**Exhibit B**
**PRIVACY, SECURITY, AND OTHER INDICATORS**

# Part 1: Privacy Indicators

***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:**
All policies, practices, and procedures were reviewed in 2022 as part of the amendments to version 3.0 of the BORN Privacy and Security Management Plan. In January 2022, a working group of the Privacy and Security Review committee ("PSRC") was formed from internal stakeholders and commenced meeting on a bi-weekly basis from February 11 through to June 17. Thereafter further reviews took place by PSRC on June 22 and June 30, 2022.

BORN's PSRC reviewed and approved version 3.1 of the BORN Privacy and Security Management Plan on July 12, 2022. Further amendments to 3.1 of the BORN Privacy and Security Management Plan were reviewed and approved by BORN's PSRC on November 2, 2022, resulting in version 3.1.1. To facilitate the review and amendment of the BORN Privacy and Security Management Plan during 2022, an internal 3.1 Working Group was formed. Meetings of the 3.1 Working Group and of the PSRC were held on the following dates in 2022:

| ***Date of review meeting*** | ***Group/Committee conducting the review*** | |
|---|---|---|
| February 11, 2022 | 3.1 Working Group | |
| February 15, 2022 | | PSRC |
| February 25, 2022 | 3.1 Working Group | |
| February 26, 2022 | 3.1 Working Group | |
| March 11, 2022 | 3.1 Working Group | |
| March 21, 2022 | | PSRC |
| March 25, 2022 | 3.1 Working Group | |
| April 7, 2022 | 3.1 Working Group | |
| April 8, 2022 | 3.1 Working Group | |
| April 19, 2022 | | PSRC |
| April 22, 2022 | 3.1 Working Group | |
| May 6, 2022 | 3.1 Working Group | |
| May 16, 2022 | | PSRC |
| May 20, 2022 | 3.1 Working Group | |

| | | |
|---|---|---|
| June 3, 2022 | 3.1 Working Group | |
| June 22, 2022 | | PSRC |
| June 30, 2022 | 3.1 Working Group | PSRC |
| July 12, 2022 | | PSRC |
| July 19, 2022 | | PSRC |
| August 16, 2022 | | PSRC |

***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:**
With the exceptions of P-11, P-11A, P-15, and P-23, all existing privacy policies and procedures were amended.

The glossary, which is used throughout, was expanded, and improved to ensure consistency. Rather than one overarching audit and enforcement and notice policy, specific sections were added throughout to ensure greater alignment to the structure of the Manual and to emphasize key policies subject to these requirements.

The introduction was reframed to improve descriptions of BORN's reporting activities and the ways that BORN uses and discloses data to facilitate or improve the provision of health care in Ontario. The introduction describes the relationship between facilitating or improving the provision of health care and the BORN Purposes. It also describes BORN's mandate as a provincial program.

**P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person**
Changes enhance the descriptions of the various committees that BORN uses to make decisions to collect, use, disclose, and retain data. In particular, the PHI Disclosure Committee was renamed to the Reporting and PHI Disclosure Committee ("RPDC") with the added mandate of reviewing and approving system-generated reports made available through the BORN Systems. Improvements were also made to clarify that RPDC approval is required for all research involving record level disclosures (even if de-identified).

The governance structure was updated so that the description of the Data Quality Committee was updated to reflect its new name- Data and Information Quality Committee ("DIQC"). There is also an improved description of the role of clinical advisory committees and other approaches used to help inform decision making.

Changes were also made to improve descriptions of how data are used and disclosed within BORN to generate reports for stakeholders and to facilitate research.

**P-02 and S-02: Triennial Review of Privacy and Security Policies and Procedures**
Minor amendments were made such as additional reviews of policies and procedures might also be as requested by the PSRC. Also identified that PSRC may form working groups from different areas of BORN to examine changes and their impacts. Changes were also made to improve structural alignment to the Manual.

Quarterly reporting was removed in preference to other approaches, such as monthly reviews of incidents, reviews of new developments and guidance, and updates to the risk log and log of recommendations all on a monthly basis at PSRC.

**P-03: Transparency of Privacy Policies and Procedures**
Substantively very similar to the prior version but its structure was modified to map more precisely to the requirements of the Manual.

**P-04 and P-06: Statements of Purpose for Data Holdings Containing Personal Health Information**
In the prior version of the Privacy and Security Management Plan, two procedures applicable to the Data Holdings Committee ("DHC") were combined. These have now been separated for improved clarity and to emphasize that the maintenance of the Statements of Purpose for Data Holdings Containing Personal Health Information is on-going. However, although separated, the considerations and procedures in P-04 are still linked with P-06.

**P-04: Collection of Personal Health Information**
This procedure now provides that the review process should make use of the Request for Collections and Changes to Holding Form to document the review and decision process by the committee. The procedure was expanded to set out the considerations that may or must be considered (as applicable):

- Description of New Collection/Changes to Collections.
- Advice, if any, received from subject matter experts and advisory committees (e.g., clinical committees, health information custodians, and key experts in the field of maternal, infant and child health and other experts as warranted).
- A detailed description of the data collection request and the flow of personal health information.
- A mapping of the request to the BORN Purposes (i.e., examples of ways this will be used to facilitate or improve the provision of health care).
- A consideration as to whether there are significant changes relating to the collection, access, use or disclosure of personal health information resulting from this proposal, including:
    - Significant changes to functionality of the service technology;
    - Significant change in vendor/technology partner;
    - Implementation of a new service delivery or management technology that stores, transmits, or retrieves personal health information;
    - Involvement of new programs, processes and systems involving personal health information;
    - significant changes to purposes, data collection, uses or disclosures; and
    - Any other programs, processes, and systems with privacy implications, as recommended by the Privacy Officer.
- Privacy and Security Risks, including whether this collection or change result in changes to the risk management log or log of recommendations maintained by the PSRC.
- Any impacts of the Indigenous Data Governance policy that apply
- Any impacts of the Data Vigilance policy that apply.
- Whether the collection of personal health information is consistent with PHIPA and its Regulation and that any and all conditions and restrictions set out in PHIPA and its Regulation have been satisfied.
- Whether there is a requirement for a Privacy Impact Assessment ("PIA") or Threat Risk Assessment ("TRA").
- What agreements or amendments to data sharing agreements are necessary to support the collection (or change).
- What changes to the BORN Holdings, BORN Purposes, and Statements of Purpose of Data Holdings Containing Personal Health Information will result (if any).
- Whether other information, namely de-identified and/or aggregate information, will serve the purpose.

- Whether no more personal health information is being requested than is reasonably necessary to meet the purpose.

The procedures for contemporaneously updating the BORN Holdings and Statements of Purpose of Data Holdings Containing Personal Health Information were improved to ensure that these remain current with each decision by the DHC.

**P-05: List of Data Holdings Containing Personal Health Information**
Previously, this policy listed the BORN Holdings. Instead, and to improve the administration of updates on an on-going basis, the list of BORN Holdings is moved to the Forms used to consider additions or changes under P-04.

As changes to this list are approved by the DHC through new collections, changes to collections, or disposals (as applicable), the form will be updated by the Chair of DHC as part of that approval process or disposal.

The policy further describes that the Chair of the DHC can be contacted for further information in relation to the purposes, elements, and sources of each data holding of PHI.

**P-06: Maintaining Statements of Purpose of Data Holdings**
This now sets out that on an ongoing basis, the DHC reviews BORN's Holdings to ensure they are still required for one or more of BORN Purposes or facilitation of Research. This is achieved as follows:

- The Request for Collections and Changes to Holding Form is used for changes to Collections under P-04: Collection of Personal Health Information. It incorporates up-to-date list and brief description of the data holdings of PHI maintained by BORN. It also attaches the Statements of Purpose of Data Holdings. This helps ensure that the Statements of Purpose of Data Holdings are reviewed on an ongoing basis as data-related decisions are made within BORN to ensure their continued accuracy and to ensure that the PHI collected for purposes of the data holding is still necessary for the identified purposes. When new collections or changes to existing collections are approved, the DHC will confirm any changes needed to the Statements of Purpose for Data Holdings that is attached to the Request for Collections (or Changes to Collections) Form.
- The Statements of Purpose of Data Holdings are also reviewed upon request received under P-8 or P-12 from the Privacy Officer sent to the Chair of DHC setting out the circumstances as to why the Statements of Purpose of Data Holdings may require updating (i.e., based on an identified request for use or possible disclosure).

The policy and procedure also set out that to the extent necessary to reflect the changes decided upon, the Statements of Purpose of Data Holdings will be updated by the DHC Chair, with the approval of the DHC. The DHC Chair will then inform the Privacy Officer of all changes to BORN Holdings, Statements of Purpose of Data Holdings, and BORN Purposes. The Privacy Officer will then work with the Communications Lead to update website content, the Privacy policy (if applicable), and will communicate these changes pursuant to P-03: Transparency of Privacy Policies and Procedures.

**P-07: Statements of Purpose for Data Holdings Containing PHI**
This policy was revised to describe the inter-relationship between the BORN Purposes and the Statement of Purpose of Holdings primarily to improve clarity. The BORN Purposes are examples of the ways that BORN facilitates or improves the provision of health care through data and related reporting

activities. These are listed in this policy and also in the Privacy policy. For clarity, the policy describes that the DHC maintains the Statements of Purpose of Data Holdings.

**P-08: Limiting Agent Access to and Use of Personal Health Information**
This procedure has been expanded and examples of typical uses by functional position are described. BORN prohibits Agents from accessing and using personal health information except as necessary for their employment or contractual responsibilities. The policy now sets out examples to help provide guidance to BORN Agents for when access is requested based on functions within BORN.

The procedure includes an additional check for uses for Research purposes to confirm dates of Research Ethics Board ("REB") and Research Review Committee ("RRC") approval.

The procedure also includes the added consideration that the proposed use of a BORN Holding is consistent with the Statements of Purposes of the Data Holdings for which access is requested (where there is inconsistency, the Privacy Officer will send a request to the Chair of the DHC for clarification as to whether the Statements of Purposes of the Data Holdings needs revision based on the request).

The procedures were also expanded to include additional information from each BORN Agent's manager to better assist the Privacy Office in performing the annual review of applications for access to PHI. Additional procedures have been added to accommodate requirements for Holdings that involve additional steps.

**P-9: Log of Agents Granted Approval to Use**
The log was revised to remove references to disclosure since they are not used.

**P-10: Use of Personal Health Information for Research**
The procedure was revised to emphasize that "use" means to "view, handle, or otherwise deal" with personal health information. BORN rarely discloses any personal health information for Research by non-Agents but it regularly facilitates Research outside of BORN through the disclosure of De-Identified or Aggregate Data. This policy was clarified to state that it governs those activities too.

The policy now clarifies:

- that the RRC reviews and approves all Research requests before any commitments are made to permit access using the procedures set out in this policy.
- The RPDC also reviews and approves all Research use in contemplation of a resulting disclosure of PHI or disclosure of record level De-Identified data. The policy clarifies that this should happen before commitment is made (i.e., in a contract).

This policy also now incorporates a checklist for use by the RRC to assist with the review and decision-making process that aligns with the policy.

The policy clarifies that reporting activities that fall within the BORN Purposes do not generally include Research, but a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them can have the result of improving or facilitating the provision of health care. Additional clarifications on what constitutes "Research" is also included.

Additional considerations were added to identify the structure of the research project and what data will be disclosed outside of BORN and in what form. Based on these considerations the RRC is then able

to consider the requirements for disclosing any data outside BORN, in consultation with the Privacy Office, resulting in the need for a supporting agreement under: P-13: Policy and Procedures for Disclosure of PHI for Research and the Execution of Research Agreements (i.e., as a condition to approval).

In addition to meeting the requirements of PHIPA and its Regulation for Research use, the considerations were expanded to incorporate approvals for linkages under P-22: Linkage of Records of Personal Health Information and consideration of additional use restrictions that might possibly apply under supplementary policies (i.e., the Data Vigilance policy and the Indigenous Data Governance policy).

An additional consideration was also added for Researchers who are BORN Agents to ensure that the Agent's manager (or BORN sponsor, where applicable for students) approved the proposal, including responsibility for ensuring that any conditions or restrictions imposed on the use of PHI for research purposes are in fact being satisfied.

**P-12: Disclosure of Personal Health Information for Purposes other than Research**

New policies and procedures for system generated reports have been developed under P-12. Also, policies and procedures for the ad hoc (as compared to system generated) disclosure of PHI were expanded. Detailed considerations for the RPDC have been developed that are set out in the policies and procedures, together with forms that can be used to assist with decision making and documenting decisions. In addition to those considerations, the RPDC must be satisfied that: (i) the disclosure is permitted by PHIPA and its Regulation and that any and all conditions or restrictions set out in PHIPA and its Regulation have been satisfied; (ii) other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure; and (iii) no more PHI is being requested than is reasonably necessary to meet the identified purpose. Additionally, the procedures are designed to consider any recommendations received from the Information and Privacy Commissioner of Ontario in respect of proposed disclosures of PHI where the Requestor is not a health information custodian (for example, where the requestor is a First Nation).

**P-13: Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements**

Jurisdiction of the Requestor (i.e., in respect of a disclosure outside Ontario) was added to the considerations. If outside Ontario but within Canada (or another country, on a case-by-case basis), BORN will only consider requests for the disclosure of personal health information for Research that is in the interests of public health. In respect of the disclosure of personal health information for Research, the procedure was simplified to provide that approved use under P-10 is necessary (subject to conditions, such as completion of the agreement requirements of P-13). The procedure clarified that the RPDC ultimately approves all requests involving Research Agreements (including record level de-identified data). A Research Agreement must be executed in accordance with the Template Research Agreement prior to the disclosure of PHI for research purposes. In respect of the Disclosure of Record Level De-Identified Information for Research, the procedures clarify that a record level disclosure of De-Identified Information for Research is treated procedurally as personal health information, with the following differences:

- The form of the Research Agreement used differs because the data has been De-Identified;
- The approval of the RPDC can proceed before the Research Agreement is prepared; and

- The data set is prepared in compliance with BORN policy P-24: De-Identification and Aggregation.

**P-14: Template Research Agreement**

The policy was revised to provide that there are two forms of research agreement:

- Research Agreements for the disclosure of PHI; and
- Research Agreements for the disclosure of record level de-identified data for Research purposes.

**P-16: Data Sharing Agreements**

Procedural enhancements were made to clarify how information required for Data Sharing Agreements is supplied to the privacy office.

**P-17: Template Data Sharing Agreement**

This procedure was revised to expressly incorporate the requirements of the Manual for Data Sharing Agreements rather than refer to the template by location.

