born Ontario

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

Privacy and Security Management Plan

July 2011 v 1.8

Table of Contents

Glossary

Term	Definition
Agent	A Children's Hospital of Eastern Ontario (CHEO) employee or consultant, contractor or seconded employee to BORN Ontario, who has authority to provide services to or on behalf of BORN Ontario. Formal relationship, completed privacy and security training and a signed Confidentiality Agreement are required before operating as a BORN Agent. For further certainty, for the purposes of these policies and procedures, the BORN Hosting Provider is an Agent of BORN.
BORN Coordinators	BORN Agents support high quality data collection and use from health information custodians providing data to BORN Ontario. BORN Coordinators are situated across the province.
BORN Ontario	The Better Outcomes Registry and Network of Ontario. Under its legacy name of Ontario Perinatal Surveillance System (OPSS), as a part of CHEO, it is recognized in regulations as a registry of Personal Health Information, as per paragraph 39(1)(c) of the Ontario *Personal Health Information Protection Act, 2004.*
BORN System Administrator	BORN System Administrator is the BORN Agent in charge of managing the administration of the BORN Data Collection System. Responsibilities include management of the application code, database and users of the system.
CEO	Chief Executive Officer
CHEO	Children's Hospital of Eastern Ontario
Data Dictionary	For each data element in the BORN System, the Data Dictionary contains a definition of the data element and a list of its parameters.
Data Dictionary Review Committee	The BORN Ontario Committee responsible for reviewing and approving the data collected by the BORN Ontario System. Committee members are: • Scientific Manager • Quality Management Specialist • A BORN Coordinator

Term	Definition
Data Sharing Agreement	A data sharing agreement with participating organizations that sets out the rights and responsibilities of the organization and BORN Ontario with regard to Personal Health Information.
Director	The Operations Director of BORN Ontario.
Disclosure of Personal Health Information Review Committee	The BORN Ontario Committee responsible for reviewing, approving and/or denying requests for Personal Health Information for research purposes or disclosures to prescribed entities. Committee members are: • Scientific Manager • Scientific Director • A BORN Coordinator • A member from the CHEO Electronic Health Information Laboratory
Hosting Provider	The organization responsible for hosting the servers which contain the application code and database leveraged by BORN Ontario for collection, use and disclosure of the Registry information.
Leadership Team	The Leadership Team has delegated responsibility for the BORN Ontario registry. Members of the BORN Ontario Leadership Team are: • BORN Ontario Medical Director • Scientific Director • Operations Director • CHEO Vice President
Legacy System Hosting Provider	Rincon Technologies Incorporated.
LHIN	Local Health Integration Networks are not-for-profit organizations across the province of Ontario that plan, fund and integrate health care services locally. There are 14 LHIN regions across Ontario. See www.lhins.on.ca
Manager of Health Informatics	The BORN Agent responsible for the technology of BORN Ontario.
Mobile Computing Equipment	Includes laptops, Universal Serial Bus (USB) flash drives, external hard drives, CDs, DVDs and other authorized mobile and mass storage devices.

Term	Definition
OPSS	Ontario Perinatal Surveillance System (BORN was formerly operational as OPSS)
Personal Health Information	Personal Health Information refers to identifying information about an individual (living or deceased) whether in oral or recorded form, where identifying information is information that could be used, either alone, or by linking with other information, to identify the individual to whom the information relates (definitive definition contained in section 4 of the *Personal Health Information Protection Act, 2004*).
PHIPA	*Personal Health Information Protection Act, 2004* is Ontario's health-specific privacy legislation. It governs the manner in which Personal Health Information may be collected, used and disclosed within the health care system.
Policy	A written statement that clearly indicates the position and values of the organization or organizational unit on a given subject.
Privacy Officer	The BORN Agent responsible for privacy and security of Personal Health Information.
Privacy and Security Review Committee	The BORN Ontario committee responsible for reviewing and approving activities related to the BORN Ontario Privacy and Security Management Program. Committee members are: • CHEO Chief Privacy Officer • Manager of Health Informatics • Scientific Manager
Requestor	An individual requesting data for purposes other than research.
Research	As per section 2 of the *Personal Health Information Protection Act, 2004*, a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research.
Research Ethics Board	As per section 2 of the *Personal Health Information Protection Act, 2004*, a Board of persons that is established for the purpose of approving research plans under section 44 and that meets the prescribed

