The user can select which method they wish to be contacted at the time of login.
- The one-time use code must be successfully entered in order to complete authentication.

S-12: CHANGE MANAGEMENT

Added Provision Submitting a Change Request – Operational Environment, as follows:

> Change requests can come from Application Service Provider, BORN Hosting Provider, or the BORN Technical Team. They may be in the form of an optimization, patch, system replacement or upgrade.
>
> All requests for change to the operational environment are submitted and tracked in Hosting Provider's change management system.
> BORN formally opens and tracks tickets in the Hosting 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
>
> Tickets that are submitted but not complete are returned to the requestor for clarification.

Also added a provision noting that the Hosting Provider is responsible for implementation of the change in the operational environment.

S-13: BACK-UP AND RECOVERY OF RECORDS OF PERSONAL HEALTH INFORMATION

Incorporated by reference the BORN Backup plan that is contained in the BORN Disaster Recovery SOP. Revised to reflect that backups will be stored in the Azure Vault for BORN via the Azure Backup Service. Storage is compliant to **S-05: Retention of Records of Personal Health Information**.

S-15: SECURITY AUDITS

Added that audit plans, activities, and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.

Added a provision that assessments are performed at a minimum every three years and on an as needed basis for individual projects.

S-17: SECURITY BREACH MANAGEMENT

Added a provision that the Information Security Officer updates the Privacy and Security Review Committee and the Executive Director and the CHEO VP on a regular basis.

The policy is also amended in the 3.0 Plan to incorporate any legal requirements to provide notification under PHIPA that may apply (e.g., Ontario Regulation 329/04 under the Personal Health Information Protection Act, section 6.3) and any guidance's issued by the Information and Privacy Commissioner such as Guidelines for the Health Sector – Reporting a Privacy Breach to the IPC, dated September 2019).

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:

In the 3.0 Plan, three new policies will be introduced: **S-19: Application Security**, **S-20: Encryption & Key Management**, and **S-21: Roles Based Access Controls for the Azure Environment**.

S-19: APPLICATION SECURITY

This policy will ensure that there are appropriate policies and procedures in place for application security. The policy will detail security assessment criteria, mitigations based on risk levels, common vulnerabilities to protect against, and security administration of web applications.

All development will be required to adhere to an industry standard framework of security requirements and controls that focus on normalizing the functional and non-functional security controls required when designing, developing and testing modern web applications.

Responsibility of this policy will be with the BORN Information Security Officer and Senior Technical Architect.

S-20: ENCRYPTION & KEY MANAGEMENT

This policy will support business processes and technical measures implemented, for the management of BORN's cryptographic keys. Key management procedures will ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.

Responsibility of this policy will be with the BORN Information Security Officer.

S-21: ROLES BASED ACCESS CONTROLS FOR THE AZURE ENVIRONMENT

This policy will detail role-based access control (RBAC) restrictions in order to access the Azure environment based on a person's role within BORN. RBAC refer to the levels of access that employees/agents have to the Azure environment. BORN employees/agents will only be allowed to access the information and systems necessary to effectively perform their job duties. Access will be based on several factors, such as authority, responsibility, and job competency. In addition, access to resources will be limited to specific tasks such as the ability to view, create, or modify user accounts.

Responsibility of this policy will be with the BORN Information Security Officer.

Indicator:
The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.

BORN Response:
The Policy was not updated since the prior review. Version 3.0 of the BORN Privacy and Security Management Plan will be e-mailed to all BORN Agents by the Privacy Officer as soon as it has been approved by the Privacy and Security Review Committee.