**P-18: Log of Data Sharing Agreements**

The title of the first field was expanded to include disclosures.

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

The procedure was revised to require that written agreements must contain the relevant language from the Template Agreement for TPSPs and that any material variations to BORN's template must meet all the requirements of the Manual or BORN must provide an explanation for any material variation in advance to the Information and Privacy Commissioner of Ontario as soon as is practicable, and prior to the execution of any contract containing material variations to third party TPSP Agreements that are reasonably expected to involve access to personal health information, in order to explain the variation to the template.

The procedure was clarified that it applies where a TPSP is contracted to retain backed-up records of PHI of BORN, or where a TPSP backs-up records of PHI of BORN it has been contracted to retain, regardless of whether the TPSP uses remote-based (cloud) systems or on-premises systems.

The procedure was enhanced to distinguish between processes for access requests for TPSPs based on Agent status, including logging requirements.

**P-20: Template Data Sharing Agreement**

This procedure was revised to expressly incorporate the requirements of the Manual for Data Sharing Agreements rather than refer to the template by location.

**P-21: Log of Agreements with Third Party Service Providers**

The policy was revised.

- To reflect consistent and more precise naming of the internal document storage location throughout version 3.1.1 of the BORN Privacy and Security Management Plan.
- To proactively and purposefully replicate wording in the previous Draft Manual in existence at the time of the review and revision, while being fully aware that Prescribed Persons were advised to rely on requirements within the 2010 Manual.

- To replicate wording in the 2010 Manual that had not been reflected in version 3.0 of the BORN Privacy and Security Management Plan.

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

The policy was revised to clarify that BORN permits linkage of personal health information for BORN Purposes and to facilitate Research in accordance with a Research Plan as approved of by an REB.

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

The procedure was clarified to provide that in establishing the criteria to be used in assessing the risk of re-identification, regard to the type of identifying information available, including information that can be used to identify an individual directly (e.g., name, address, health card number) or indirectly (e.g., date-of-birth, postal code, gender) must be given.

The procedure was also expanded to include a consideration where projects similar to the BORN Data Warehouse and some Research projects cannot make use of the De-Identification Tools and therefore no "numerical risk level" can be achieved through the use of such De-Identification Tools. In such instances, the procedure clarified that RPDC may approve an alternative risk-based approach to be applied on a cases by case basis (for example, through the use of an expert opinion or through the manual application of the De-identification Guidelines for Structured Data published by the Information and Privacy Commissioner of Ontario by a Data Analyst with the guidance of the RPDC) to ensure that it is not reasonably foreseeable that the data can be used to identify an individual.

The policy and procedures were clarified to reflect changes in PHIPA. Subject to subsection (2) of PHIPA s. 11.2 and to any other exceptions that may be prescribed, no person shall use or attempt to use information that has been de-identified to identify an individual, either alone or with other information, unless PHIPA or another Act permits the information to be used to identify the individual. This includes a prohibition against any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge.

**P-25: Privacy Impact Assessments**

Wording has been updated and approved by the BORN PSRC such that it states the following:

"BORN undertakes privacy impact assessments:

- on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated; and on any other information system, technology, or program with privacy implications, as recommended by the Privacy Officer."

The policy was also amended to provide that the Privacy Officer, in conjunction with the Executive Director, may develop a timetable for the conduct of clinical, stakeholder, and community consultations by BORN related to existing holdings to recommend additional controls in consideration of the concerns of vulnerable groups and/or other stakeholders involved in the consultation.

The content of the privacy impact assessment was revised based on the additional considerations in the draft Manual.

**P-29: Privacy Breach Management**

The definition of a privacy breach was revised to include contraventions of written acknowledgements and collection, use or disclosure without authority. The notification of privacy breaches was expanded to include electronic service providers of BORN and encompass privacy audits, privacy complaints and inquiries. Notification to the Information and Privacy Commissioner of Ontario was defined to include the circumstances set out in subsections 6.3(1) and 18.3(1) of Regulation 329/04 to the Act, as if BORN were a health information custodian.

**P-30: Log of Privacy Breaches**

This log was amended:

- To reflect consistent and more precise naming of the internal document storage location throughout version 3.1.1 of the BORN Privacy and Security Management Plan.
- To proactively and purposefully replicate wording in the Draft Manual, while being fully aware that Prescribed Persons were advised to rely on requirements within the 2010 Manual.
- To replicate wording in the 2010 Manual that had not been reflected in version 3.0 of the BORN Privacy and Security Management Plan.

***Indicator:***

*Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.*

**BORN Response**:

An "overarching" privacy policy was developed and included in the glossary of BORN's policies and procedures. It is based on the Introduction and P-01: Privacy policy in Respect of CHEO's Status as a Prescribed Person, adapted as a stand-alone document to enhance transparency.

***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:**

July 22, 2022, by email to all agents, together with a description of key changes. Both the updated Privacy and Security Management Plan and the overarching Privacy policy were included in the communication to all agents.

***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:**

The web pages on Privacy Frequently Asked Questions (FAQs) and Statement of Information Practices were both adapted to incorporate the overarching privacy policy. Concurrently, the former version of the privacy and security management was removed from the website to achieve alignment with BORN's transparency policy.

***Indicator:***

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

**BORN Response:**
13 data holdings containing personal health information are maintained.

***Indicator:***
*The number of statements of purpose developed for data holdings containing personal health information.*

**BORN Response:**
8 (i.e., 8 BORN Purposes in total, 6 of which were updated and 2 were added)

There are 8 BORN purposes:

A. Identifying where certain Health Care Services have not been offered or made sufficiently available to Health Care Recipients to facilitate access to such services.

B. Facilitating continuous improvement of Health Care delivery tools to minimize adverse outcomes for Health Care Recipients.

C. Identifying where outcomes for Health Care Recipients are statistically discrepant with accepted norms.

D. Enabling Health Care providers to improve care to Health Care Recipients by providing them with Reports to compare themselves with peers and/or benchmarks.

E. Knowledge translation to improve the quality and efficiency of care for Health Care Recipients.

F. Providing Health Care providers with comprehensive and timely Reports to support quality improvement, effective planning, administration, and management of Health Care delivery for Health Care Recipients.

G. Enabling the provision of technologies within BORN Services to improve efficiencies, data accuracy, and data protection for Providers and Health Care Recipients.

H. Creating and providing Reports:

- for surveillance or to support local planning, coordination among providers, and implementation of provincial standards and guidelines.
- to make Health Care service delivery easier and more efficient for Submitters, Health Care providers, and Health Care Recipients who receive such services.
- for public use designed to help prevent disease or injury or to promote health;
- to educate professionals involved in the delivery of Health Care; and
- to educate potential Researchers interested in improving Health Care.

***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**:
13 statements of purpose for data holdings containing personal health information are listed. Each statement of purpose for data holdings contains 5 components, including the need for PHI in relation to the 8 BORN Purposes.

| HOLDING | PURPOSE OF HOLDING | PHI CONTAINED IN THE DATA HOLDING | SOURCE OF PHI | NEED FOR PHI IN RELATION TO BORN PURPOSES |
|---|---|---|---|---|
| **BORN Information System (BIS)** Encounters: CARTR Plus, PSO, Cytogenetics, Antenatal General, Labour/Birth, Postpartum, NICU/SCN, Birth Centre, MPG, Newborn Screening, Ontario Antenatal Record, Well Baby Visit Information, Autism (ABA), eHBHC, Genetics/MFM prenatal whole exome sequencing, NSO CCHD screening results | A single BORN data holding comprised of personal health information collected from health information custodians for specific maternal, newborn and child encounters with the Health Care system for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | Health information custodians in Ontario, including: prenatal and newborn screening providers; hospitals; midwives and midwifery practice groups; outpatient clinics; fertility clinics; Family Health Teams and other primary care providers; birth centres, autism treatment centres; public health units; and laboratories. | A-H |

| | | | | |
|---|---|---|---|---|
| FAN (Fetal Alert Network) historical database | A BORN data holding of the historical dataset from one of BORN's founding members for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | Hospitals in Ontario | A-F |
| Ontario prenatal screening historical database | A BORN data holding of the historical dataset from one of BORN's founding members, for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | North York General Hospital | A-F |
| Niday Perinatal and NICU/ICU historical database | A BORN data holding of the historical dataset from one of BORN's founding members, for the purposes of improving or facilitating the provision of health care and for research. | Risk Factors, Heath Status, Treatment, Outcomes | Hospitals in Ontario | A-F |

| | | | | |
|---|---|---|---|---|
| Ontario Midwifery legacy data historical database | A BORN data holding of the historical dataset from one of BORN's founding members, for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | Data contributed by Midwifery Practice Groups (MPGs) to the Ontario MOH Midwifery Program who signed it over to BORN | A-F |
| CARTR (Canadian Assisted Reproductive Technology) historical database | A BORN data holding of a historical dataset, for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | Canadian Fertility and Andrology Society on Behalf of the Medical Directors of IVF clinics in Canada | A-F |
| NIPT (non-invasive prenatal testing) historical data | A BORN data holding of a historical dataset, for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Outcomes | Laboratories in Ontario | B, C, E, F |
| Cytogenetic Testing Results historical data | A BORN data holding of a historical dataset antenatal and newborn cytogenetic analyses, for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Outcomes | Hospitals in Ontario | B, C, E, F |
| Ontario Midwifery Invoicing System (MIS) | A BORN data holding of midwifery course of care data and a subset of data from the BORN Information System for the purposes of billing for midwifery courses of care. | Identifiers | Midwifery Practice Groups in Ontario | F |

| | | | | |
|---|---|---|---|---|
| COVID-19 Infection Data and Vaccination Data (COVAX) | A BORN data holding of data on the clinical characteristics and laboratory testing of COVID-19 infection and vaccination in pregnant individuals for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | Ontario Ministry of Health, hospitals in Ontario, Midwifery Practice Groups in Ontario | A-H |
| Infant Death Registration Files | A BORN data holding of an extract of infant death registration files for the purpose of Research under P-10 | Identifiers, Outcomes | Ontario Ministry of government and Consumer Services (MGCS) under the VSA to use for undertaking statistical, epidemiological, or other research that is in the public interest | N/A<br><br>Limited to purposes of performing the research protocol subject to our policies, procedures, and any REB requirements. Information derived from that must be de-identified before being shared with service recipients. |
| CIHI (DAD and NACRS) Records | A BORN data holding of DAD and NACRS records of personal health information received from CIHI for Ontario residents for purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | CIHI pursuant to paragraph 39(1)(c) of PHIPA and subsection 18(4) of the PHIPA Regulation, data submitted to CIHI by Ontario hospitals | A-F |
| Niday Maternal, Child Health Card Numbers and Prenatal Billing Codes | A BORN data holding of data received from IC/ES for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | IC/ES pursuant to paragraph 39(1)(c) of PHIPA and subsection 18(4) of the PHIPA Regulation | A-F |

***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:**

Amendments existing statements of purpose for data holdings were made to reflect new holdings related to COVID-19 and infant mortality data for research use.

| | | | | |
|---|---|---|---|---|
| COVID-19 Infection Data and Vaccination Data (COVAX) | A BORN data holding of data on the clinical characteristics and laboratory testing of COVID-19 infection and vaccination in pregnant individuals for the purposes of improving or facilitating the provision of health care and for research. | Identifiers, Risk Factors, Heath Status, Treatment, Outcomes | Ontario Ministry of Health, hospitals in Ontario, Midwifery Practice Groups in Ontario | A-H |

| | | | | |
|---|---|---|---|---|
| Infant Death Registration Files | A BORN data holding of an extract of infant death registration files for the purpose of Research under P-10 | Identifiers, Outcomes | Ontario Ministry of government and Consumer Services (MGCS) under the VSA to use for undertaking statistical, epidemiological, or other research that is in the public interest | N/A<br><br>Limited to purposes of performing the research protocol subject to our policies, procedures, and any REB requirements. Information derived from that must be de-identified before being shared with service recipients. |

## Use

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

**BORN Response:**
92 agents were approved to access and use personal health information 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:**
57 (November 1, 2019, through to July 7, 2022).

***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:**
55 requests were granted; 0 denied (November 1, 2019, through to August 2, 2022).

In two (2) instances, as of September 9, 2022, approval for the use of PHI was pending (i.e., neither granted nor denied as of that date) submission of a final research plan.

## 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:**
1 request received for the disclosure of personal health information for such purposes.

There were also 257,408 System Generated Reports with PHI generated for Submitters within the BORN Systems (BORN has 263 data sharing agreements with health information custodians). There were also 155,374 HBHC screens provided to Public Health Units pursuant to 32 data sharing agreements. (November 1, 2019, through to August 2, 2022)

***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:**
1 was granted; 0 were denied.
(November 1, 2019, through to July 7, 2022)

***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:**
2 requests were received for the disclosure of personal health information for research purposes.
(November 1, 2019, through to July 7, 2022)

***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:**
1 was granted; 0 were denied.
(November 1, 2019, through to July 7, 2022)

***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:**
1 Research Agreement was executed with researchers to whom personal health information was disclosed.
(November 1, 2019, through to July 7, 2022)

***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:**
451 requests received as follows:

- 5 requests for the disclosure of de-identified information for research purposes;
- 6 requests for the disclosure of de-identified information for non-research purposes;
- 108 requests for the disclosure of aggregate information for research purposes; and
- 332 requests for the disclosure of aggregate information for non-research purposes.

(November 1, 2019, through to August 2, 2022)

***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 agreements executed for research purposes;
- 1 agreement executed for the disclosure of information other than research (6 de-identified and 2 aggregate disclosures occurred under this agreement);
- 375 acknowledgements received for the disclosure of aggregate information for research and other purposes;
- 16 disclosures with acknowledgements not received but still pending for the disclosure of aggregate information for research and other purposes requested prior to November 1, 2020 (i.e., the date by which written acknowledgements were required as part of the request); and
- 1 disclosure with missing documentation of acknowledgement (i.e., for data requested after November 1, 2020).

(November 1, 2019, through August 2, 2022).

## 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:**
Seven (7) data sharing agreements executed for the collection of personal health information since the prior review by the Information and Privacy Commissioner of Ontario.