Term	Definition
	requirements.
Scientific Manager	The BORN Agent responsible for: • Scientific analysis of BORN Ontario information • Review of requests for disclosure of Personal Health Information for research purposes
Third Party Service Provider	An individual or organization engaged by BORN Ontario to provide a service which may involve work associated with BORN data. An example is Dapasoft, the software development company engaged to develop the software required by BORN to meet its purposes.

Introduction

BORN Ontario is a prescribed Registry with a vision for the best possible beginnings for lifelong health.

By bringing together timely, high-quality clinical maternal-child health information into an authoritative data set, BORN Ontario works to ensure the mothers and children of Ontario are offered the best possible care. From 2011 – 2014, BORN Ontario will meet its vision through a number of initiatives:

Facilitating Care to Mothers

1. **Gestational diabetes screening reminder**. Mothers testing positive for gestational diabetes require follow-up as they are at increased risk for Type 2 diabetes and its many resultant complications later in life. The Registry can gather the gestational diabetic status from any of a number of antenatal providers (family doctor, midwife, obstetrician, birthing hospital) and then alert the primary care physician to ensure appropriate follow-up care is offered.
2. **Improving Screening Algorithms**. Screening is a mechanism to assess and report risk and as such, involves false-positive and false-negative results. While this is expected, the anxiety for families upon receiving a positive screen is significant and the impact on individuals with a false negative result can be catastrophic. By gathering all screening results and all associated follow-up and outcome information, trained analysts can review the information to identify triggers for the false results. Once analyzed, the screening thresholds can be adjusted to reduce false-positive and false-negative results. The costs of false negative can be significant – from lifelong disability to potential death. Reduction in the false positives will reduce the number of families impacted by the anxiety associated with a positive result.
3. **Antenatal 1 and 2 Forms**. Complete pregnancy history and documentation of care is tracked across providers using the provincially mandated Antenatal 1 and Antenatal 2 forms. These forms should be sent to the birthing hospital at 35 weeks' gestation. A survey by BORN Ontario suggests that women frequently deliver without their providers having access to this information – either they deliver unexpectedly, early, or the forms cannot be located. Providing access to these forms in emergent situations will ensure that providers have key clinical information available and also reduces the duplication of tests used to facilitate care (ultrasounds and laboratory).

Facilitating Care to Babies

1. **Missed Screens**. Newborn Screening Ontario tests for 28 rare diseases in newborns. Test results can lead to early identification and proper, life-saving treatment. By capturing every birth in the province and then cross-referencing to every baby tested by Newborn Screening Ontario, BORN Ontario can promptly identify the babies that have not been tested and inform the primary care provider to ensure the test is offered.
2. **Being born in the right place at the right time**. Newborns from high-risk pregnancies do best when they are born in the centre best equipped to handle their complex needs (e.g. being born in the best possible place at the right time). For example, if neonatal surgery is required, delivering at a hospital that can provide that care is critical to the best possible outcome for the baby. Hospitals across the province have specific levels

of care they can provide. Ensuring they are appropriately accepting or diverting patients is key to improving outcomes for this vulnerable population.