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: August 23, 2019

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 23, 2018	Verify audit logs of system activity of BORN System Administrator. No recommendations. All activity in line with expectations of BORN System Administrator role. Verify audit of logs of BORN Agent on the BORN Technical Team. No recommendations. All activity in line with expectations

May 24, 2018	Verify audit logs of system activity by two (2) BORN Agent on technical team. No recommendations. All activity in line with expectations
July 10, 2018	Verify audit logs of system activity of BORN System Administrator. No recommendations. All activity in line with expectations of BORN System Administrator role. Verify audit of logs of BORN Agent on the BORN Technical Team. No recommendations. All activity in line with expectations
October 26, 2018	Verify audit logs of system activity of BORN System Administrator. No recommendations. All activity in line with expectations of BORN System Administrator role. Verify audit of logs of two (2) BORN Agent on the BORN Technical Team. No recommendations. All activity in line with expectations
December 18, 2018	Verify audit logs of system activity by two (2) BORN Agent on technical team. No recommendations. All activity in line with expectations
January 17 & 18, 2019	Extensive audit/review of all security policies was undertaken to ensure sufficient policies and procedure in place for the BIS migration to Microsoft Azure. Policies were updated to reflect the BIS being hosted in the "cloud".
January 25, 2019	Verify audit logs of system activity by BORN Agent on technical team. No recommendations. All activity in line with expectations
March 19, 2019	Verify audit logs of system activity of BORN System Administrator. No recommendations. All activity in line with expectations of BORN System Administrator role. Verify audit of logs of two (2) BORN Agent on the BORN Technical Team. No recommendations. All activity in line with expectations
June 6, 2019	The PHI drive was re-configured to better control access to specific PHI data sets. The access control form was updated to align with the new configuration and permission groups.
June 7, 2019	Verify audit logs of system activity by BORN Senior Technical Architect. No recommendations. All activity in line with expectations of BORN System Administrator role.
June 20, 2019	Verify audit logs of system activity by BORN Agent on technical team. No recommendations. All activity in line with expectations
June 24, 2019	The PHI drive was re-configured to better control access to specific PHI data sets. The access control form was updated to align with the new configuration and permission groups. This is because BORN completed a BORN PHI Drive restructuring project in June 2019. Access controls on the BORN PHI Drive are improved to appropriately restrict access within BORN based on a need to access and use. BORN is currently examining technical reporting solutions that will improve BORN's ability to better audit Agent use of the PHI Drive.

July 17, 2019	Verify audit logs of two (2) BORN Agent on the BORN Technical Team. No recommendations. All activity in line with expectations
August 20, 2019	Verify audit logs of system activity of BORN System Administrator. No recommendations. All activity in line with expectations of BORN System Administrator role. Verify audit of logs of a BORN Agent on the BORN Technical Team. No recommendations. All activity in line with expectations
September 5, 2019	Users requiring access to non-PHI reports in the BIS were not able to access the BIS as no roles existed to allow for that scenario. Roles were created and the form updated to allow for non-PHI reporting access to the BIS.
September 17, 2019	Verify audit logs of one (1) BORN Agent on the Technical Team. No recommendations. All activity in line with expectations
October 8, 2019	Verify audit logs of system activity by BORN Senior Technical Architect. No recommendations. All activity in line with expectations of BORN System Administrator role.

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	Threat Risk Assessment – Prenatal Screening Program	The audit was completed March 2018. The scope of the TRA included a security assessment of the NIPT & Cytogentics data feeds and an evaluation of safeguards, risks and implications of the initiative's technologies and processes, and to identify recommendations for managing information security risks. **Recommendations:**