***Indicator:***
*The number of Data Sharing Agreements have been 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:**
There were no 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:**
There were six (6) new or restated third-party service provider agreements 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:**
20 approved:
(This covers the period November 1, 2019, through July 7, 2022)

1. BORN Information System (BIS); CIHI DAD - Gestational diabetes and delivery time: a population-based study in Ontario, Canada.
2. BORN Information System (BIS); Integrated Public Health Information System (IPHIS) - Canadian COVID-19 in Pregnancy Surveillance: Epidemiology, Maternal and Infant Outcomes.
3. BORN Information System (BIS) CCM and COVAXon Registry - COVID-19 vaccination in pregnancy: A province-wide epidemiological assessment of safety and effectiveness using the BORN Ontario Registry.
4. BORN Information System (BIS); CIHI DAD; COVID CRF; Integrated Public Health Information System (IPHIS) - Universal SARS-CoV-2 screening among obstetric patients (UNIVERSE-OB) in Ottawa, Ontario.
5. BORN Information System (BIS); Integrated Public Health Information System (IPHIS) - Assessing the mother-to-infant transmission capabilities of COVID-19 infection among pregnant women in Ontario, Canada.
6. BORN Information System (BIS); CARTR Plus; CIHI - Understanding adverse maternal outcomes in women pregnant by in vitro fertilization: a population-based cohort study of the Better Outcomes Registry & Network (BORN) Ontario.
7. BORN Information System (BIS); CARTR Plus; CIHI DAD; CIHI NACRS - Assisted Reproductive Technology: Association with Pregnancy and Birth Outcomes and Health Services Utilization in the First 12 Months: A Population-Based Cohort Study in Ontario, Canada.
8. BORN Information System (BIS); CIHI DAD - Inter-pregnancy weight change and risk of gestational diabetes mellitus.
9. BORN Information System (BIS); CIHI DAD - Comparing adverse perinatal outcomes between Blacks and Caucasians: a population-based retrospective cohort study in Ontario.

10. BORN Information System (BIS); CIHI DAD; CIHI NACRS; Integrated Public Health Information System (IPHIS) - COVID-19 in pregnancy: An investigation of the characteristics and management of affected women and risk to maternal, fetal, and infant health.
11. BORN Information System (BIS); CIHI - A population-level investigation into the epidemiological patterns of chronic conditions and adverse maternal outcomes across Ontario.
12. BORN Information System (BIS); CIHI DAD - Severity and Rate of Hyperbilirubinemia in Ontario
13. BORN Information System (BIS); CIHI - Antenatal corticosteroids for preventing neonatal morbidity and mortality in preterm twins.
14. BORN Information System (BIS); CIHI DAD; CIHI NACRS - Associations between Socioeconomic status and Health Care Utilization and Hospital Mortality among Infants with Congenital Heart Diseases: A Population-Based Study in Ontario, Canada.
15. BORN Information System (BIS); CIHI-DAD - Social determinants of maternal mental health in pregnancy and associations between maternal anxiety and depression during pregnancy and adverse perinatal outcomes: a population-based study in Ontario, Canada
16. BORN Information System (BIS); CIHI DAD - Cytogenetic and pregnancy outcomes following an increased nuchal translucency measurement.
17. BORN Information System (BIS); CIHI DAD - Investigating the association between cfDNA screening failure and adverse perinatal outcomes.
18. BORN Information System (BIS); CIHI DAD - Outcomes of pregnancies with a double-positive multiple marker screening result.
19. BORN Information System (BIS); Vital Statistics infant death registration - Testing a New Linkage of Births and Deaths in Ontario to Report the Infant Mortality Rate
20. BORN Information System (BIS); Midwifery Invoicing System (MIS) – Linkage of data from the Unaccommodated Client Tracking Tool in the Midwifery Invoicing System to data from the BIS to produce a rate of unaccommodated midwifery clients.

## Privacy Impact Assessment

***Indicator:***
*The number and a list of privacy impact assessments completed since the prior review by the Information and Privacy Commissioner of Ontario and for each privacy impact assessment:*

- *The data holding, information system, technology, or program,*
- *The date of completion of the privacy impact assessment,*
- *A brief description of each recommendation,*
- *The date each recommendation was addressed or is proposed to be addressed, and*
- *The manner in which each recommendation was addressed or is proposed to be addressed.*

**BORN Response:**
One (1) privacy impact assessment was completed as follows:

BORN engaged the services of MD+A to conduct a Privacy Impact Assessment (PIA) in the spring of 2021 related to the Data Warehouse solution and its integration with the BORN network. The PIA was completed in October 2021 and the following recommendations were identified:

***Recommendation 1:*** BORN should update their privacy governance structure and Committee Terms of References to reflect the activities that will be supported by the introduction of the data warehouse and BI application in future, with consideration of the intent to use these systems to better support access to BORN data, and potentially expand access to data products derived from patient data for purposes that align with BORN's mandate. This includes:

- Updating the Terms of Reference for the PHI Disclosure Committee and Reporting Analysts Team to accommodate the BDW and related decision-making.
- Developing decision-making and operational supports for the Committees, Reporting Analysts and Data Analysis and Research Team to clarify the types of decisions made at each group and escalation pathways for decisions.

***Recommendation 2:*** BORN should update the policies and procedures in the privacy manual to reflect the new policies and procedures required for the data warehouse and BI application, in particular revising policies and procedures related to de-identification and aggregation of data to reflect the constraints of de-identification processes associated with the BDW environment.

Both above noted recommendations were addressed by way of amendments to the Privacy and Security Management Plan, approved on July 22, 2022. For Recommendation 1, the BORN Privacy Officer and Counsel at the time worked with the BORN team working on the review and revision of the BORN Privacy and Security Management Plan to update the BORN privacy governance structure and committee terms of reference. For Recommendation 2, the BORN Privacy Officer and Counsel at the time collaborated with the BORN team working on the review and revision of the BORN Privacy and Security Management Plan to update the policies and procedures such that they would incorporate data warehouse and business intelligence applications and related reports.

***Indicator:***

*The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion.*

**BORN Response:**

One (1) privacy impact assessment was undertaken but not yet completed for the FHIR Application for BORN Clinical Data Integrations. A draft PIA has been received and reviewed, yet not formally signed off by CHEO leadership, since subsequent to the receipt of the draft PIA, CHEO made the operational decision to not proceed with the integration of the FHIR application into the data collection mechanisms of the BORN Information System.

***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:**
None

***Indicator:***
*The number and a list of privacy impact assessments reviewed since the prior review by the Information and Privacy Commissioner and a brief description of any amendments made.*

**BORN Response:**
One (1) privacy impact assessment (BORN Data Warehouse) reviewed the fall of 2021 described in detail above.

## Privacy Audit Program

***Indicator:***
*The dates of audits of agents granted approval to access and use personal health information since the prior review by the Information and Privacy Commissioner of Ontario and for each audit conducted:*

- *A brief description of each recommendation made,*
- *The date each recommendation was addressed or is proposed to be addressed, and*
- *The manner in which each recommendation was addressed or is proposed to be addressed.*

**BORN Response:**

| Dates of audits of agents granted approval to access and use PHI since prior review by the 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 |
|---|---|
| November 19, 2019 | Verify BIS audit logs of system activity by 11 BORN employees with access to PHI Oct 19, 2019, to November 19, 2019.<br>No recommendations. All activity in line with expectations |
| December 4, 2019 | Verify BIS audit logs of system activity by 13 BORN employees with access to PHI Nov. 4, 2019, to Dec. 4, 2019.<br>No recommendations. All activity in line with expectations |
| December 19, 2019 | Verify BIS audit logs of system activity by 13 BORN employees with access to PHI Nov. 19, 2019, to Dec. 19, 2019.<br>No recommendations. All activity in line with expectations |
| January 21, 2020 | Verify BIS audit logs of system activity by 12 BORN employees with access to PHI from Dec. 21, 2019, to Jan. 21, 2020. No recommendations. All activity in line with expectations of BORN employees (agent) with access to PHI. |
| January 21, 2020 | Ad hoc audit of DART Team BIS access – audit revealed that 2 Agents had coordinator access that may not be required. Findings reviewed with the manager who advised that coordinator access for one staff was no longer required, and access was removed accordingly |

| | |
|---|---|
| | No recommendations |
| February 13, 2020 | Verify BIS audit logs of system activity by 11 BORN employees with access to PHI from Jan. 13, 2020, to Feb. 13, 2020<br>No recommendations. All activity in line with expectations |
| March 17, 2020 | Verify BIS audit logs of system activity by 9 BORN employees with access to PHI from Feb. 17, 2020, to Mar. 17, 2020<br>No recommendations. All activity in line with expectations |
| April 21, 2020 | Verify BIS audit logs of system activity by 12 BORN employees with access to PHI from Mar. 21, 2020, to Apr. 21, 2020<br>No recommendations. All activity in line with expectations |
| May 21, 2020 | Verify BIS audit logs of system activity by 16 BORN employees with access to PHI from Apr. 21, 2020, to May 21, 2020<br>No recommendations. All activity in line with expectations |
| June 16, 2020 | Verify BIS audit logs of system activity by 16 BORN employees with access to PHI from May 16, 2020, to June 16, 2020<br>No recommendations. All activity in line with expectations |
| July 21, 2020 | Verify BIS audit logs of system activity by 28 BORN employees with access to PHI from June 21, 2020, to July 21, 2020<br>No recommendations. All activity in line with expectations |
| Aug 19, 2020 | Verify BIS audit logs of system activity by 11 BORN employees with access to PHI from July 19, 2020, to Aug. 19, 2020<br>No recommendations. All activity in line with expectations |
| August 25, 2020 | Verify BIS audit logs of Information Security Officer from Jan 1, 2020, to Aug. 25, 2020.<br>No recommendations. All activity in line with expectations |
| September 15, 2020 | Verify BIS audit logs of system activity by 16 BORN employees with access to PHI from Aug. 15, 2020, to Sept. 15, 2020<br>No recommendations. All activity in line with expectations |
| October 16, 2020 | Verify BIS audit logs of system activity by 14 BORN employees with access to PHI from Sept. 15, 2020, to Oct. 16, 2020<br>No recommendations. All activity in line with expectations |
| November 2, 2020 | Verify BIS audit logs of Information Security Officer from Aug. 25, 2020, to Oct. 31, 2020<br>No recommendations. All activity in line with expectations |
| November 17, 2020 | Verify BIS audit logs of system activity by 16 BORN employees with access to PHI from Oct. 17, 2020, to Nov. 17, 2020<br>No recommendations. All activity in line with expectations |
| December 18, 2020 | Annual access review audit for all agents with X Drive Access. Report sent to managers with data holding access for each of their staff. Two managers made minor changes to their staff access.<br>No recommendations. |
| December 21, 2020 | Verify BIS audit logs of system activity by 16 BORN employees with access to PHI from Nov. 21, 2020, to Dec. 21, 2020<br>No recommendations. All activity in line with expectations |

| | |
|---|---|
| January 21, 2021 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from Dec. 21, 2020, to Jan. 21, 2021<br>No recommendations. All activity in line with expectations |
| February 28, 2021 | Verify BIS audit logs of system activity by 14 BORN employees with access to PHI from Jan. 26, 2020, to Feb. 28, 2021<br>No recommendations. All activity in line with expectations |
| March 24, 2021 | Verify BIS audit logs of system activity by 18 BORN employees with access to PHI from Feb. 24, 2021, to Mar. 24, 2021<br>No recommendations. All activity in line with expectations |
| April 20, 2021 | Verify BIS audit logs of system activity by 18 BORN employees with access to PHI from Mar. 20, 2021, to Apr. 20, 2021<br>No recommendations. All activity in line with expectations |
| May 28, 2021 | Verify BIS audit logs of system activity by 16 BORN employees with access to PHI from Apr. 28, 2021, to May. 28, 2021<br>No recommendations. All activity in line with expectations |
| June 30, 2021 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from June 1, 2021, to June 30, 2021<br>No recommendations. All activity in line with expectations |
| July 22, 2021 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from June 23, 2021, to July 22, 2021<br>No recommendations. All activity in line with expectations |
| Aug 23, 2021 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from July 23, 2021, to Aug. 22, 2021<br>No recommendations. All activity in line with expectations |
| September 30, 2021 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from Sep. 1, 2021, to Sep. 30, 2021<br>No recommendations. All activity in line with expectations |
| October 30, 2021 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from Oct. 1, 2021, to Oct. 31, 2021<br>No recommendations. All activity in line with expectations |
| November 5, 2021 | Verify BIS audit logs of Information Security Officer from June 1, 2021, to Oct 31, 2021<br>No recommendations. All activity in line with expectations |
| November 30, 2021 | Verify BIS audit logs of system activity by 13 BORN employees with access to PHI from Nov. 1, 2021, to Nov. 30, 2021<br>No recommendations. All activity in line with expectations |
| December 31, 2021 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from Dec. 1, 2021, to Dec. 31, 2021<br>No recommendations. All activity in line with expectations |
| January 31, 2022 | Verify BIS audit logs of system activity by 14 BORN employees with access to PHI from Jan. 1, 2022, to Jan. 31, 2022<br>No recommendations. All activity in line with expectations |
| Feb 28, 2022 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from Feb. 1, 2022, to Feb. 28, 2022<br>No recommendations. All activity in line with expectations |

| | |
|---|---|
| March 31, 2022 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from Mar. 1, 2022, to Mar. 31, 2022<br>No recommendations. All activity in line with expectations |
| April 30, 2022 | Verify BIS audit logs of system activity by 16 BORN employees with access to PHI from Apr. 1, 2022, to Apr. 30, 2022<br>No recommendations. All activity in line with expectations |
| May 31, 2022 | Verify BIS audit logs of system activity by 14 BORN employees with access to PHI from May. 1, 2022 to May. 31, 2022<br>No recommendations. All activity in line with expectations |
| June 30, 2022 | Verify BIS audit logs of system activity by 15 BORN employees with access to PHI from Jun. 1, 2022, to Jun. 30, 2022<br>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 | June 2020<br>Audit of Log of Confidentiality Agreements (HR-07) for 2020 fiscal year | Review of staff Confidentiality Agreements for all BORN Staff to ensure that all current Agents renewed their confidentiality pledge with BORN and that all Agent agreement were up-to-date and in good standing for 2019-20 fiscal year<br><br>No recommendations. All documentation in line with expectations |
| 2 | August 2020<br>Review of log P-18 Log of Data Sharing Agreements to ensure that agreements and amendments listed align with retained documentation. | Review of each log entry to ensure that agreements and amendments listed aligned with retained documentation.<br><br>No recommendations. All documentation was in order and aligns with P-18 Log entries |

