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

The purpose of this policy is to ensure that BORN has a privacy and security accountability framework to implement its status and overall responsibility as a prescribed person under PHIPA.

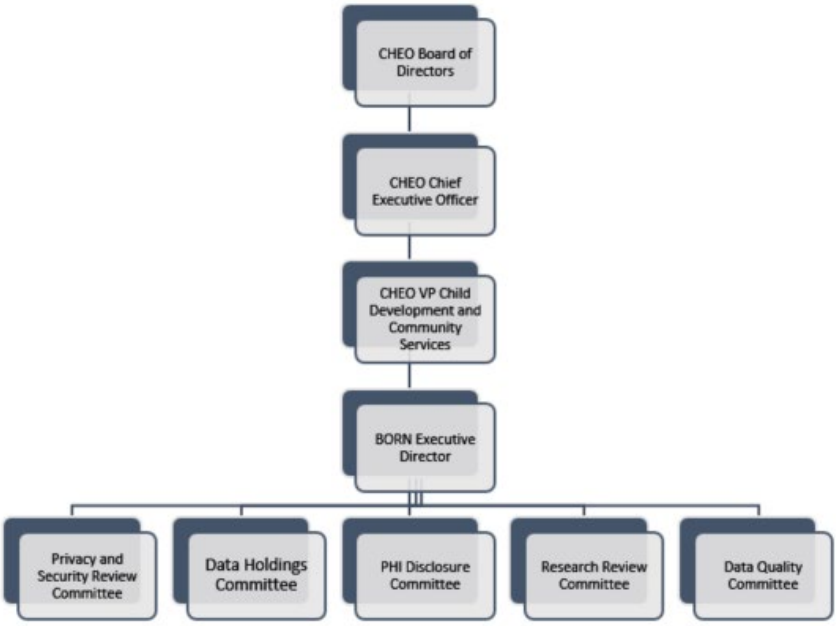

Figure 1: Accountability Structure

Status of Prescribed Registry

The Children's Hospital of Eastern Ontario (CHEO) is a prescribed person in respect of BORN as provided for in section 13(1) of Ontario Regulation 329/04-General (Regulation), enacted under PHIPA for the purposes of facilitating or improving the provision of Health Care for mothers, infants, and children.

Section 13(2) of Ontario Regulation 329/04-General (Regulation) requires BORN, as a prescribed registry, to:

- Have in place practices and procedures to protect the privacy of individuals whose Personal Health Information BORN receives
- Maintain the confidentiality of that information
- Have its practices and procedures approved by the Information and Privacy Commissioner of Ontario every three years

BORN is committed to complying with the provisions and regulations of PHIPA applicable to a person holding a registry, as well as any other applicable legislation.

Privacy and Security Accountability Framework

BORN has developed comprehensive privacy and security policies and procedures to ensure compliance with PHIPA and its regulation.

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

Privacy and Security Review Committee (PSRC)

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

Data Holdings Committee (DHC)

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

PHI Disclosure Committee (PDC)

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

Research Review Committee (RRC)

The RRC is responsible for reviewing, approving and/or denying requests for the use of Personal Health Information for research purposes. The RRC is responsible for reviewing requests for the

disclosure of Personal Health Information for research purposes which are ultimately referred to the PHI Disclosure Committee for approval.

Data Quality Committee (DQC)
BORN is an authoritative source of accurate, trusted, and timely data used to monitor, evaluate, and plan for the best possible beginnings for lifelong health. The purpose of the DQC is to facilitate the implementation and refinement of BORN's data quality framework, including overseeing and assessing the quality of BORN's data and developing and implementing plans, processes and tools to enhance data quality.

Additional Roles and Responsibilities
The Executive Director has delegated responsibility for:

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

The Privacy Officer, Information Security Officer and the Data Request and Research Coordinator(s) can delegate work to other BORN employees.

The duties and responsibilities of the Privacy Officer focus on developing and maintaining a strong culture of privacy at BORN and include:

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

The duties and responsibilities of the Information Security Officer include managing the security program as follows:

- Management of the security program, including monitoring compliance, conducting regular audits and providing reports to senior management and recommendations for changes to policy or procedures

- Execution of security training
- Execution and oversight of threat and risk assessments
- Execution and oversight of vulnerability assessments
- Any and all related security oversight
- Responsibility for the technology used to collect and securely store the Personal Heath Information used by BORN

The Data Request and Research Coordinators have responsibility for coordinating the review of all use and disclosure requests with the PHI Disclosure Committee and/or the Research Review Committee to ensure that they comply with the requirements of PHIPA and its regulation. The Data Request and Research Coordinators are also responsible for ensuring that De-identification is conducted in accordance with this Plan.