		1) Update Privacy & Security Policy Manual: BORN has an opportunity to update its Privacy & Security Manual and add a section on Application Security Policy Requirement. 2) Update Dapasoft Service Agreement BORN should update Dapasoft's agreement and add specific requirements for Application Security. 3) Implement stronger Interface Security Controls: Information Security Services. 4) Cytogenetic - Maternal-Child Encounter Upload security a. Ensure Purging policies are defined for the SFTP Services. This will ensure file are deleted after they have been consumed by Load Utility for BIS Consumption b. Enable File Scanning policies on the SFTP services c. IP filtering means setting up the server's IP filter rules so that only users from permitted IP addresses are able to access the server. IP addresses that do not pass the rule set to have their connection terminated immediately d. Auto-banning is the second useful security mechanism. It works by automatically banning IP addresses from connecting (for a period of time) if they have failed to authenticate a certain number of times within a time period. For example, an attacker from a given IP address might fail to guess a password correctly 10 times within a 60 second period e. disable SSH terminal access unless it is absolutely required. SSH terminal access is dangerous – it gives far greater access to the operating system than SFTP does. SFTP also runs over an SSH connection, but it does not give terminal access. If a certain user must have SSH terminal access, disable it for all other use. f. ensure the SSH banner message that is sent to clients contains the appropriate legal warnings about unauthorized access Before file upload, files are compressed & encrypted using AES 256 with a salt
2	Threat Risk Assessment – Migration to Microsoft Azure – March 2018	Recommendations: Update Privacy & Security Policy Manual (Priority Medium): • Draft updates have been made to the BORN Privacy & Security Management Plan based on using the Cloud Security Alliance Cloud Control Matrix as a checklist. Each recommendation in the matrix was reviewed and the appropriate policy was updated based on those recommendations. 1. Access controls for Network and Infrastructure assets a. BORN has updated the Security polices to reflect the changes necessary to reflect an improved security framework that protects Personal Health Information (PHI) against theft, unauthorized use or disclosure, unauthorized copying, modification and disposal in the Azure environment. b. BORN's Privacy & Security Management Plan has been updated to reflect access controls (i.e. Passwords and Multi-

		Factor Authentication-MFA). The use of MFA has been extended to all BIS users. c. BORN has introduced a new Security Policy -"S20: Encryption and Key Management" that clarifies BORN's responsibility to manage our own cryptographic keys and which establishes the policy for key management and controls. 2. Third Party Partners/vendor access a. BORN has prepared an agreement for partners to include appropriate conditions to ensure adherence to BORN's Privacy & Security Management plan. b. Security policies have been updated to reflect conditions under which third party partners and vendors are permitted access to BORN's information as well as their responsibilities in ensuring physical security of data and record retention. 3. Security Monitoring and end-point protection controls a. BORN has modified the policies related to security monitoring and controls to reflect the requirement for controls and audit logs appropriate to its environment. The policies detail responsibilities, process steps necessary to ensure timely monitoring, and action responses to any identified anomalies. 4. Administration controls a. BORN has updated the administrative management policies to reflect access and security of PHI, including MFA, audit logs, and system controls such as patch and change management procedures. 5. Auditing access a. These policies were updated to reflect BORN's approach that any significant change to the system or environment will require revisiting and a Privacy Impact Assessment (PIA) to ensure the appropriate level of security and protection of PHI remains constant. 6. Encryption and Key Management a. Encryption and cryptographic key management is a key component in BORN's environment. The keys are managed by CHEO, and accessible only by BORN's authorized Managed Service Provider (CSP). Third party providers do not have access to the encryption keys. Update the Privacy & Security Manual and add specific requirements for Third Party Services Provider responsible for managing Infrastructure, Host and Network services. • Terms have been added so that Third Party Service provider's must comply with the BORN Privacy & Security Management Plan.

		Update the Privacy & Security Manual and add a section on Application Security Policy Requirement. • New policy "S-19: Application Security" has been added to the Privacy & Security Management Plan. This policy ensures that are appropriate procedures in place for application security and describes risk levels and associate remediation procedures to address identified risk exposures in the application. • Reference to "Open Web Application Security Project (OWASP) - Application Security Verification Standard 3.0" added to new policy "S-19: Application Security" as an example of an industry standard framework that may be use for development. BORN must ensure service provider managing its network and Infrastructure resources assume the following responsibilities: a. On-going Deployment and management of Network and Host assets b. Managing VPN Connectivity and site access c. Managing on-going Azure Directory services permissions and access controls d. Manage Web Application FW controls e. Manage Security Threat Protection controls and provide on-going management of rules to block attack vectors f. Manage permissions of multiple VNET's and Management network g. Patch and Vulnerability Management h. Provide Monthly security and operations dashboard BORN should define these Roles and Responsibilities matrix where a clear expectation should be set for BORN Administrators, Services Providers/Partners and their Third Parties • A roles and responsibilities matrix has been created outlining the different users and groups (internal and external to BORN) and associated tasks. Where applicable, roles and responsibilities that belong to external service providers are included as responsibilities in the service agreements. Update Service Agreement(s) once roles and responsibilities are clearly defined, a services provider agreement should be created for Infrastructure and Manage Security Services where requirements should be clearly articulated. • Appropriate terms and conditions have been added to the agreement describing services and the requirement to adhere to BORN Privacy and Security policies.