Supporting Individual Providers

1. **NTQA.** Nuchal translucency (NT), a measurement on the neck of the fetus during ultrasound, is a key component in the prenatal screening algorithm. With values smaller than a millimetre being an important differentiation, it is critical that sonographers measure it accurately. Much work has been done internationally on quality assurance of NT measurements that involve plotting all measurements done by a single sonographer and comparing the distribution to accepted norms. BORN Ontario is able to collect these key measurements from labs across the province and report back to sonographers and their managers on the quality of their work. By minimizing errors in NT measurements, prenatal screening results will be much more accurate, reducing false positives and false negatives and the associated repeat tests and analysis.
2. **Discrepant Practice**. Evidence associated with labour, birth and newborn care in the province shows significant variation in key indicators such as caesarean section rates and other labour interventions. Tracking, reporting and addressing these variations will ensure women in the province are offered consistent, high-quality and appropriate care. Once data are available, BORN coordinators will work with the hospital or individual provider to understand why their rates are discrepant and to develop and implement quality improvement strategies.
3. **Midwifery Billing.** In order to be the authoritative source for births in the province of Ontario, midwifery information must be combined with hospital birth information. Timely, high-quality data collection is supported by having the data entry linked to payment. The Ministry of Health and Long Term Care has asked that BORN Ontario collect, on their behalf, both clinical and administrative data elements associated with the billing agreement between the Ministry of Health and the Ontario midwifery community.

Informing Provider Organizations

1. **Access to Aggregate data**. Health care providers collect key clinical information for an individual as part of every visit such as the clinical details associated with labour, including the indications for interventions, the timing of the labour, the medications and analgesia administered and final outcome for mother and baby. It is only when this data are aggregated that the information highlights important trends in the care being provided, for example, many women having emergency c-sections, many women being induced rather than labour starting spontaneously. Providers are willing to invest the time required to enter the information into the BORN Ontario system because it provides them great value for program planning and management of care to analyse their data in aggregate.
2. **Benchmarks and Key Performance Indicators**. The aggregate information does allow for analysis of one's own information. That same information becomes much more meaningful when compared to one's peers through the use of Benchmarks or when compared to Key Performance Indicators with organizational targets. With 100% of hospitals and midwives providing data to BORN Ontario, we are well positioned to facilitate access to key benchmarks by geography and level of care for care providers across the province.

Informing the System

1. **Unexplained poor outcomes, such as increased anomalies**. As an authoritative source of maternal-child health outcomes information, BORN Ontario is the only organization in the province with timely access to health trends in the population. Previously, a cluster of congenital anomalies was suspected in south-western Ontario. It was through detailed analysis of the data entry, outcomes, risk factors and interventions that the signal was found to be in error.
2. **Reports.** The Ontario health care system is dependent on high-quality information for decision making. Public Health Units and LHINs regularly request reports from the BORN founding members to plan the delivery of services in their region. Using aggregate information from the BORN System, we can inform regions and populations of key trends that need to be addressed.
3. **Effectiveness.** Providing feedback to public health units and health promotion agencies on the effects of their campaigns around smoking cessation, breastfeeding promotion, prenatal class attendance and the relationships between these and newborn and childhood outcomes will help improve the care provided to mothers and children.
4. **Determinants of Health**. Providing health policy makers with information on the determinants of health (through collection of demographic information) and outcomes will help create the knowledge of how these factors affect health status of mothers, infants and children.

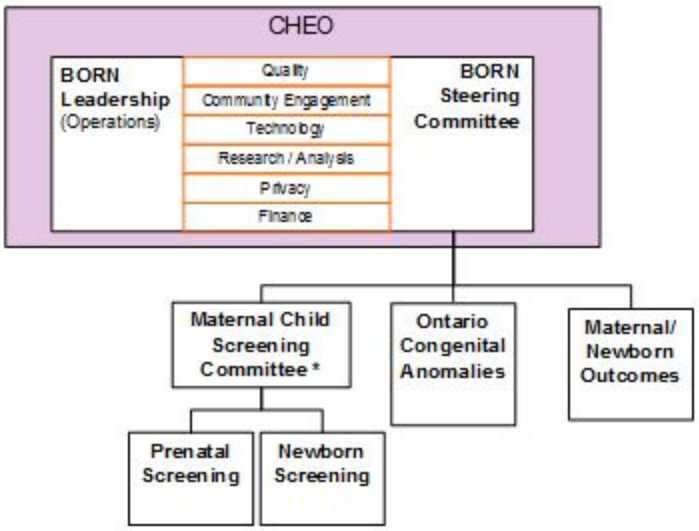
Every data element collected by the BORN System is required to meet these deliverables. The model by which the decision was made to include these data elements is based on the following equation:

Identifiers + Health Status + Health Risk Factors + Care Provided = Health Outcomes

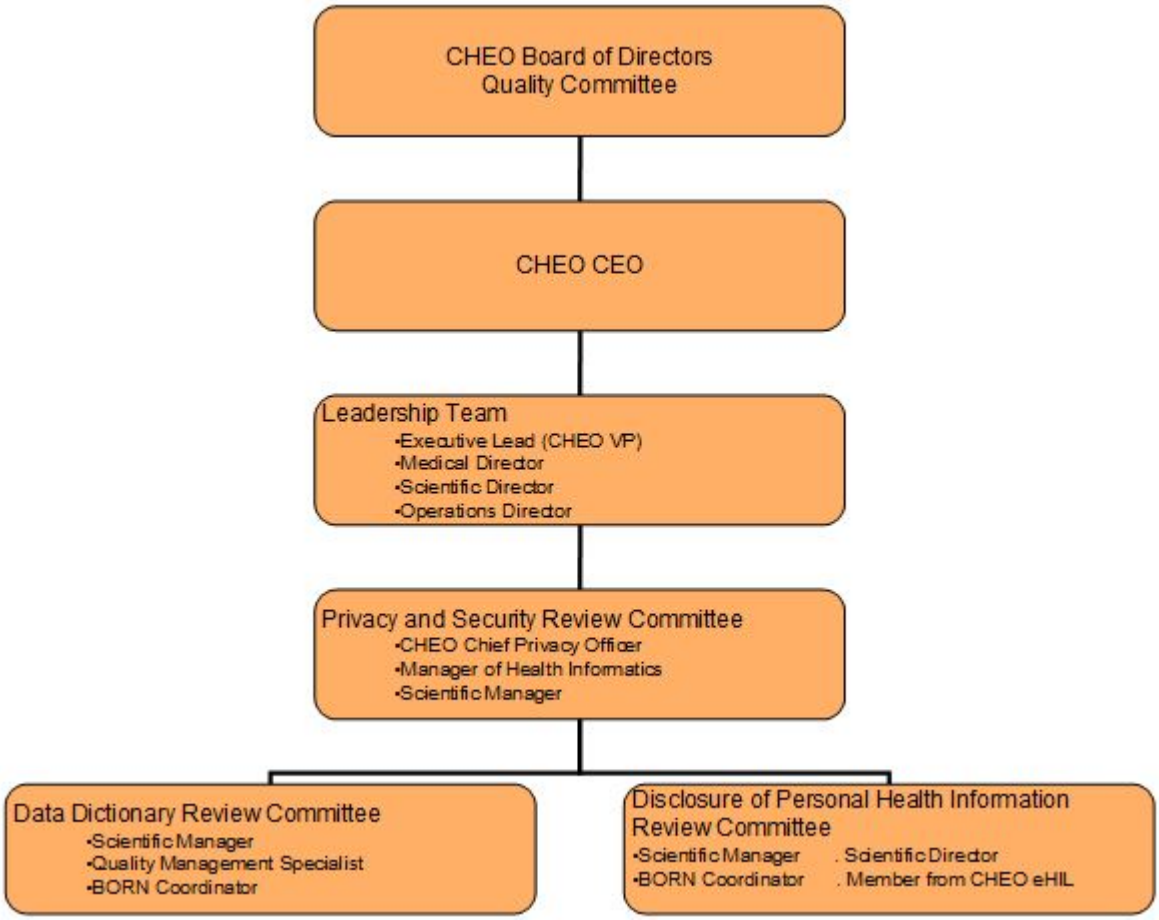
Without high-quality information in each of these categories, BORN Ontario is not able to address the purposes defined above. It is the clinical data included in the system that provides the authoritative information and context required to make the decisions and conclusions of the Registry. To illustrate, we use the example of discrepant practice above: a c-section at 36 weeks would be appropriate for a mother with preeclampsia, but not for a healthy first time mother with no risk factors and good health status. When studying c-section rates, it is important to differentiate between these two scenarios before drawing conclusions about the care being provided.