Collection of Personal Health Information

BORN collects Personal Health Information for the purpose of facilitating or improving the provision of Health Care in compliance with s. 39(1)(c) of PHIPA.

The types of Personal Health Information collected include demographic information (e.g. age, postal code) and clinical information about fetuses, newborn babies, children and their mothers (including pregnancy history, medical history and a summary of care provided during pregnancy, labour, birth and the newborn and early childhood periods).

This information is collected from health information custodians involved in the care of children, newborns and their mothers.

BORN ensures that the collection of Personal Health Information is consistent with PHIPA and its regulation. BORN does not collect Personal Health Information if other information will serve the purpose and does not collect more Personal Health Information than is reasonably necessary to meet the purposes outlined above.

BORN collects only those data elements that have been identified through the rigorous review process undertaken by the Data Holdings Committee. As described in this Plan, the Data Holdings Committee has been delegated responsibility for:

- Reviewing new proposed BORN data holdings
- Reviewing new statements of purpose that may improve or facilitate the provision of Health Care

- Reviewing BORN's existing data holdings to ensure their statements of purpose are still relevant and necessary for the identified purposes including: the purpose of the data holding, the PHI contained in the data holding, the source(s) of the PHI, and the need for PHI in relation to the identified purpose

Use of Personal Health Information

BORN uses the Personal Health Information that it collects for the purposes of facilitating or improving the provision of Health Care. Such activities may encompass:

- Identifying where appropriate care has not been received and facilitate access to care and treatment for mothers, infants and children (e.g. identifying false negative screens and informing the relevant Health Care provider in order to enable them to offer parents appropriate care for their baby)
- Facilitating continuous improvement of screening thresholds to minimize missed cases
- Raising alerts where maternal and/or newborn outcomes are clinically or statistically discrepant with accepted norms
- Enabling Health Care providers to improve care by providing them the information and tools to compare themselves with peers and/or benchmarks
- Identifying strategies to improve the quality and efficiency of care for mothers, infants and children
- Creation of reports that can be used to provide the Ministry of Health and Long-Term Care, and Public Heath Units with comprehensive and timely information to support effective planning and management of Health Care delivery for mothers, babies and children in the province

Information provided in reports to the Ministry of Health, and Public Health Units does not contain Personal Health Information or identify individuals; they present an overview of aggregated Health Care data. The reports are carefully reviewed to ensure there is no risk of re-identification through small cell counts or other forms of possible residual disclosure as per p.24: De-identification and Aggregation. The reports are made available through the BORN website at www.BORNOntario.ca.

BORN ensures that each identified use of Personal Health Information is consistent with the uses of Personal Health Information permitted by the Act and its regulations. BORN does not use Personal Health Information if other information will reasonably serve the purpose and

does not use more Personal Health Information than is reasonably necessary to meet the purpose, using de-identified or aggregate information wherever possible.

BORN may use Personal Health Information to conduct Research only when the strict requirements of PHIPA are adhered to, including review by a Research Ethics Board as per p.10: Use of Personal Health Information for Research.

BORN remains responsible for Personal Health Information used by its Agents. Access and use by Agents is strictly controlled. Agents are trained on their privacy obligations and sign a Confidentiality Agreement acknowledging the requirements to use only the information necessary for their work, to keep Personal Health Information secure at all times, and to notify BORN of any discovered or suspected breach as per:

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

Disclosure of Personal Health Information

The PHI Disclosure Committee has responsibility for reviewing all requests for disclosure of Personal Health Information.

The Research Review Committee has responsibility for reviewing all requests for use of Personal Health Information for Research (including use of Personal Health Information for Research for subsequent disclosure of record level data that has undergone De-identification prior to such disclosure).

In cases involving disclosure of Personal Health Information for Research that has not undergone De-identification (including De-identification through aggregation) prior to disclosure (if any), the Research Review Committee will review requests and then refer the matter with its recommendations to the PHI Disclosure Committee for consideration and possible approval.