		Services provider to maintain a comprehensive set of Security Policies which provides assurance of its practices for Cloud Security policy implementation, system hardening, patch and vulnerability management. • Service Provider must follow an industry standard such as ISO-27018 for their security policies and procedures. • The Service Provider policies are auditable by BORN. Services provider to have a documented Standard Operating Procedures (SOP) for Security Incident Response as it relates to managing BIS Security Operations, Infrastructure and Manage Services. • A standard operating procedure for security incident response is included. Services Provider to produce Monthly security and operations dashboard • The requirement to provide a monthly security and operations dashboard are included in agreements. Further the requirement to provide monthly operations reports are also defined. Services Provider to define and document logging, monitoring and auditing controls framework and supporting procedures • The service provider is required to implement logging and monitoring as well as an auditing controls framework and supporting procedures. Services Provider to define a robust security architecture from which BIS Services will be managed. • The BORN Architecture document defines network segregation and security. The service provider is required to maintain and manage connectivity. Service Provider to have a defined Cybersecurity strategy and its ability to detect and respond to threats with a Governance structure • The strategy, tools and reports are included as a requirement. • The Service Provider must follow an industry standard such as ISO-27018 for their cybersecurity strategy. • The Server Provider policies are auditable by BORN. BORN to have the right to audit the control framework which needs to be defined in the Services Provider Agreement • The right to audit the control framework is defined in the service agreements. If the services provider also manages the application and its deployment processes, then additional clauses need to be added for application security framework and following secure coding best practices.

		• The agreement states that all development must adhere to an industry standard framework of security requirements and controls that focus on normalizing the functional and non-functional security controls required when designing, developing and testing modern web applications. An example of such a framework is "The Open Web Application Security Project (OWASP)" (https://www.owasp.org). • The policies related to patch and change management have also been updated to reinforce procedures for managing changes to the application. A specific section for "Systems Development, Maintenance and Support" should be created in the Services Agreement that include steps to check for common vulnerabilities during the development of any Deliverables or in the provision of the Services. • The procedure to check for vulnerabilities is described in the Services Agreement. Further, policy **S-19: Application Security** has been created to describe application security protection procedures. The service provider is obligated to provide a vulnerability management process and continually assess new vulnerabilities. Vulnerability checks must include, but are not limited to, the following 10 common vulnerabilities: ○ Injection vulnerability prevention ○ Cross-Site Scripting (XSS); ○ Broken Authentication and Session Management; ○ Insecure Direct Object References; ○ Cross-Site Request Forgery (CSRF); ○ Security Misconfiguration; ○ Insecure Cryptographic Storage; ○ Failure to Restrict URL Access; ○ Insufficient Transport Layer Protection; and ○ Un-validated Redirects and Forwards Services provider to have security agreements in place with its services provider to ensure compliance. This would include passing on the obligation for Privacy & Security • Service Provider is required to enter into agreements with subcontractors on terms and conditions that are consistent with the obligations set out in agreements with BORN. Those subcontracts are to be delivered within seven (7) days of the execution of the agreement. Document Standard Operating Procedure (SOP) for BIS Infrastructure & Application Change Management. This Standard Operation Procedure (SOP) for BIS hosting would define clear procedures for any changes to: Virtual Hosts,