| | | |
|---|---|---|
| 3 | October 2020<br>Audit of disclosure agreements with Public Health Units | Audit of Disclosure agreement with 27 Public Health Units to ensure all authorized users have in place a signed Confidentiality Agreement, as per DSA and compliance with DSA terms<br><br>No recommendations. All confirmed that all authorized users have signed Confidentiality Agreements and that they were in compliance with all DSA terms |
| 4 | November 2020<br>Audit review of HR-02 Log of Ongoing privacy training | Review of BORN Agent completion of annual ongoing privacy training to ensure that all BORN Agents completed. Some Agents were not in attendance at the ongoing privacy training session but were sent the presentation by email – all confirmed that they read and understood the contents.<br><br>No recommendations as all BORN Agents completed the required training |
| 5 | December 2020<br>Audit of X Drive Access for BORN Agents | Annual review of agent access to the X Drive to ensure that the documentation for access to the X Drive for each BORN Agent is completed and up to date. Managers requested minor edits to access which were implemented.<br><br>No recommendations. All documentation in line with expectations. |
| 6 | July 2021<br>Audit of Log of Confidentiality Agreements (HR-07) for 2020 fiscal year | Review of staff Confidentiality Agreements for all BORN Staff to ensure that all current Agents renewed their confidentiality pledge with BORN and that all Agent agreement were up-to-date and in good standing for 2020-21 fiscal year.<br><br>No recommendations. All documentation in line with expectations |
| 7 | August 2021<br>Review of log P-18 Log of Data Sharing Agreements to ensure that agreements and amendments listed align with retained documentation. | Review of each log entry to ensure that agreements and amendments listed align with retained documentation.<br><br>No recommendations. All documentation was in order and aligned with P-18 Log entries |
| 8 | October 2021<br>Audit of Log of 3rd party service providers to ensure that all current 3rd party service providers were captured | Review of log of 3rd party service providers to ensure that all 3rd party service agreements were appropriately documented.<br><br>No recommendations. All documentation in line with expectations |
| 9 | October 2021<br>Audit of disclosure agreements with Public Health Units | Audit of Disclosure agreement with 27 Public Health Units to ensure all authorized users have in place a signed Confidentiality Agreement, as per DSA and compliance with DSA terms. |

| | | |
|---|---|---|
| | | No recommendations. Confirmed that all authorized users signed Confidentiality Agreements and in comply with all DSA terms. |
| 10 | October 2021<br>Audit of BORN Information System (BIS) Access for BORN Agents | Annual review/audit of agent access to the BIS to ensure that the documentation for access for each BORN Agent was completed and up to date.<br><br>No recommendations. All documentation in line with expectations. |
| 11 | November 2021<br>Audit review of HR logs 02 and 04 ongoing privacy and security training | Review of BORN Agent completion of annual ongoing privacy and security training to ensure that all BORN Agents completed the annual required training. Some Agents were not in attendance but were sent the presentation by email – all confirmed that they read and understood the contents.<br><br>No recommendations as all BORN Agents completed the required training |
| 12 | December 2021<br>Audit of X Drive Access for BORN Agents | Annual review of agent access to the X Drive to ensure that the documentation for access to the X Drive for each BORN Agent was completed accurately and is up to date. Manager minor requested edits were implemented immediately, and the log was updated accordingly.<br><br>No recommendations. All documentation in line with expectations. |
| 13 | March 2022<br>Privacy Audit (Audit ID A-01) as per 2021 Audit Plan | Review of privacy policies and security policies pursuant to the 2021-22 Audit Plan audit id A-01). Completion of all questions contained in SA-01 Excel spreadsheet audit framework. The audit revealed some areas for improvement as follows:<br>1. Update quarterly reporting template to include newly implemented Risk Log and Log of Recommendations<br>• The former quarterly reporting template was discontinued in favour of including the review of the Risk Log and Log of Recommendations as a standing agenda item in the monthly PSRC meeting. Other PSRC standing items include a monthly review of incidents and any privacy breaches, plus discussion about new privacy developments and Information and Privacy Commissioner of Ontario guidance.<br>2. Update BORN website data holding page to include all BORN data holdings<br>• This web page update was implemented on August 24, 2022, and is updated following each monthly DHC meeting, as required.<br>3. Amend RRC Terms of Reference |

| | | |
|---|---|---|
| | | • The RRC Terms of Reference were updated on September 14, 2022.<br>4. Support DART team in defining parameters needed to generate Privacy logs P-11, P-11A, P-15 and P-22 from the Visor tool.<br>• Work on this recommendation is in progress as a component of the 2023-2024 BORN operational plan and is targeted for completion by end of March 2024.<br>5. Update the Visor tool to include dates that the PHI Disclosure Committee approved disclosures<br>• Work on this recommendation is in progress as a component of the 2023-2024 BORN operational plan and is targeted for completion by end of March 2024.<br>6. Develop a contingency plan to address a major breach should it arise<br>• BORN policy S-17 does not directly use the phrase *major breach contingency plan,* in part because this term is not defined in the Manual. CHEO reviewed the BORN *Business Continuity and Disaster Recovery Plan* along with policy S -17 on June 24, 2022, July 27, 2022, and October 28, 2022. Amendments directly related to recommendation 6 were: the development of the severity and priority ratings; the notification of key stakeholders and designated incident responders; and a forensic analysis following containment. |
| 14 | April 2022<br>Audited a staff member recent birth to ensure no unauthorized access. | Reviewed audit logs of a staff member who recently gave birth to ensure that no unauthorized access to their records occurred.<br>No recommendations as no unauthorized access found. |
| 15 | May 2022<br>Ad hoc audit of X Drive access to the Data Quality folder on the X Drive | Review of access to the Data Quality folder revealed that an agent was inadvertently given access to the Data Quality folder by CHEO IS without the request being made by the privacy office or the Information Security Officer. The findings revealed that it had been done in error. A recommendation to transition the X Drive request process from email to the CHEO IS Vector ticket system was implemented on May 10, 2022, and is now in place. This enhancement will ensure more accurate tracking of all requests for access to the X Drive. |
| 16 | January to June 2022<br>privacy review | The Privacy Officer conducted a concurrent review of privacy activities to supplement the findings of the annual audit plan and in particular Part 1 of the Privacy and Security Management Plan.<br><br>The recommendations from this internal review were implemented with the revised version 3.1 of the BORN |

| | | |
|---|---|---|
| | | Privacy and Security Management Plan, which was approved by the PSRC on July 22, 2022, except where noted below:<br><br>Recommendations:<br>1. Improved tools for review of Research Plans to assist with review of these in relation to the requirements of PHIPA and its regulation.<br>2. Improved transparency in Privacy policy for what it means to "facilitate or improve the provision of health care," including our program commitments and PSO.<br>3. Improved clarity, consistency, and conformity with the structure of the Manual in relation to the maintenance of data holdings.<br>4. The data governance framework should be updated to incorporate more formal oversight of BORN's system generated reporting systems through the RPDC.<br>5. At inception, BORN started with the BORN Information System. Over time, extensions have been developed (e.g., the MIS and CART+ and in the future, the BDW). Those systems should be included within the glossary, policies, and procedures to clarify that they are all subject to the same set of policies.<br>6. For improved transparency, the plan should be updated to build express references to clinical and external advisory committees that influence our collection, retention, use and disclosure decisions at the data committees.<br>7. The policies and procedures should make use of more checklists or forms to assist committees with data decisions (collection, use, disclosure, and retention). This will help ensure continued operational compliance and simplify the application of our procedures to assist decision making.<br>8. Subject to the limitations and requirements of PHIPA and the Manual, BORN has the authority to disclose personal health information for the purpose of facilitating or improving the provision of health care under PHIPA, but the procedures and decision-making processes are not sufficiently described. Those procedures should be further developed to ensure that BORN has the capacity to make PHI available when appropriate.<br>9. BORN should revise policies and procedures related to de-identification and aggregation of data to overcome the constraints of de-identification software and develop additional tools to assist with risk-based assessments.<br>10. BORN should incorporate a Data Vigilance policy for adaptive decision making regarding additional use |

| | | |
|---|---|---|
| | | limitations as may be recommended by external committees.<br>11. BORN should consider incorporating an interim Indigenous Data Governance policy in respect of reports that identify Indigenous Peoples so that as changes are implemented over time in respect of Indigenous Data Governance, we can more readily implement such changes.<br>12. An expanded glossary with more roles is needed to improve consistency throughout the procedures and to help agents better understand their roles and responsibilities.<br>13. The end user terms for the services delivered through the BORN Systems should be updated.<br>14. Additional follow-up with TPSP is recommended in regard to extension of third-party audit that a subsidiary is currently undertaking.<br>• Target completion date was March 31, 2024. Confirmed completion in October 2023.<br>15. Improved supporting documentation for Agent access requests into the Privacy Office is recommended.<br>• Was piloted with the BORN Management Team, and subsequently revised given identified operational issues. Informed by the findings in the first implementation, the approval process will be updated in the 2023-2024 fiscal year (by March 31, 2024).<br>16. Except for BORN Agents, all permissions to the BIS need an underlying agreement to support the end user terms (i.e., even for those who do not have access to anything other than aggregate data). Four were identified as not having current agreement and they should be put into place.<br>17. Our existing holdings listed in the policies should be updated to reflect recent changes.<br><br>**Action plan to address recommendations:**<br>Adoption of the proposed revisions to Part 1 of the plan (3.1 revised Privacy and Security Management Plan) would address all recommendations (with the exceptions of:<br>- Five (5) agreements recommended for organizations with access to de-identified system generated reports since end user terms anticipate this structure. These agreements have been drafted, three (3) have been executed, and two (2) are nearing completion. Access to the Midwifery Stakeholder aggregate reports has |

| | | |
|---|---|---|
| | | not been removed, and access by those who have signed the End User Agreement for the BORN Information System is being logged and monitored.<br>- The privacy office requested the extension of a third-party audit to encompass all services supplied by the TPSP. The TPSP has completed the audit encompassing all services supplied by the TPSP. |
| 17 | June 2022<br>Audit of Log of Confidentiality Agreements (HR-07) for 2020 fiscal year | Review of staff Confidentiality Agreements for all BORN Staff to ensure that all current Agents renewed their confidentiality pledge with BORN and that all Agent agreements were up-to-date and in good standing for 2021-2022 fiscal year.<br><br>No recommendations. All documentation in line with expectations |

## 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:**
46 privacy incidents

***Indicator:***
*With respect to each privacy breach or suspected privacy breach:*

1. *The date that the notification was received,*
2. *The extent of the privacy breach or suspected privacy breach,*
3. *Whether it was internal or external,*
4. *The nature and extent of personal health information at issue,*
5. *The date that senior management was notified,*
6. *The containment measures implemented,*
7. *The date(s) that the containment measures were implemented,*
8. *The date(s) that notification was provided to the health information custodians or any other organizations,*
9. *The date that the investigation was commenced,*
10. *The date that the investigation was completed,*
11. *A brief description of each recommendation made,*
12. *The date each recommendation was addressed or is proposed to be addressed, and*
13. *The manner in which each recommendation was addressed or is proposed to be addressed.*

**BORN Response:**
Privacy incidents mostly related to external data provider sites inadvertently sending PHI via email to troubleshoot data entry issues. Specific follow up is provided at the time. Additionally, the privacy office provided training at the annual session in October 2021 to assist BORN Agents to mitigate these incident

occurrences with sites. Additionally, BORN will be using its best efforts to implement the following changes to its Data Sharing Agreements with submitter sites commencing September 15, 2022, for completion by January 31, 2023:

- Adding a clause requiring the data provider to ensure that authorized users complete privacy training before access is granted.
- Adding a clause that requires the data provider and BORN to coordinate privacy breach notification and investigation obligations if such a scenario arises.
- An additional clause to the End User Terms to complete the privacy training is also to be implemented though the BORN Systems no later than September 15, 2022.

In addition, there were 5 incidents regarding sites sending COVID Report Forms by email rather than the instructed method for transfer to use the BIS secure messaging service in the BORN Information System. A risk was identified as a result of the COVID pandemic, and this item was logged in the risk log and there is a planned technology solution through the introduction of a new encounter in the BIS related to the pandemic, which has not yet been implemented as it awaits funding related to the development. In the interim, BORN Agent coordinators work with their sites to help guide them on the proper delivery processes in sending PHI to BORN.

| No. | Incident Details/Containment/Recommendations |
|---|---|
| 1 | 1. Date notification was received: July 2, 2020<br>2. Extent of the privacy incident: A BORN data provider hospital site sent an email to a BORN Agent with an attachment containing PHI of COVID data report forms<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: COVID data report forms containing PHI sent to BORN by data provider site<br>5. Date senior management notified: July 2, 2020<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: July 2, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations:<br>9. Date investigation commenced: July 2, 2020<br>10. Date investigation completed: July 2, 2020<br>11. Brief description of each recommendation made: A risk was entered into the Risk Log pertaining to the use of sites using email to send COVID Report Forms instead of using the BIS messaging Tool. A technology solution was considered and funding for the solution was requested, however it was not implemented as BORN ceased collecting the COVID Report Form on Dec 31, 2022<br>12. Date each recommendation addressed or proposed to be addressed: n/a BORN ceased collecting the COVID Report Form on December 31, 2022<br>13. Manner in which each recommendation was addressed or is proposed to be addressed: n/a BORN ceased collecting the COVID Report Form on December 31, 2022 |

| | |
|---|---|
| 2 | 1. Date notification was received: July 13, 2020<br>2. Extent of the privacy incident: July 13, 2020<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: COVID data report form containing PHI sent to BORN by data provider site (Midwifery Practice Group) to the Information BORN mailbox as an attachment<br>5. Date senior management notified: July 30, 2020<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: July 13, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: July 13, 2020<br>10. Date investigation completed: July 13, 2020<br>11. Brief description of each recommendation made: A risk was entered into the Risk Log pertaining to the use of sites using email to send COVID Report Forms instead of using the BIS messaging Tool. A technology solution was considered and funding for the solution was requested, however it was not implemented as BORN ceased collecting the COVID Report Form on Dec 31, 2022<br>12. Date each recommendation addressed or proposed to be addressed: BORN ceased collecting the COVID Report Form on December 31, 2022<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: BORN ceased collecting the COVID Report Form on December 31, 2022 |
| 3 | 1. Date notification was received: July 24, 2020<br>2. Extent of the privacy incident: BORN Agent inadvertently placed PHI in a file on a shared drive accessible to other BORN Agents. Another BORN Agent discovered the incident while reviewing the file and informed the privacy office<br>3. Internal or External: Internal<br>4. Nature and extent of PHI at issue: PHI - name, birthdate, and birth location of a baby in a file on a shared drive accessible to other BORN Agents<br>5. Date senior management notified: July 30, 2020<br>6. Containment measures implemented: The PHI was removed from the file as soon as it was discovered, and the incident was fully contained. Privacy office followed up with the Agent<br>7. Dates containment measures implemented: July24, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: July 24, 2020<br>10. Date investigation completed: July 24, 2020<br>11. Brief description of each recommendation made: None – isolated mistake dealt with through specific reminder by privacy office at the time of the incident and general training at the annual meeting<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 4 | 1. Date notification was received: Aug 10, 2020<br>2. Extent of the privacy incident: Data provider site (hospital) sent an email to a BORN Agent that contained PHI for 19 patients from the BORN Information System<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: personal health information<br>5. Date senior management notified: Sept 2020 |