BORN does not disclose Personal Health Information if other information serves the purpose and does not disclose more Personal Health Information than is reasonably necessary to meet the purpose.

Personal Health Information is disclosed to the following groups and for the following purposes, in accordance with the disclosures of Personal Health Information permitted by PHIPA and its regulation:

- To health information custodians, when facilitating access for mothers, babies and children for care and treatment; for example, to ensure appropriate screening is offered in a meaningful timeframe;
- To a prescribed entity for the management, evaluation, monitoring or planning for the health system
- To Researchers for Research purposes as defined in PHIPA. Personal Health Information is provided to Researchers only if de-identified information is not sufficient to conduct the Research. The research plan must be approved by a Research Ethics Board, meet the requirements set out in PHIPA, and be approved by the Data Request and Research Coordinator who ensures that the minimum amount of Personal Health Information and the least identifiable information is disclosed

More information on the disclosure of Personal Health Information is provided in:

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

Disclosure of De-identified and/or Aggregate Personal Health Information

The Data Request and Research Coordinator has responsibility for reviewing all De-identified and/or aggregate information prior to its disclosure in order to ensure that it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual. The Data Request and Research Coordinator is assisted by the user of the De-Identification Tools for empirical assessment regarding risk of re-identification.

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

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

- Ministry of Health to inform policy and planning

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

BORN prohibits paper records of personal health information.

BORN ensures that electronic records are kept safe and secure as follows:

- Electronic records of personal health information are securely retained in identifiable format within the transactional database for 28 years after which they are converted to a de-identified format and then securely destroyed. Secure retention, timeline, and secure destruction are detailed in:
    - **S-05: Secure Retention of Records of Personal Health Information**
    - **S-08: Secure Disposal of Records of Personal Health Information**
- Electronic records of Personal Health Information are securely transferred and disposed of as per:
    - **S-07: Secure Transfer of Records of Personal Health Information**, and
    - **S-08: Secure Disposal of Records of Personal Health Information**

Implementation of Administrative, Technical and Physical Safeguards

BORN has in place administrative, technical and physical safeguards to protect the privacy of individuals whose Personal Health Information is received and to maintain the confidentiality of that information. BORN takes steps to protect Personal Health Information against theft, loss and unauthorized use or disclosure and to protect records of Personal Health Information against unauthorized copying, modification or disposal. These safeguards are set out in:

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

Privacy and security policies and procedures are reviewed at least once prior to each scheduled review by the IPC pursuant to subsection 13(2) of the Regulation under the Act by the Privacy and Security Review Committee as per S-02: Ongoing Review of Security Policies and Procedures.

Inquiries, Concerns or Complaints Related to Information Practices

All inquiries, concerns or complaints related to the privacy policies and procedures of BORN and BORN's compliance with PHIPA and its regulation must be directed to:

Privacy Officer
CHEO
Centre for Practice Changing Research building
401 Smyth Road
Ottawa ON K1H 8L1
Email: privacy@BORNOntario.ca

See the BORN website at www.BORNOntario.ca

Individuals may also direct complaints regarding the compliance of BORN to the Information and Privacy Commissioner of Ontario:

Information and Privacy Commissioner of Ontario
2 Bloor Street East
Suite 1400
Toronto, ON M4W 1A8

Telephone:
Toronto Area: 416-326-3333
Toll Free (within Ontario): 1-800-387-0073
TDD/TTY: 416-325-7539
Fax: 416-325-9195

Transparency of Practices in Respect of Personal Health Information

BORN Ontario makes its privacy policies available on the BORN website at www.bornontario.ca, including **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person** and the Statement of Information Practice. The privacy policies can also be obtained by contacting the Privacy Officer as per above.

Compliance Audit and Enforcement

BORN Ontario Agents must comply with this Plan. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with **P-27: Privacy Audits** and **S-15: Security Audits**.

BORN Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with **P-29: Privacy Breach Management** or **S-17: Security Breach Management**, as applicable. Consequences of breach are detailed in each respective breach policy as well as in **P-01: Privacy Policy in Respect of CHEO's Status as a Prescribed Person**. **HR-11: Discipline and Corrective Action** which clarifies:

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

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