		Network Security Group, Change submission and approval process for any Application & Network level changes, On-going system Patch and Vulnerability Management Process, Security Incident Reporting process, and Backup and on-going configuration management processes • CHEO and Service Provider have a comprehensive Change Management process to manage changes to the BIS environment (BIS Application and Infrastructure). Further, the operating model is described in detail as part of the Service Agreement. • Changes to the operational environment are covered in the change management section of the Service Agreement. Any and all changes must be approved by BORN's Manager of Health Networks or their designate. • As per the BORN Architecture document: Network security is implemented through the use of Network Security Groups (NSG). Network security groups operate similar to having a firewall protecting each one of the resources to which they are associated. • Each network security group is composed of one or more network security rules that either allow or deny traffic based on criteria, such as: o Source and destination IP address/network; o Source and destination port; o Protocol (TCP / UDP) • A network security group is configured for each virtual machine created in the environment. • In accordance with the approved change management process all changes to application or network must be submitted using an standard change request form and must follow a formal approval process to determine a final disposition (i.e. approved or denied). • The Patch Management policy described previously provides for on-going control of system patches. Vulnerability management obligations are included in the Service Agreement. • Incident management has always been a component of the service agreements with the Service Provider. The policy has been updated to reflect incident management in the BORN environment. • Backups, ongoing configuration management and operational process responsibility is defined in the Service Agreement. Policies have been updated to reflect the requirement in the BORN environment. Enable Strong Application Authentication Controls (Priority Medium-High): Moving BIS services to cloud will have many users accessing the services over the Internet. Strong authentication controls should be enabled at the application layer such as the use of Multi-factor authentication (MFA). • As part of the BIS Cloud project, Dapasoft has developed and implemented a multi-factor authentication (MFA) layer, users cannot

		access the BIS-Azure platform without completing multi-factor authentication. Alerts should be configured to report on abnormal access attempts. This is rather simple to implement and should be added to the manage services contract. • Logging and reporting of alerts is included. Document Logging, Monitoring & Auditing standard and operationalize Security Information & Event Management Controls (Priority Medium) • The requirement for logging, monitoring and auditing requirement is added. The requirement will be that Dapasoft will provide a "scorecard" of activity in the BORN environment. The frequency of this scorecard will be monthly at a minimum. BORN should document a comprehensive strategy for Logging, Monitoring & Auditing along with Security Information & Event Management controls. This includes the following components: Document Threat use cases which BORN would like to get alerted on; Ensure all security event logs from key critical devices are being centrally logged; Document expectations for services providers for security event reporting including monthly dashboards; and Integrate FW logs with Log Analytics • Specific responsibilities of the Service Provider commensurate with the strategy to securely manage the BORN environment are described. • An attack/defence tree has been developed and added to BORN's Security Analysis documentation. • Responsibilities to report on security events is defined in Dapasoft Agreement. Further, policies related to Security Audits and Security Breach Management have been updated to reflect the BORN environment. • This has been implemented in the BORN environment as per the BIS design document. Enable Secure File Transfer Protocol (SFTP) Services: There is an opportunity to improve security controls on the current implementation of SFTP services. • BORN implemented a new FTP server solution. Enable security controls as per the Detailed Design Document. • Security controls have been implemented and Service Provider responsibilities related to such controls are clearly defined. • The BORN Architecture document details the implementation, security controls, logging and monitoring. • Site recovery is detailed in the BORN Disaster Recovery Plan.

		Remediate Technical Vulnerability Assessment Findings and establish a Vulnerability Management Program. BORN should ensure High and Medium severity findings are remediated prior to go-live and on-going vulnerability scanning should be included as part of security and Infrastructure manage services. • All findings have been remediated. On-going vulnerability scanning is included as a component of the Services agreement.
3	Technical Vulnerability Assessment/Penetration Test – BORN Information System – March 2018	5 issues were noted: 0 Critical, 2 High, 2 Medium, and 1 Low Risk. No Critical findings were identified. Specifics of the issues were detailed in the final penetration test report and were addressed immediately.