| | |
|---|---|
| | 6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN<br>7. Dates containment measures implemented: Aug 10, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Aug 10, 2020<br>10. Date investigation completed: Aug 10, 2020<br>11. Brief description of each recommendation made: none - Isolated mistake dealt with through specific reminder to use the BIS Messaging Tool to send PHI securely to BORN<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 5 | 1. Date notification was received: Aug 11, 2020<br>2. Extent of the privacy incident: BORN Agent sent an email to their BORN team that contained PHI (chart number). The BORN Agent contacted the Privacy Office to confirm that a chart number was indeed PHI. The Privacy Office contacted the Agent that sent the email to discuss the incident. The Agent advised that they were not aware that a chart number alone was considered PHI. Additional clarification and training and education was provided to the Agent on PHI.<br>3. Internal or External: Internal<br>4. Nature and extent of PHI at issue: Chart number<br>5. Date senior management notified: Sept 2020<br>6. Containment measures implemented: The BORN Agent was instructed to delete the email, and the email was subsequently deleted from their sent box and delete bin. The email was deleted from the inbox and delete bin by all team members that received the email, and the incident was fully contained.<br>7. Dates containment measures implemented: The email was deleted from sent box, inbox, delete bins and server (if applicable) by all BORN Agents copies on the email<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Aug 11, 2020<br>10. Date investigation completed: Aug 11, 2020<br>11. Brief description of each recommendation made: None – isolated mistake dealt with through specific follow-up by privacy office and general training at the annual meeting<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 6 | 1. Date notification was received: Aug 17, 2020<br>2. Extent of the privacy incident: Data provider hospital site sent an email to a BORN Agent that contained PHI to troubleshoot an issue that they were having<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Patient name, DOB, and hospital ID)<br>5. Date senior management notified: Sept 2020<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN |

| | |
|---|---|
| | 7. Dates containment measures implemented: Aug 17, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Aug 17, 2020<br>10. Date investigation completed: Aug 17, 2020<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 7 | 1. Date notification was received: Sept 14, 2020<br>2. Extent of the privacy incident: A data provider site sent a BIS message to a BORN Agent and inadvertently included another BORN Agent in the communication that had a patient's ID number, details of location and dates<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: patient's ID number details of location and dates<br>5. Date senior management notified: Sept 14, 2020<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN<br>7. Dates containment measures implemented: Sept 14, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Sept 14, 2020<br>10. Date investigation completed: Sept 14, 2020<br>11. Brief description of each recommendation made: None - isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 8 | 1. Date notification was received: Dec 9, 2020<br>2. Extent of the privacy incident: Midwife at a Midwifery Practice Group inadvertently sent an email to a BORN Agent that contained a client code.<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: Feb 26, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Dec 9, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Dec 9, 2020<br>10. Date investigation completed: Dec 9, 2020<br>11. Brief description of each recommendation made: None - isolated mistake dealt with through specific reminder and general training at the annual meeting |

| | |
|---|---|
| | 12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 9 | 1. Date notification was received: Dec 17, 2020<br>2. Extent of the privacy incident: A midwife at a Midwifery Practice Group data provider, inadvertently sent an email to a BORN Agent that Contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: Feb 26, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Dec 17, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Dec 17, 2020<br>10. Date investigation completed: Dec 17, 2020<br>11. Brief description of each recommendation made: None – isolated incident<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 10 | 1. Date notification was received: Dec 22, 2020<br>2. Extent of the privacy incident: A midwife at a Midwifery Practice Group data provider, inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: Feb 26, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN<br>7. Dates containment measures implemented: Dec 22, 2020<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Dec 22, 2020<br>10. Date investigation completed: Dec 22, 2020<br>11. Brief description of each recommendation made: None – isolated incident<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |

| | |
|---|---|
| 11 | 1. Date notification was received: Jan 13, 2021<br>2. Extent of the privacy incident: Data provider site (hospital) inadvertently sent an email to a BORN Agent that contained a PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Chart ID in an email<br>5. Date senior management notified: Feb 26, 2020<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN<br>7. Dates containment measures implemented: Jan 13, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: Jan 13, 2021<br>10. Date investigation completed: Jan 13, 2021<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 12 | 1. Date notification was received: Jan 14, 2021<br>2. Extent of the privacy incident: Inadvertent disclosure within BORN between BORN agents --- more PHI than was required was inadvertently copied to a data analyst student folder on the PHI X Drive<br>3. Internal or External: Internal<br>4. Nature and extent of PHI at issue: More PHI than was required was inadvertently copied to a data analyst student folder on the PHI X Drive<br>5. Date senior management notified: Feb 26, 2021<br>6. Containment measures implemented: The student noticed immediately that the data set contained more variables than required. She advised her supervisor and was instructed to not enter into the folder or touch any data until it could be removed. The additional variables were deleted from the folder and the incident was fully contained.<br>7. Dates containment measures implemented: Jan 14, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: Jan 14, 2021<br>10. Date investigation completed: Jan 14, 2021<br>11. Brief description of each recommendation made: None - isolated mistake dealt with through specific reminder and general training at the annual meeting<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |

| | |
|---|---|
| 13 | 1. Date notification was received: Feb 9, 2021<br>2. Extent of the privacy incident: Data provider hospital site sent an email to a BORN Agent that contained a PHI COVID Report form<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Email from a hospital that contained a COVID Report Form<br>5. Date senior management notified: Feb 26, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Feb 9, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Brief description of each recommendation made: A risk was entered into the Risk Log pertaining to the use of sites using email to send COVID Report Forms instead of using the BIS messaging Tool. A technology solution was considered and funding for the solution was requested, however it was not implemented as BORN ceased collecting the COVID Report Form on Dec 31, 2022.<br>10. Date each recommendation addressed or proposed to be addressed: n/a BORN ceased collecting the COVID Report Form on Dec 31, 2022<br>11. The manner in which each recommendation was addressed or is proposed to be addressed: n/a – BORN ceased collecting the COVID Report Form on Dec 31, 2022 |
| 14 | 1. Date notification was received: Feb 11, 2021<br>2. Extent of the privacy incident: Data provider Hospital site sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: OHIP number<br>5. Date senior management notified: Feb 26, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Feb 11, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Feb 11, 2021<br>10. Date investigation completed: Feb 11, 2021<br>11. Brief description of each recommendation made: None<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 15 | 1. Date notification was received: Mar 9, 2021<br>2. Extent of the privacy incident: A BORN data provider site (hospital) sent an email to a BORN Agent with an attachment containing PHI of COVID Report Forms<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: COVID Report Form |

| | |
|---|---|
| | 5. Date senior management notified: Apr 20, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Mar 9, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 9, 2021<br>10. Date investigation completed: Mar 9, 2021<br>11. Brief description of each recommendation made: A risk was entered into the Risk Log pertaining to the use of sites using email to send COVID Report Forms instead of using the BIS messaging Tool. A technology solution was considered and funding for the solution was requested, however it was not implemented as BORN ceased collecting the COVID Report Form on Dec 31, 2022.<br>12. Date each recommendation addressed or proposed to be addressed: n/a BORN ceased using the COVID Report Form on Dec 31, 2022<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a BORN ceased using the COVID Report Form on Dec 31, 2022 |
| 16 | 1. Date notification was received: Mar 22, 2021<br>2. Extent of the privacy incident: Data provider site (Midwifery Practice Group) inadvertently sent an email to a BORN Agent that contained a PHI - client code.<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: Apr 20, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Mar 22, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 22, 2021<br>10. Date investigation completed: Mar 22, 2021<br>11. Brief description of each recommendation made: None – isolated mistake by a midwife<br>12. Date each recommendation addressed or proposed to be addressed: n/a BORN ceased collecting the COVID Report Form on Dec 31, 2022<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a BORN ceased collecting the COVID Report Form on Dec 31, 2022 |
| 17 | 1. Date notification was received: Mar 22, 2021<br>2. Extent of the privacy incident: Data provider site (Midwifery Practice Group) inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Patient name, OHIP number, client code and DOB<br>5. Date senior management notified: Apr 20, 2021 |

| | |
|---|---|
| | 6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Mar 22, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 22, 2021<br>10. Date investigation completed: Mar 22, 2021 |
| 18 | 1. Date notification was received: Mar 29, 2021<br>2. Extent of the privacy incident: Data provider site (hospital) inadvertently sent an email to a BORN Agent that contained PHI. The site submission included an attempt to cover the PHI using tape, but the information was still visible through the tape<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Patient name, ID number<br>5. Date senior management notified: Apr 20, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Mar 29, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 29, 2021<br>10. Date investigation completed: Mar 29, 2021<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 19 | 1. Date notification was received: Mar 30, 2021<br>2. Extent of the privacy incident: A file was created by a BORN Agent that contained PHI was accidently loaded to SharePoint.<br>3. Internal or External: Internal<br>4. Nature and extent of PHI at issue: Health Card Number, First Name, Last Name, Address, BIS Identifier<br>5. Date senior management notified: Apr 20, 2021<br>6. Containment measures implemented: The PHI was removed from the file on SharePoint and the incident was fully contained<br>7. Dates containment measures implemented: Mar 30, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 30, 2021<br>10. Date investigation completed: Mar 30, 2021<br>11. Brief description of each recommendation made: None - isolated mistake dealt with through specific reminder and general training at the annual meeting |

| | |
|---|---|
| | 12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 20 | 1. Date notification was received: Apr 21, 2021<br>2. Extent of the privacy incident: While a BORN Agent was investigating a data quality issue, it was discovered that BORN inadvertently received data from a lab that contained out of province data in October 2018. The BORN Information System should only contain Ontario data and it was determined that the records should be deleted.<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Out of province personal health information<br>5. Date senior management notified: May 18, 2020<br>6. Containment measures implemented: The PSO Team worked with the Information Security Officer to remove the erroneous files from the BORN Information System. The incident was fully contained<br>7. Dates containment measures implemented: Apr 21, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Apr 21, 2021<br>10. Date investigation completed: Apr 21, 2021<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 21 | 1. Date notification was received: May 25, 2021<br>2. Extent of the privacy incident: A hospital site sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Ultrasound personal health information<br>5. Date senior management notified: Jul 21, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: May 25, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: May 25, 2021<br>10. Date investigation completed: May 25, 2021<br>11. Brief description of each recommendation made: none<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 22 | 1. Date notification was received: Jun 2, 2021<br>2. Extent of the privacy incident: Data provider site (hospital) sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Maternal cytogenetics records DOB, OHIP, postal code, city, and genetic results<br>5. Date senior management notified: Jul 21, 2021 |

| | |
|---|---|
| | 6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Jun 2, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Jun 2, 2021<br>10. Date investigation completed: Jun 2, 2021<br>11. Brief description of each recommendation made: None<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 23 | 1. Date notification was received: Jun 30, 2021<br>2. Extent of the privacy incident: A BORN Agent inadvertently sent an email containing PHI to other BORN Agents on their team containing PHI<br>3. Internal or External: Internal<br>4. Nature and extent of PHI at issue: Chart numbers, hospital name<br>5. Date senior management notified: Jul 21, 2021<br>6. Containment measures implemented: The BORN Agent was instructed to delete the email, and the email was subsequently deleted from their sent box and delete bin. The other BORN Agents on the team were instructed to delete the email from their inbox and delete bin and advise when it was done. Confirmation that all emails pertaining to the incident were deleted was received and the incident was fully contained.<br>7. Dates containment measures implemented: Jun 30, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: Jun 30, 2021<br>10. Date investigation completed: Jun 30, 2021<br>11. Brief description of each recommendation made: None - isolated mistake dealt with through specific reminder and general training at the annual meeting<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 24 | 1. Date notification was received: Aug 20, 2021<br>2. Extent of the privacy incident: A stakeholder site (The Ontario Midwifery Program) inadvertently sent an email attachment to a BORN Agent that contained PHI. The BORN Agent did not realize that the attachment contained PHI and they forwarded the email to another BORN Agent.<br>3. Internal or External: External / Internal<br>4. Nature and extent of PHI at issue: Client codes and client addresses<br>5. Date senior management notified: Sep 21, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so. The BORN Agent who received the email from the site was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The BORN Agent who received the email from their teammate was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email from their sent box and delete bin. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Aug 20, 2021 |

| | |
|---|---|
| | 8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Aug 20, 2021<br>10. Date investigation completed: Aug 20, 2021<br>11. Brief description of each recommendation made: none – isolated incident<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 25 | 1. Date notification was received: Aug 26, 2021<br>2. Extent of the privacy incident: Data provider site (hospital) inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Hospital chart numbers<br>5. Date senior management notified: Sep 21, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN<br>7. Dates containment measures implemented: Aug 26, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: Aug 26, 2021<br>10. Date investigation completed: Aug 26, 2021<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 26 | 1. Date notification was received: Sep 9, 2021<br>2. Extent of the privacy incident: An internal data provider site (NSO) inadvertently sent an email to a BORN Agent containing PHI<br>3. Internal or External: Internal<br>4. Nature and extent of PHI at issue: Newborn Screening Ontario personal health information<br>5. Date senior management notified: Sep 21, 2021<br>6. Containment measures implemented: The individual at NSO was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent who received the email was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Sep 9, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: Sep 9, 2021<br>10. Date investigation completed: Sep 9, 2021<br>11. Brief description of each recommendation made: None – isolated incident<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |