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:
- 52 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:

2016-17 ongoing organizational privacy/security training

- There were 69 BORN agents in 2016-17:
    - 51 agents attended organizational privacy/security training
    - 18 agents did not attend organizational privacy/security training in person. Of these 18 agents:
        - 9 agents are CHEO IS employees (also BORN agents for BORN Helpdesk services); CHEO IS employees attend mandatory CHEO privacy training every two years –in addition these agents were sent the privacy and security presentations via email to review and they all confirmed by email that they read and fully understood the contents of the presentations.
        - 9 agents were unable to attend ongoing privacy/security training in person due to other commitments (i.e. conference, vacation etc., however, they were provided with a copy of the privacy and security presentations by email and all confirmed (by email) that they read and fully understood the contents of the presentations.

2017-18 ongoing organizational privacy/security training:

- There were 80 BORN agents in 2017-18:
    - 56 agents attended organizational privacy/security training
    - 24 agents did not attend organizational privacy/security training. Of these 24 agents:
        - 6 agents did not attend annual privacy/security training in person, however the presentation was sent to them via email and all confirmed that they read and understood the contents.
        - 12 agents are CHEO IS employees (also BORN agents for BORN Helpdesk services); CHEO IS employees attend mandatory CHEO privacy training every two years – in addition all agents were provided with a copy of the privacy and security presentation via email and each confirmed by email that they read and fully understood the contents of the presentations
        - 7 agents left BORN before the training session was scheduled

2018-19 on-going organizational privacy/security training:

- There were 90 BORN agents in 2018-19:
    - 55 agents attended organizational privacy/security training
    - 35 agents did not attend organizational privacy/security training in person. Of these 35 agents:
        - 7 agents are CHEO IS employees (also BORN agents for BORN Helpdesk services); CHEO IS employees attend mandatory CHEO privacy training every two years – and in addition all of these agents were sent the privacy and

security presentation via email and each they confirmed by email that they read and fully understood the contents of the presentations

- 16 agents were unable to attend organizational privacy and security training in person but all 16 were provided with the presentations via email and all confirmed that they read and understood the contents
- 1 agent could not attend as they were out of the country however, they received their initial privacy training in that year and also was sent a supplementary security presentation via email and confirmed that they read and understood the contents
- 1 agents did not attend but left BORN shortly afterwards
- 5 agents left BORN before the organization privacy and security training was given
- 5 agents joined BORN after the organizational privacy/security training was conducted, however they all received initial privacy and security training when hired and all signed a confidentiality agreement at that time

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

1	7-Nov-16	Privacy Officer provided an in person update on the 2016 IPC Tri-ennial Review at the BORN monthly meeting
2	7-Dec-16	Privacy Officer provided general privacy update at BORN Free: update on PHIPA Summit including security update,
3	21-Dec-16	Privacy Officer sent reminder to all BORN re BORN PHI drive (how access is requested and approved and logged; what the drive is to be used for)
4	25-Jan-17	Privacy Officer sent reminder to all BORN managers and BORN leadership team to review mandatory step of contacting BORN HR for all new hires; message contained mandatory acknowledgement.

5	28-Feb-17	Privacy Officer emailed BORN staff an article on stuffed toys leak millions of voice recordings from kids and parents. A security vulnerability allowed anyone to view personal information, photos and recordings of children's voices from CloudPets toys. And at one point, some people tried to hold all of that information for ransom. According to a report compiled by security researcher Troy Hunt, over 820,000 user accounts were exposed. That includes 2.2 million voice recordings. Link to the article is below: *http://money.cnn.com/2017/02/27/technology/cloudpets-data-leak-voices-photos/index.html*
6	29-Mar-17	Privacy Officer issued part 1 of 10 of CHEO's cyber security tips in the BORN Buzz addendum.
7	31-May-17	Privacy Officer issued part 2 of 10 of CHEO's cyber security tips in the BORN Buzz.
8	15-Jun-17	Privacy Officer issued part 3 and 4 of 10 of CHEO's cyber security tips in the BORN Buzz.
9	30-Jun-17	Privacy officer sent message to managers reminding them about their responsibilities about HR hires/terminations
10	18-Aug-17	Privacy Officer issued part 5 and 6 of 10 of CHEO's cyber security tips in the BORN Buzz.
11	1-Nov-18	Privacy Officer provided Privacy Quick Reference - How to Handle PHI -- this was attached to the BORN Buzz internal newsletter
12	14-Nov-19	Phish email test sent to all BORN Agents
13	1-Feb-19	Article regarding phishing emails emailed to all BORN Agents - Tips on how to avoid attack
14	14-May-19	• Annual Ongoing Security Training presented at the BORN Team Meeting • Annual Ongoing Privacy Training presented at the BORN team meeting
15	17-Jul-19	Privacy Officer sent an email to all BORN staff to remind them that healthcare phishing is a real danger and the preferred method for hackers to breach healthcare organizations to deploy ransomware – email included a list of tips on how to prevent attacks as prepared by IPC -Technology Fact Sheet July 2019 edition (attachment)
16	26-Jul-19	Privacy Officer posted a reminder in the by-weekly internal newsletter (BORN Buzz) advising staff that BORN privacy and security teams are always available for individual one-on-one training upon request
17	10-Oct-19	The BORN Privacy Officer provided the BORN team with an update on the status of the upcoming Three Year Review IPC submission
18	17-Oct-19	Security Officer posted an update in the by-weekly internal newsletter (BORN Buzz) advising staff about the BORN Information System migration to Azure

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:

- 52 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:

2016-17 ongoing organizational privacy/security training

- There were 69 BORN agents in 2016-17:
    - 51 agents attended organizational privacy/security training
    - 18 agents did not attend organizational privacy/security training in person. Of these 18 agents:
        - 9 agents are CHEO IS employees (also BORN agents for BORN Helpdesk services); CHEO IS employees attend mandatory CHEO privacy training every two years –in addition these agents were sent the privacy and security presentations via email to review and they all confirmed by email that they read and fully understood the contents of the presentations
        - 9 agents were unable to attend ongoing privacy/security training in person due to other commitments (i.e. conference, vacation etc., however, they were provided with a copy of the privacy and security presentations by email and all confirmed (by email) that they read and fully understood the contents of the presentations

2017-18 ongoing organizational privacy/security training:

- There were 80 BORN agents in 2017-18:
    - 56 agents attended organizational privacy/security training

- 24 agents did not attend organizational privacy/security training. Of these 24 agents:
  - 6 agents did not attend annual privacy/security training in person, however the presentation was sent to them via email and all confirmed that they read and understood the contents
  - 12 agents are CHEO IS employees (also BORN agents for BORN Helpdesk services); CHEO IS employees attend mandatory CHEO privacy training every two years – in addition all agents were provided with a copy of the privacy and security presentation via email and each confirmed by email that they read and fully understood the contents of the presentations
  - 6 agents left BORN before the privacy and security training session was conducted

2018-19 on-going organizational privacy/security training:

- There were 90 BORN agents in 2018-19:
  - 55 agents attended organizational privacy/security training
  - 35 agents did not attend organizational privacy/security training in person. Of these 35 agents:
    - 7 agents are CHEO IS employees (also BORN agents for BORN Helpdesk services); CHEO IS employees attend mandatory CHEO privacy training every two years – and in addition all of these agents were sent the privacy and security presentation via email and each they confirmed by email that they read and fully understood the contents of the presentations
    - 16 agents were unable to attend organizational privacy and security training in person but all 16 were provided with the presentations via email and all confirmed that they read and understood the contents
    - 1 agent could not attend as they were out of the country however, they received their initial privacy training in that year and was provided with a supplementary security presentation via email and confirmed that they read and understood the contents
    - 1 agents did not attend but left BORN shortly afterwards
    - 5 agents left BORN before the training session was conducted
    - 5 agents joined BORN after the organizational privacy/security training session was conducted, however they all received initial privacy and security training when hired and signed a confidentiality agreement

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.