| | |
|---|---|
| 27 | 1. Date notification was received: Sep 9, 2021<br>2. Extent of the privacy incident: A BORN data provider site (hospital) sent an email to a BORN Agent with an attachment containing PHI of COVID data report forms<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: COVID Report Form<br>5. Date senior management notified: Sep 21, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Sep 9, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Sep 9, 2021<br>10. Date investigation completed: Sep 9, 2021<br>11. Brief description of each recommendation made: A risk was entered into the Risk Log pertaining to the use of sites using email to send COVID Report Forms instead of using the BIS messaging Tool. A technology solution was considered and funding for the solution was requested, however it was not implemented as BORN ceased collecting the COVID Report Form on Dec 31, 2022<br>12. Date each recommendation addressed or proposed to be addressed: n/a - BORN ceased collecting the COVID Report Form on Dec 31, 2022<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a - BORN ceased collecting the COVID Report Form on Dec 31, 2022 |
| 28 | 1. Date notification was received: Dec 6, 2021<br>2. Extent of the privacy incident: A BORN Coordinator (Agent) discovered that on 3 separate occasions, a hospital staff member who has BIS privileges at 2 different hospitals, entered postpartum mother and HBHC encounters under the wrong site<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Postpartum mother and Heathy Babies Healthy Children encounters containing PHI<br>5. Date senior management notified: Dec 21, 2021<br>6. Containment measures implemented: The BORN Agent contacted the site to advise of them of their error and deleted the incorrect encounters in the BORN Information System (BIS). The incident was fully contained<br>7. Dates containment measures implemented: Dec 6, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Dec 6, 2021<br>10. Date investigation completed: Dec 6, 2021<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |

| | |
|---|---|
| 29 | 1. Date notification was received: Dec 9, 2021<br>2. Extent of the privacy incident: Data provider site (hospital lab) inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Postal code<br>5. Date senior management notified: Dec 21, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Dec 9, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Dec 9, 2021<br>10. Date investigation completed: Dec 9, 2021<br>11. Brief description of each recommendation made: None - isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 30 | 1. Date notification was received: Dec 13, 2021<br>2. Extent of the privacy incident: Data provider site (hospital) inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: PHI Clinical Care details<br>5. Date senior management notified: Dec 21, 2021<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Dec 13, 2021<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Dec 13, 2021<br>10. Date investigation completed: Dec 13, 2021<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 31 | 1. Date notification was received: Jan 10, 2022<br>2. Extent of the privacy incident: Data provider site (hospital) inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Chart numbers<br>5. Date senior management notified: Mar 21, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed |

| | |
|---|---|
| | to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Jan 10, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: Jan 10, 2022<br>10. Date investigation completed: Jan 10, 2022<br>11. Brief description of each recommendation made: None<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 32 | 1. Date notification was received: Feb 15, 2022<br>2. Extent of the privacy incident: A BORN Agent inadvertently sent another BORN Agent an email that contained PHI<br>3. Internal or External: Internal<br>4. Nature and extent of PHI at issue: Newborn Screening Chart numbers<br>5. Date senior management notified: Mar 21, 2022<br>14. Containment measures implemented: The BORN Agent was instructed to delete the email, and the email was subsequently deleted from their sent box and delete bin. The BORN Agent who received the email was instructed to delete the email, and the email was subsequently deleted from their inbox and delete bin. The incident was fully contained.<br>6. .<br>7. Dates containment measures implemented: Feb 15, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Feb 15, 2022<br>10. Date investigation completed: Feb 15, 2022<br>11. Brief description of each recommendation made: None - isolated mistake dealt with through specific reminder and general training at the annual meeting<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 33 | 1. Date notification was received: Feb 24, 2022<br>2. Extent of the privacy incident: Data provider site (lab manager at a hospital site) sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: - patient's name, HCN, sex, DOB, postal code, date of sample, acc #, clinical indication, results<br>5. Date senior management notified: Mar 21, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Feb 24, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Feb 24, 2022 |

| | |
|---|---|
| | 10. Date investigation completed: Feb 24, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 34 | 1. Date notification was received: Mar 14, 2022<br>2. Extent of the privacy incident: Data provider sent an email to BORN Team member working on the ORU project that contained PHI to help problem solve an issue. The note was sent to 6 BORN recipients<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: List of Medical Record Numbers (MRN)<br>5. Date senior management notified: Mar 21, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the 6 BORN Agents who were copied on the email were instructed to delete the email, and subsequently all 6 BORN Agents deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: xx<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 14, 2022<br>10. Date investigation completed: Mar 14, 2022<br>11. Brief description of each recommendation made: None<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 35 | 1. Date notification was received: Mar 21, 2022<br>2. Extent of the privacy incident: Data provider site (hospital) inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: PHI in an email inquiry<br>5. Date senior management notified: Mar 21, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Mar 21, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 21, 2022<br>10. Date investigation completed: Mar 21, 2022<br>11. Brief description of each recommendation made: None - isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |

| | |
|---|---|
| 36 | 1. Date notification was received: Mar 21, 2022<br>2. Extent of the privacy incident: A hospital site sent an email to the BORN Help Desk containing patient PHI – Help Desk loaded the information into CHEO Vector System and then contacted a BORN Agent to address.<br>3. Internal or External: External and Internal<br>4. Nature and extent of PHI at issue: Mother and baby chart numbers<br>5. Date senior management notified: Mar 21, 2022<br>6. Containment measures implemented: The BORN Agent reminded the BORN Help Desk that PHI should never be entered into the Vector system. BORN Agent instructed the Help Desk to delete the ticket and email and then contacted the site instructing them that they must delete the email from their sent box and send an email confirmation when done. The site confirmed that they deleted the email from their sent box and delete bin. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Mar 21, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 21, 2022<br>10. Date investigation completed: Mar 21, 2022<br>11. Brief description of each recommendation made: None<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 37 | 1. Date notification was received: Mar 29, 2022<br>2. Extent of the privacy incident: A midwife at a Midwifery Practice Group sent an email that contained PHI to a BORN Agent to troubleshoot an issue<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: May 16, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Mar 29, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 29, 2022<br>10. Date investigation completed: Mar 29, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 38 | 1. Date notification was received: Mar 30, 2022<br>2. Extent of the privacy incident: Local Admin at a hospital site requesting help sent an email to a BORN Agent containing PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: May 16, 2022 |

| | |
|---|---|
| | 6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Mar 30, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Mar 30, 2022<br>10. Date investigation completed: Mar 30, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 39 | 1. Date notification was received: Apr 11, 2022<br>2. Extent of the privacy incident: Data provider hospital site sent an email to a BORN Agent that contained (PHI)<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Hospital ID number<br>5. Date senior management notified: May 16, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: April 11, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Apr 11, 2022<br>10. Date investigation completed: Apr 11, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 40 | 1. Date notification was received: May 10, 2022<br>2. Extent of the privacy incident: Midwife at Midwifery Practice Group inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: May 16, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: May 10, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a |

| | |
|---|---|
| | 9. Date investigation commenced: May 10, 2022<br>10. Date investigation completed: May 10, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 41 | 1. Date notification was received: May 12, 2022<br>2. Extent of the privacy incident: Hospital sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: OHIP number<br>5. Date senior management notified: May 16, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: May 12, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: May 12, 2022<br>10. Date investigation completed: May 12, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 42 | 1. Date notification was received: May 30, 2022<br>2. Extent of the privacy incident: Midwife at Midwifery Practice Group inadvertently sent an email to a BORN Agent that contained PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: Jun 22, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: May 30, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: May 30, 2022<br>10. Date investigation completed: May 30, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |

| | |
|---|---|
| 43 | 1. Date notification was received: Jun 7, 2022<br>2. Extent of the privacy incident: Hospital sent a file that contained potential PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Ultrasound data<br>5. Date senior management notified: Jun 22, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Jun 7, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Jun 7, 2022<br>10. Date investigation completed: Jun 7, 2022<br>11. Brief description of each recommendation made: none – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 44 | 1. Date notification was received: Jun 8, 2022<br>2. Extent of the privacy incident: Hospital sent email containing PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Hospital ID number for a patient<br>5. Date senior management notified: Jun 22, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they<br>must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Jun 8, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: n/a<br>9. Date investigation commenced: Jun 8, 2022<br>10. Date investigation completed: Jun 8, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 45 | 1. Date notification was received: Jun 15, 2022<br>2. Extent of the privacy incident: A midwife at a Midwifery Practice Group sent an email containing PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: Jun 22, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Jun 15, 2022 |

| | |
|---|---|
| | 8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: Jun 15, 2022<br>10. Date investigation completed: Jun 15, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |
| 46 | 1. Date notification was received: Jun 24, 2022<br>2. Extent of the privacy incident: A midwife at a Midwifery Practice Group sent an email containing PHI<br>3. Internal or External: External<br>4. Nature and extent of PHI at issue: Client code<br>5. Date senior management notified: Jul 19, 2022<br>6. Containment measures implemented: The site was instructed to delete the email from their sent box and delete bin and to provide email confirmation that they did so, and the BORN Agent was instructed to delete the email, and subsequently deleted the email from their inbox and delete bin. The site confirmed that they deleted the email. The incident was fully contained. The site was reminded that they must use the secure BIS Messaging Tool when sending PHI to BORN.<br>7. Dates containment measures implemented: Jun 24, 2022<br>8. Date(s) notification provided to the health information custodians or any other organizations: xx<br>9. Date investigation commenced: Jun 24, 2022<br>10. Date investigation completed: Jun 24, 2022<br>11. Brief description of each recommendation made: None – isolated mistake<br>12. Date each recommendation addressed or proposed to be addressed: n/a<br>13. The manner in which each recommendation was addressed or is proposed to be addressed: n/a |

## 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, Procedures and Practices

***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:**
The formal update and review of the security policies and procedures by the PSRC took place on July 12, 2022. Working review sessions, and related PSRC meetings, occurred on the following dates:

| ***Date of review meeting*** | ***Group/Committee conducting the review*** | |
|---|---|---|
| February 11, 2022 | 3.1 Working Group | |
| February 15, 2022 | | PSRC |
| February 25, 2022 | 3.1 Working Group | |
| February 26, 2022 | 3.1 Working Group | |
| March 11, 2022 | 3.1 Working Group | |
| March 21, 2022 | | PSRC |
| March 25, 2022 | 3.1 Working Group | |
| April 7, 2022 | 3.1 Working Group | |
| April 8, 2022 | 3.1 Working Group | |
| April 19, 2022 | | PSRC |
| April 22, 2022 | 3.1 Working Group | |
| May 6, 2022 | 3.1 Working Group | |
| May 16, 2022 | | PSRC |
| May 20, 2022 | 3.1 Working Group | |
| June 3, 2022 | 3.1 Working Group | |
| June 22, 2022 | | PSRC |
| June 30, 2022 | 3.1 Working Group | PSRC |
| July 12, 2022 | | PSRC |

Security policies and procedures are reviewed at a minimum:

(i.) every three (3) years during the triennial review and approval process;
(ii.) when a new Manual or guidance is issued; or
(iii.) When the law or regulations are amended.

***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**:
"Compliance, Audit and Enforcement" and "Notification of Breach" details have been removed from the footnotes and added as separate sections to each appropriate policy.

References to Secure Socket Layer (SSL) encryption has been updated to Transport Layer Security (TLS) encryption to align with industry standards.

Improved structural alignment to the Manual in all policies.

**S-03: Ensuring Physical Security of Personal Health Information**
Details have been added that differentiate the BORN offices and data centres where BORN retains PHI and the policy, procedures, and practices with respect to access by BORN agents. It further details the policy, procedures, and practices with respect to access by visitors in all BORN associated locations:

> "Visitors to the BORN premises must be supervised by a BORN Agent at all times, including departure and are required to sign in and record their name, date and time of arrival, time of departure and the name of the Agent(s) with whom the visitors are meeting. Visitors must wear identification issued by the Information Security Officer; the supervising agent ensures the identification is returned prior to departure; and ensures that the visitors complete the appropriate documentation upon arrival and departure. "

**S-05: Secure Retention of Records of PHI**
This policy has been updated to align with the privacy policy P-08: Limiting Agent Access to and Use of Personal Health Information. The policy has been simplified to ensure all agents are aware that they 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, collection, or disposal.

The retention period for PHI has been further clarified. For records of PHI used for Research purposes, BORN's policy is that the records of PHI are not being retained for a period longer than that set out in the written Research Plan approved by a REB. For records of PHI collected pursuant to a Data Sharing Agreement, BORN prohibits the records from being retained for a period longer than that set out in the Data Sharing Agreement. Subject to any earlier date decided by the BORN DHC or as required in the applicable data sharing agreement, records will be maintained in identifiable form within the transactional database for 28 years. For the avoidance of any doubt Retention in the PHI Storage Vault ("X" drive) is based on REB requirements as set out in individual research agreements. Project specific PHI (e.g., for the creation of ad hoc reports for non-research purposes) is to be deleted in a secure manner as set out in the BORN policy S-08: Secure Disposal of Records of Personal Health Information.

The policy further defines where and how PHI is allowed to be securely retained.

**S-06: Securing Records of PHI on Mobile Devices and Remotely Accessing PHI**
The policy has been updated to prohibit the storage, collection, use, disclosure, retainment, transfer and/or disposal of personal health information on mobile computing equipment. Mobile Computing Equipment includes laptops, Universal Serial Bus (USB) flash drives, external hard drives, CDs, DVDs, and other mobile and mass storage devices. Previously this had been allowed under exceptional circumstances with the approval of the privacy officer.

The use of cloud services for file storing and sharing (e.g., Dropbox and Google Drive) is now expressly prohibited for collecting, using, disclosing, retaining, transferring and/or disposing of PHI.

Details on accessing PHI through a secure connection or a virtual private network (VPN) have been added to the policy specifically for the BORN Azure back-end environment.

**S-08: Secure Disposal of Records of Personal Health Information**
The responsibility for this policy and its associated procedures has been updated to be the Information Security Officer.

The method of secure disposal of electronic records is now defined to be, at a minimum, the U.S. Department of Defense (DoD 5220.22-M) secure deletion method.

**S-09: Passwords and Multi-Factor Authentication**
The procedures for assigning and resetting passwords for all BORN systems has been thoroughly detailed to align with current practices and industry standards.

The lifetime of BORN systems passwords has been extended to one-year (365) days.

The conditions surrounding the use of password managers has been added to the policy.

**S-10: Logging, Monitoring and Auditing Privacy and Information Security Events**
The structure of this policy has undergone extensive changes to align with updated Information and Privacy Commissioner of Ontario guidance and terminology and to make it easier to understand.

The policy and procedures have been updated to specifically outline which privacy and information security events to log, what information must be contained for each entry, the methods of monitoring the networks, information systems, technologies, applications, and programs relating to PHI for privacy and information security events, and the reasons for which, and circumstances in which, audits of the logs of privacy and information security events must be conducted.

Furthermore, the policy and procedures identify the specific BORN Systems and information sources that must be systematically monitored (i.e., scope of monitoring) and who is responsible for that monitoring, to identify and assess real-time evidence of actual or potential privacy breaches and/or information security breaches.