- 2016-2017: of the 69 BORN Agents all agents re-acknowledged their confidentiality agreement pledge via email as part of the organizational privacy and security training
- 2017-2018: of the 80 BORN Agents, all agents re-acknowledged their confidentiality agreement pledge via email as part of the organizational privacy and security training
- 2018-2019: of the 90 BORN Agents, 55 agents executed a confidentiality agreement at the BORN team meeting on May 14, 2019; 23 agents who were not able to attend the team meeting in person re-acknowledged their confidentiality pledge via email; 1 agent didn't need to re-acknowledge because they joined BORN in January 2019; 5 BORN agents joined BORN after the Mary 14, 2019 team meeting and signed confidentiality agreements as part of the initial privacy and security training, and 6 left BORN before the annual renewal of confidentiality was required

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:
27 termination notices were received from BORN agents who terminated their employment with BORN Ontario since the prior review.

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:

- April 9, 2018
- April 25, 2018

- June 6, 2018
- July 19, 2018
- August 31, 2018
- November 8, 2018
- January 15, 2019
- January 17, 2019
- February 13, 2019
- March 28, 2019
- May 31, 2019
- July 12, 2019
- July 18, 2019

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 amendments were made to the corporate risk register as a result of the reviews:

- April 9, 2018
  Added a risk to document that with the BIS migration to Azure, there is a need to ensure that CHEO IS have the necessary skills to build and maintain cloud environments.
- April 25, 2018
  Added a risk related to the maintenance agreement with BORN Information System developer to ensure that roles/responsibilities for maintenance services for the Azure environment need to be clearly defined.
- June 6, 2018
  - Added a risk to identify that the expiry of RSA tokens used for second factor authentication to Systems Administrator BIS users and the RSA appliance reached the end of life and is no longer supported.
  - Added a risk to document the security issues related to the BORN "PHI" Drive and to initiate a project to be reconfigure.

- July 19, 2018
  - Added a risk to identify that the master service agreement with the developer of the BORN information System does not contain necessary Privacy conditions to satisfy IPC requirements. August 31, 2018
  - Added a risk to identify that as a result of a recent PIA/TRA on the BIS migration to Azure, it would be necessary to create new policies and update existing policies to comply with recommendations.
  - Added a risk to identify that CHEO IS does not have the appropriate skill set to support and manage the BIS environment on Azure

- August 31, 2018

Added several risks to document policy issues related to BORN migrating to the Azure environment.

- January 15, 2019
  Added a risk to document that the terms of the Microsoft Agreement (related to BIS migration to Azure) does not contain clauses the comply with IPC requirements
- January 17, 2019
  Added a risk to document the rise of ransomware in the healthcare environment specifically the Dharma ransomware variant called "Adobe".
- February 13, 2019
  Added a risk to document a phishing attack of a compromised email account. Note that BORN does not allow access to PHI by email. Notwithstanding, as a precaution, an investigation was performed which included audits of the BORN Information System and BORN PHI Drive to ensure there were no unauthorized accesses.
- March 28, 2019
  Added a risk to document a phishing attack of an email impersonation
- May 31, 2019
  Added a risk to document that BORN should ensure that contract related costing /budgets forecasts are in line with what is anticipated.
- July 12, 2019
  Added a risk to document that the current agreement with the BORN Information System developer does not comply with IPC requirements
- July 18, 2019
  Added a risk to identify and document issues relating to "PHI access"-- Microsoft cannot have access to PHI and BORN obtain confirmation from the developer and Microsoft that 1. that Microsoft does not have access to PHI; 2. that data is encrypted; 3 that Microsoft does not have access to the encryption keys

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:
   - Dec 6, 2016
   - Feb 22, 2017
   - Feb 23, 2018
   - May 28, 2018
   - Apr 30, 2019

On November 20, 2017 the BORN infrastructure suffered a catastrophic hardware failure. At that time BORN and its hosting service provider implemented its business continuity plan. Users and stakeholders were notified of the outage, replacement hardware was obtained, and the BORN Information System was restored from backups. Implementation of the business continuity plan was deemed successful. No updates to the plan were considered necessary or desirable.

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:
No new policies and/or procedures have been identified.