A section on selection, use, and configuration of monitoring tools has been added as well as procedures for reviewing, assessing, and responding to outputs of those tools.

The policy and procedures now detail the relationship with BORN's privacy and security audit policies including the specific types of audits that must be conducted.

A section on the review of logging, monitoring, and auditing practices has been added to ensure an evaluation of the efficacy of the current practices is conducted on an annual basis.

**S-11: Vulnerability and Patch Management**

The structure of this policy has undergone changes to bring it into alignment with industry best practices and standards and BORN practices with the majority of the changes made to the vulnerability management section.

The vulnerability risk assessment and recommendations section introduce the criteria for determining impact and likelihood of risks as well as the description of likelihood levels and criteria. This section further requires that risks associated with identified vulnerabilities be assessed and that recommendations be developed and implemented to mitigate those risks in accordance with BORN's security audit policy.

**S-15: Security Audits**
To prevent the compromise of the confidentiality, integrity, and availability of the Production environment, the policy has been updated to indicate that penetration testing is performed against the BORN Staging environment. The BORN Staging environment is a duplicate of the Production environment. Any identified risks and recommendations resulting from testing the Staging environment are treated as though they were found in the Production environment.

The types of security audits have been updated to include audits of information security breach procedures (e.g., tabletop exercise).

**S-16: Log of Security Audits**
The policy has been updated in the case where a log entry relates to a vulnerability risk assessment. In this case, the log of security audits must also include:

- The risk severity for each identified vulnerability;
- A description of the vulnerability;
- The number of components within the BORN Environment with the identified vulnerability; and
- For each asset with the identified vulnerability:
    - The date that each recommendation was or is expected to be addressed; and
    - The manner in which each recommendation was or is expected to be addressed.

**S-17: Information Security Breach Management**
The definition of an information security breach has been updated to be:

- Any act or incident, internal or external, that actually or imminently jeopardizes the confidentiality and integrity of information in the custody and control of BORN or the Information Environment
- Constitutes a contravention or imminent threat of contravention of the Act or its regulations, the terms of any written agreements, other legal obligations, or security policies, procedures and practices implemented by BORN.

This policy has also been updated to include BORN's cybersecurity incident response plan and encompasses the six phases of incident response: preparation, detection, containment, investigation, remediation, and recovery.

BORN's methodology used to respond to information security breaches is based on the Information and Privacy Commissioner of Ontario, Healthcare Insurance Reciprocal of Canada (HIROC), and the National Institute of Standards and Technology (NIST) guidance.

Details on the severity and priority ratings of any actual or suspected breach has been added.

***Indicator:***
*Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.*

**BORN Response:**
No new security policies and procedures were developed or implemented as a result of the review.

***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:**
July 22, 2022, by email to all agents, together with a description of key changes. The Privacy and Security Management Plan was provided to all agents.

***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:**
The web pages on Privacy Frequently Asked Questions (FAQs) and Statement of Information Practices were both adapted to incorporate the overarching privacy policy. Concurrently, the former version of the privacy and security management was removed from the website.

## 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:**
No agents have been 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.

## 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:**
Review of audit log of agents granted approval to access and use personal health information since the prior review by the Information and Privacy Commissioner of Ontario are listed in the Privacy Audit Program section above.

A review of system controls was performed February 2022. A recommendation to implement a "VIP" flag in the BIS for high profile births/patients was noted. The ability to set a VIP flag was added to the BIS as well, audit reports were updated to highlight VIP patients on February 22, 2022.

System audit logs are continuously monitored and reviewed by the security team at BORN's Managed Service Provider. Anomalies are subject to specific log reviews as noted in the following table.

Specific reviews of audit logs were performed as follows:

| Date of Audit Log Review | Description | Findings |
|---|---|---|
| 2019-12-17 | Review of BIS audit logs after LifeLabs online booking system were compromised. LifeLabs sends data to the BIS through a secure web service. | BORN systems were not compromised. No privacy or security breach. |
| 2021-02-07 | Review of BIS audit logs and BORN PHI vault audit logs during and after cyber-attack at CHEO. | BORN systems and PHI holdings were not compromised. No privacy or security breach. |
| 2021-06-15 | Review of BIS audit logs after the Humber River hospital were hit with a ransomware attack. | BORN systems were not compromised. No privacy or security breach. |
| 2021-06-29 | Review of BIS audit logs after the KFL&A Public Health experienced a cyber security incident. | BORN systems were not compromised. No privacy or security breach. |
| 2021-08-13 | Review of BIS audit logs and BORN PHI vault audit logs after security team at MSP received phishing email from purported BORN agent to ensure agent's credentials were not compromised. | BORN systems were not compromised. BORN agent's email was spoofed (i.e., counterfeited). No privacy or security breach. |
| 2022-02-14 | Review of BIS audit logs after the Scarborough hospital were hit with a ransomware attack. | BORN systems were not compromised. No privacy or security breach. |
| 2022-03-09 | Firewall logs indicated an increased prevalence in outbound traffic attempts to the suspicious IP 139.45.197.253. | IP Address blocked for incoming and outgoing traffic. Investigation by security team at MSP indicated no issues. Further details in security incident section below. |

| | | |
|---|---|---|
| | | No privacy or security breach. |
| 2022-06-22 | Firewall logs indicated a notable increase in outbound traffic attempts from endpoints in monitored environments to 72.21.81. | IP Address blocked for incoming and outgoing traffic. Investigation by security team at MSP indicated no issues. Further details in security incident section below. No privacy or security breach. |

***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:**

| Nature/Typeof Security Audit | Date Audit Completed | Recommendations | Date Implemented or to Be Implemented | Manner in Which Each Recommendation was or is to be Addressed |
|---|---|---|---|---|
| Threat Risk Assessments | September 2021 | BORN should implement a 90-day password expiry policy based on their privacy and security management plan. | July 2022 | Policy S-09: Passwords and Multi-Factor Authentication was updated in version 3.1 to include the Azure environment and increase password lifetime to one year (365 days). |
| Threat Risk Assessments | September 2021 | BORN should implement additional security requirements for unlocking the account, such as asking secret questions and answers or user details. | July 2022 | Policy S-09: Passwords and Multi-Factor Authentication was updated to include the Azure environment in version 3.1 detailing password reset procedures for all environments. |
| Threat Risk Assessments | September 2021 | Local Admin rights are enabled by default in the | August 2022 | 1. Discover and document the purpose |

| | | | | |
|---|---|---|---|---|
| | | Azure environment. The level of access should only be granted on need-to-know and least privilege principles. | | of all local admin account(s).<br>2. Provide local admin access only on a need-to-know basis.<br>3. Review local admin access frequently and revoke the access if it is no longer required. |
| Threat Risk Assessments | September 2021 | In the Azure environment, BORN should define the maximum time period permitted for each session and sessions should be set to expire after the maximum time period. | August 2022 | BORN will work with their managed service provider to setup session timeouts on backend systems. |
| Threat Risk Assessments | September 2021 | While agreements with BORN's managed service provider protects BORN legally, it does not give BORN insight into who is accessing its systems. | August 2022 | 1. Document the purpose of all BORN<br>2. Azure accounts. Ensure provided access is only on a need-to-know basis.<br>3. Ensure all Azure accounts are approved by the BORN Information Security Officer.<br>4. Review access frequently and revoke the access if it is no longer required as per BORN policy S-15: Security Audits. |
| Threat Risk Assessments (FHIR Application) | June 17, 2022 | 1. Validate the request origin and do not trust in arbitrary cross-origins request.<br>2. Validate the redirect URI to only allow trusted URLs.<br>3. Configure the TLS session cookies with the Secure flag set.<br>4. Configure the HTTP response headers implementing the security headers and avoid returning sensitive system information. | Estimated October 2022 | Items 1 through 6 have been escalated to the application developer to address.<br><br>Item 7 is addressed as per BORN policy **S-15: Security Audits.**<br><br>Item 8 will be addressed upon completion of development updates for items 1 though 6. |

| | | | | |
|---|---|---|---|---|
| | | 5. Apply the latest patches and updates provided by the vendor.<br>6. Validate the application access permission to avoid unauthorized access to sensitive information.<br>7. Periodically perform security audits focusing on vulnerability analysis and intrusion testing to preventively detect and address identified security issues.<br>8. Perform a retest to validate if the remediation were properly applied and fixed all vulnerabilities. | | |

## 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:**
There have been no notifications of information security breaches since the last Information and Privacy Commissioner of Ontario review.

***Indicator:***
*With respect to each information security breach or suspected information security breach:*

- *The date that the notification was received,*
- *The extent of the information security breach or suspected information security breach,*
- *The nature and extent of personal health information at issue,*
- *The date that senior management was notified,*
- *The containment measures implemented,*
- *The date(s) that the containment measures were implemented,*
- *The date(s) that notification was provided to the health information custodians or any other organizations,*
- *The date that the investigation was commenced,*
- *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, and*
- *The manner in which each recommendation was addressed or is proposed to be addressed.*

**BORN Response:**
There have been no information security breaches since the last Information and Privacy Commissioner of Ontario review.

BORN had 16 information security incidents:

| Date of Occurrence | Issue | Description | Status |
|---|---|---|---|
| 2019-11-28 | Hardcoded cryptographic key in the FortiGuard services communication protocol | https://fortiguard.com/psirt/FG-IR-18-100 | No systems compromised. No privacy or security breach. Issue Closed – The firewall was patched as per vendor recommendations. |
| 2019-12-17 | Data breach and theft at LifeLabs Genetics | On October 31, 2019, LifeLabs' online booking system was compromised which resulted in a data theft of clients' information including PHI. LifeLabs sends data to the BIS through a secure web service. | No systems compromised. No privacy or security breach. Issue Closed |
| 2020-12-19 | Citrix Vulnerability | A security bulletin for Citrix was issued (https://support.citrix.com/article/CTX267027). An unauthenticated attacker could perform arbitrary code execution and potentially gain access to the CHEO network. | No systems compromised. No privacy or security breach. Issue Closed – CHEO Citrix was patched as per vendor recommendations. |
| 2020-02-19 | BORN PHI Drive accessible remotely | The BORNSAS server can be mapped while logged into VPN. Users can also RDP directly to the server as well through VPN. This was locked when access was restricted to the Citrix client. The lock was mistakenly removed. | No systems compromised. No privacy or security breach. Issue Closed – Lock re-enabled. |
| 2020-08-28 | Temporary passwords logged | When using the Add user to ADB2C function, if you double clicked the add button quickly it would attempt to create the user twice generating an error. This error would record the temporary password in the error table in the database and send to the technical team for troubleshooting. The temporary password was sent in the clear but restricted to BORN staff. | No systems compromised. No privacy or security breach. Issue Closed – Temporary password was excluded from |

| | | | |
|---|---|---|---|
| | | | error logging by the Application Service Provider. |
| 2020-11-18 | SQL Injection attack | A user reported an error message while attempting to login to the BORN Information System. The error indicated that the login page was blocked by the web application firewall (WAF). A critical ticket was raised with iSecurity, BORN's managed service provider to investigate the error. The investigation indicated one of the tracking cookies was generating a Common Vulnerabilities and Exposures (CVE) event. The alert was a false positive by the WAF as the cookie was created by legitimate software of the BORN public website. | No systems compromised. No privacy or security breach. Issue Closed – The alert was a false positive by the WAF as the cookie was created by legitimate software of the BORN public website. |
| 2021-02-01 | Suspected abuse of FTP server | The Canadian Centre for Cyber Security ("Cyber Centre") reported a possible misuse of the BORN FTP server. The FTP server was configured to allow traffic through port 21 over TLS which generated a generic warning from a routine port scan. The error was "This host is running an FTP service, which may be exposed unintentionally to the Internet." | No systems compromised. No privacy or security breach. Closed – As a preventative measure the FTP server was updated to block port 21 as it was not being used. |
| 2021-02-07 | CHEO accounts attacked | On Feb 7, 2021, starting at 2:45 am hackers attacked over 400 CHEO accounts. | No systems compromised. No privacy or security breach. Issue Closed – BORN systems were not compromised. |
| 2021-06-15 | Humber River Ransomware attack | Humber River hospital was hit with a ransomware attack on Monday June 14th at 2am. Code Grey was announced. Kurian Chandy discovered the attack from local news sources on 6/15/21 at 18:00 and informed BORN. | No systems compromised. No privacy or security breach. Issue Closed – BORN systems were not compromised. |

| | | | |
|---|---|---|---|
| 2021-06-29 | KFL&A Public Health cyber security incident | On the morning of Friday, June 25, KFL&A Public Health discovered it was the target of a cyber security incident. The cyber security incident did affect the KFL&A Public Health servers, rendering them inaccessible and resulting in an information technology (IT) outage. | No systems compromised.<br>No privacy or security breach.<br>Closed – BORN systems were not compromised. |
| 2021-07-02 | Microsoft Print Spooler Remote Code Execution Vulnerability | CVE-2021-34527: a remote code execution vulnerability that affects Windows Print Spooler (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527)<br>CVE-2021-1675: a critical Windows print spooler vulnerability that allows for remote code execution (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675) | No systems compromised.<br>No privacy or security breach.<br>Closed – BORN systems were patched as per Microsoft recommendations. |
| 2021-08-13 | Spear Phishing Attempt | Security team at MSP received phishing email from purported BORN agent to ensure agent's credentials were not compromised. Forwarded to CHEO IS for review. Confirmed with user that there was no issue. | No systems compromised.<br>No privacy or security breach.<br>Closed – After review, no BORN systems were compromised. |
| 2021-11-18 | CVE-2021-42306 | Application Credential Exposure: Microsoft recently mitigated an information disclosure issue resulting from the vulnerability disclosed in CVE-2021-42306, which enabled customers and Azure Services to store private key data in clear text in the key Credentials property of an Azure Active Directory (Azure AD) Application and/or Service Principal. | No systems compromised.<br>No privacy or security breach.<br>Closed – BORN systems were patched as per Microsoft recommendations. |
| 2021-12-11 | CVE-2021-44228 | On 10 December 2021, Apache released a Security Advisory [1][2] highlighting a critical remote code execution vulnerability in Log4j, a widely deployed Java-based logging utility. Open-source reporting indicates that active scanning and exploitation of this vulnerability have been observed.<br>An attempt to utilize the exploit was made against a BIS firewall. | No systems compromised.<br>No privacy or security breach.<br>Closed – The firewall does not utilize the compromised code. |

| | | | |
|---|---|---|---|
| 2022-01-27 | Linux security advisory (AV22-042) | On 25 January 2022, several Linux distributions released security updates to address a vulnerability in the following product: PolKit – all versions. | No systems compromised. No privacy or security breach. Closed – BORN systems were patched as per vendor recommendations. |
| 2022-02-14 | Scarborough Health Network security incident | On Friday February 4 BORN was informed in a meeting with Scarborough that they were experiencing a partial code grey. | No systems compromised. No privacy or security breach. Issue Closed – BORN systems were not compromised. |
| 2022-03-09 | IP Blocking Recommendation | An increased prevalence in outbound traffic attempts to the suspicious IP 139.45.197.253. There was no direct evidence of malicious activity by this host, it is classified as a multi-content hosting IP by IBM X-Force that was previously threat listed for hosting several iterations of spyware known as Omnatuor. | No systems compromised. No privacy or security breach. Closed – As a preventative measure the IP address was blocked. |
| 2022-06-22 | IP Blocking Recommendation | The security team at the BORN MSP observed notable increases in outbound traffic attempts from endpoints in monitored environments to this suspicious host. As a precaution we have blocked traffic to or from 72.21.81.200 in all external facing firewalls. | No systems compromised. No privacy or security breach. Closed – As a preventative measure the IP address was blocked. |

# 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:**

- 59 agents have received initial privacy orientation since the last review. This number includes those agents who no longer work for BORN.
- All agents received privacy training; there are no agents awaiting initial 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:**
*2019-20 ongoing organizational privacy training*

- There were 92 BORN agents in 2019-20:
    - 70 agents attended organizational privacy training
    - 22 agents did not attend organizational privacy training in person. Of these 22 agents:
        - 11 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 presentation via email to review and they all confirmed by email that they read and fully understood the contents of the presentation. While all CHEO Agents, including these IS employees, receive CHEO privacy training every two years, they also receive separate BORN-specific privacy training annually.
        - 9 agents left BORN before the annual ongoing security training session was conducted
        - 2 agents were on maternity leave at the time the ongoing privacy training session was presented. For individuals who are on leave at the time of the annual BORN privacy training, an opportunity is provided upon their return from leave, and this completion is logged by the BORN Privacy Office.

*2020-21 ongoing organizational privacy training*:

- There were 104 BORN agents in 2020-21:
    - 67 agents attended ongoing organizational privacy training

- 37 agents did not attend ongoing organizational privacy training. Of these 37 agents:
  - 12 agents did not attend annual privacy training at the time that it was presented, 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. While all CHEO Agents, including these IS employees, receive CHEO privacy training every two years, they also receive separate BORN-specific privacy training annually.
  - 11 agents left BORN before the annual ongoing privacy training session was conducted
  - 2 agents were on maternity leave at the time the ongoing privacy training session was presented. For individuals who are on leave at the time of the annual BORN privacy training, an opportunity is provided upon their return from leave, and this completion is logged by the BORN Privacy Office.

*2021-22 ongoing organizational privacy training*:

- Ongoing privacy organizational training occurred on October 20, 2022.

***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:**

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

| No. | **Date** | **Description of Communication** |
|---|---|---|
| 1 | 27-Jan-20 | Privacy Officer sent email to all BORN Staff - Privacy Day 2020 - Message from the Commissioner |
| 2 | 25-Mar-20 | Email to all staff regarding working from home and a link to a video on KnowBe4's Home Course |
| 3 | 06-May-20 | Email sent to staff regarding previous day email sent by security officer with a simulated phishing attacks advising that simulated attacks will be run from time to time |
| 4 | 01-Jun-20 | Email to all staff with a copy of the updated approved Privacy and Security Management Plan 3.0 along with a summary of changes |
| 5 | 15-Oct-20 | Delivery of annual ongoing Privacy Training (Privacy Officer)<br>Delivery of annual ongoing Security Training (Information Security Officer) to all BORN Staff at annual team meeting |

| | | |
|---|---|---|
| 6 | 19-Oct-20 | Email to all BORN staff regarding the use of MFA for all remote access to Citrix - user guide and instructions on process |
| 7 | 28-Oct-20 | Email to all staff regarding BORN being subject to 2 targeted phishing attacks that week. Reminders on how to deal with this type of attack. |
| 8 | 10-Nov-20 | Email to all staff regarding the tri-annual review process with Information and Privacy Commissioner of Ontario completed on Oct 31/20 - advised that an update to the P&SMP was now available and provided link - also attached a summary of the changes |
| 9 | 11-Mar-21 | Email to all staff with link to a video on tips and cautions with upcoming tax season approaching and how to avoid scammers etc. |
| 10 | 13-Aug-21 | Email sent to all staff regarding a warning received from The Security Operation Center at iSecurity that detected an active phishing campaign coming from Health Unit. Instructions on how to address |
| 11 | 06-Oct-21 | Delivery of Ongoing Security training to all BORN Staff at the Oct 6/22 BORN monthly Team meeting |
| 12 | 07-Oct-21 | Email sent to all staff regarding tips on how to spot SMiShing and Vishing emails and how to address |
| 13 | 12-Oct-21 | Email sent to all staff regarding Cybersecurity Tips for Business email compromises and tips on how to navigate the process |
| 14 | 14-Oct-21 | Email sent to all staff regarding working from home tips |
| 15 | 18-Oct-21 | Email sent to all staff regarding tips on how to deal with spam and phishing attach |
| 16 | 19-Oct-21 | Cybersecurity update on Working from home sent to all staff - invitation to staff living in the Ottawa area to bring laptop in the CHEO for a tune-up. A remote solution for those living outside the Ottawa area will be forthcoming |
| 17 | 21-Oct-21 | Delivery of Ongoing Privacy training to all BORN Staff at annual BORN Team meeting |
| 18 | 25-Oct-21 | Email to all staff with how to deal with a malicious cyber attach - tips on what to look for etc. |
| 19 | 29-Oct-21 | Email to all staff regarding Cybersecurity Tips - Knowledge is best defence |
| 20 | 12-Nov-21 | Email to all BORN staff regarding the migration of mailboxes on Exchange server to the Azure Exchange server - timeline and instructions on what this means |
| 21 | 19-Nov-21 | Email to all staff regarding migration to 365 - instructions, tips etc. |
| 22 | 23-Nov-21 | Follow up email sent regarding migration to 365 - further instructions to troubleshoot issues |
| 23 | 01-Dec-21 | Email to all staff regarding an invitation to watch a video on how to keep cyber secure during the holidays |

| | | |
|---|---|---|
| 24 | 08-Feb-22 | Email sent to all staff regarding Safer Interne Day from cyberbullying to social networking to digital identity - this was from the Canadian Centre for Child Protection who urge parents to regularly check in with their children |
| 25 | 17-Feb-22 | Email sent to all staff regarding the migration of hosting provider system for the BORN Website - |
| 26 | 28-Feb-22 | Cybersecurity Alert regarding a recent license Scam. Security officer alerted all staff to an example of a smishing attack involving license plate sticker refunds - tips on what to avoid |
| 27 | 05-May-22 | Email sent to all staff regarding World Password Day - tips on creating strong passwords |
| 28 | 18-May-22 | Privacy Officer sent email to all BORN Staff with *Commissioner's Blog - Ripe for public debate: Legal and ethical issues around de-identified data* encouraging all staff to review |
| 29 | 22-Jun-22 | Email sent to all staff regarding connecting to CHEO remotely to commonly accessed file shares without the need to go through Citrix - instructions to staff on how to apply this function |
| 30 | July 22, 2022 | Communication to all BORN staff providing the revised Privacy and Security Management Plan version 3.1 and along with a high-level summary of the changes. |

## 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:**

- 59 agents have received initial security orientation since the prior review by the Information and Privacy Commission of Ontario. 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:**
*2019-20 ongoing organizational security training*

- There were 92 BORN agents in 2019-20:
    - 70 agents attended annual ongoing organizational security training.
    - 22 agents did not attend organizational security training in person. Of these 22 agents:
        - 11 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 security presentation via email to review and confirmed that they read and understood the contents of the presentation;
        - 9 agents left BORN before the annual ongoing security training session was conducted; and
        - 2 agents were on maternity leave at the time the ongoing security training session was presented.

*2020-21 ongoing organizational security training*:

- There were 104 BORN agents in 2020-21:
    - 66 agents attended organizational security training.
    - 38 agents did not attend organizational security training. Of these 38 agents:
        - 12 agents did not attend annual 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 were provided with a copy of the security presentation via email and each confirmed by email that they read and understood the contents of the presentation;
        - 11 agents left BORN before the privacy and security training session was conducted;
        - 1 agent was hired after the annual ongoing security training session was conducted but received initial security training at the commencement of their employment; and
        - 2 agents were on maternity leave at the time the ongoing security training session was presented.

*2021-22 ongoing organizational security training*:

- Ongoing security training has been scheduled to take place on October 20, 2022.

## 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 BORN 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.

- 2019-2020: There were 92 agents during the period and all re-acknowledged their Confidentiality Agreement pledge via email.
- 2020-2021: There were 104 agents during the period. Of the 104 agents, 100 agents re-acknowledged their Confidentiality Agreement pledge via email, 3 agents left BORN before the annual renewal of confidentiality was required and 1 was on leave during the period.
- 2021-2022: There were 108 BORN Agents during the period. Of the 108 agents, 96 agents re-acknowledged their Confidentiality Agreement pledge via email, 2 agents were on maternity leave, 1 agent left BORN shortly after the annual renewal of Confidentiality Agreement process began; 7 left BORN before the annual renewal of confidentiality was required, 1 agent returned from maternity leave in early July and has not yet re-acknowledged their Confidentiality Agreement (this agent will not have access to PHI); 1 agent, who was a casual employee with no access to PHI, resigned on July 30, 2022.

***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*:***
As noted above, as of August 1, 2022, 1 agent had yet to renew their Confidentiality Agreement, and did not have access to any PHI.

| | Agent 1 |
|---|---|
| Date of commencement of employment | October 9, 2018 |
| Date by which the Confidentiality Agreement must be executed | August 8, 2022 |

## 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:**
Twenty-four (24) termination notices were received from BORN agents who terminated their employment with BORN Ontario since the prior review.

Five (5) contract employees reached the end of their contract. No notices are received with respect to their termination as their end date is known.

## 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:**

January 2020
February 2020
April 2020
July 2020
September 2020
October 2020
November 2020
February 2021
March 2021
April 2021
May 2021
June 2021
August 2021
September 2021
October 2021
November 2021
December 2021
January 2022
February 2022
March 2022
April 2022
May 2022
June 2022
July 2022

***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:**
Privacy and information security risks and recommendations were discussed by the Information Security Officer and the Privacy Officer prior to and in preparation for review at monthly meetings of the PSRC.

PSRC meetings at which risks were discussed and/or amended:

- January 2020
    - Risk and mitigations discussed and documented pertaining to update to desktop and application visualization software to address vulnerability.
- February 2020

    - Updated BORN Information System end user terms to address risks.
- April 2020
    - Risks and mitigation discussed and documented pertaining to penetration test results.
    - Risks mitigated through revisions to Privacy and Security Management Plan.
- July 2020
    - Risks and mitigation discussed and documented pertaining to disaster recovery.
    - Risks and mitigation discussed and documented pertaining to the COVID data from MOH.
    - Risks and mitigation discussed and documented pertaining to agents working from home.
- September 2020
    - Risks and mitigation discussed and documented pertaining to disaster recovery.
    - Risks and mitigation discussed and documented pertaining to temporary passwords.
- October 2020
    - Risks and mitigation discussed and documented pertaining to written acknowledgements.
    - Risks and mitigation discussed and documented pertaining to security training and onboarding of new agents.
- November 2020
    - Risks and mitigation discussed and documented pertaining to service provider agreements.
    - Risk and mitigation discussed and documented pertaining to security operations centre.
- February 2021
    - Risks and mitigation discussed and documented pertaining to agent knowledge of privacy and security management plan components.
    - Risks and mitigation discussed and documented pertaining to data warehouse.
- March 2021
    - Risks and mitigation discussed and documented pertaining to waiver of consent for research.
    - Risks and mitigation discussed and documented pertaining to changes in cloud service/product roadmap.
    - Risks and mitigation discussed and documented pertaining to remote agent access.
- April 2021
    - Risks and mitigation discussed and documented pertaining to agents working from home.
- May 2021
    - New format for risk log and log of recommendations discussed.

*(note- new format for risk log and log of recommendations created)*

- June 2021
    - Risk entered pertaining to contract matter.
    - Risk entered pertaining to end point security.
- August 2021
    - Risk entered pertaining to changes in encryption technology.
    - Risk entered pertaining to audit and review.

    - Risk entered pertaining to inadvertent email use instead of BIS messaging related to pandemic.
    - Risk entered pertaining to extended support.
    - Risk entered pertaining ticketing system.
- September 2021
    - Risk entered pertaining to network vulnerability.
    - Risk entered regarding the use of generic accounts.
- October 2021
    - Risk pertaining to a software upgrade.
    - Risk pertaining to public website protocols.
    - Risks pertaining to contract matter, end point security, ticketing systems all closed.
- November 2021
    - Risk pertaining to need to update contract.
    - Risks from PIA entered.
    - Risk entered pertaining to network vulnerability closed.
- December 2021
    - Updates on status entered.
    - Risk entered related to data entry errors.
    - Risk entered pertaining to the upgrade of firewalls.
    - Risk entered pertaining to a Security Advisory highlighting a critical remote code.
- January 2022
    - Updates on status entered.
    - Risk pertaining to a software upgrade closed.
- February 2022
    - Risks entered pertaining to review.
    - Updates on status entered.
    - Risk entered pertaining to the upgrade of firewalls closed.
- March 2022
    - Updates on status entered.
- April 2022
    - Updates on status entered.
- May 2022
    - Updates on status entered.
    - Risk pertaining to public website protocols closed.
    - Risk entered pertaining to a Security Advisory highlighting a critical remote code closed.
- June 2022
    - Updates on status entered.
    - Risk entered related to data entry errors closed.
- July 2022
    - Updates on status entered.
    - Risk pertaining to changes in encryption technology, audit and review, and PIA closed.
    - Risk pertaining to scope of third-party audit entered.

## 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:**

| | |
|---|---|
| June 1, 2020 | Data backup recovery test |
| September 10, 2020 | Data backup recovery test |
| May 5, 2021 | Data backup recovery test |
| September 25-27, 2021 | Full disaster recovery test including fail-over to secondary site |
| December 1, 2021 | Data backup recovery test |

***Indicator:***

*Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made*.

**BORN Response:**

No amendments were made.