Beyond the data system, BORN is employing a number of supporting strategies:

- A team of BORN Coordinators across the province work with data providers to ensure information is of the highest possible quality, and timely.
- An analysis and research team translate the data into information and knowledge for users, providers and planners. They also facilitate access to the BORN data by researchers as a secondary use of the information as per the *Personal Health Information Protection Act, 2004*.
- An external and internal committee structure provides the oversight and expertise required to make informed and responsible decisions.



As a division of CHEO, BORN benefits from the infrastructure and leadership of CHEO. The Privacy Officer of BORN has a hierarchy of responsibility to which s/he can access the necessary approvals and disclosures, outlined below.



To learn more about BORN Ontario please see www.BORNOntario.ca.

Note: in the event of a conflict between BORN Ontario Privacy and Security policies and CHEO policies, the more strict of the two policies shall apply.

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

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-01
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that the Better Outcomes Registry & Network, or BORN Ontario, has a privacy and security accountability framework to implement its status and overall responsibility as a prescribed person under the *Personal Health Information Protection Act, 2004.*
Policy	**Status** The Children's Hospital of Eastern Ontario (CHEO) is a prescribed person in respect of BORN Ontario as per section 13(1) of Ontario Regulation 329/04-General (Regulation), enacted under the *Personal Health Information Protection Act, 2004* for the purposes of facilitating or improving the provision of health care for mothers, infants and children. Section 13(2) of Ontario Regulation 329/04-General (Regulation), enacted under the *Personal Health Information Protection Act, 2004* requires BORN Ontario, as a prescribed registry: • To have in place practices and procedures to protect the privacy of individuals whose Personal Health Information BORN Ontario receives • To maintain the confidentiality of that information • These practices and procedures must be approved by the Information and Privacy Commissioner of Ontario every three years BORN Ontario is committed to complying with the provisions and regulations of the *Personal Health Information Protection Act, 2004* applicable to a person holding a registry, as well as any other applicable legislation. **Privacy and Security Accountability Framework** BORN Ontario has developed comprehensive privacy and security policies and procedures to ensure compliance with the *Personal Health Information Protection Act, 2004* and its regulation.

	The President and Chief Executive Officer of CHEO is ultimately accountable for ensuring compliance with the *Personal Health Information Protection Act, 2004* and its regulation and ensuring compliance with BORN's privacy and security policies and procedures. The President and Chief Executive Officer of CHEO has delegated day-to-day responsibility for ensuring compliance with the *Personal Health Information Protection Act, 2004* and its regulation, and for ensuring compliance with BORN Ontario privacy and security policies and procedures to the BORN Ontario Leadership Team. The BORN Ontario Leadership Team has delegated the day-to-day management of the privacy and security program to the Privacy Officer who reports to the BORN Ontario Leadership Team on all related privacy and security matters. The duties and responsibilities of the Privacy Officer focus on developing and maintaining a strong culture of privacy at BORN Ontario and include: • Management of the privacy program and security program, including monitoring compliance, conducting regular audits and providing reports to senior management and recommendations for changes to policies or procedures • Execution of privacy training • Execution and oversight of privacy impact assessments • Responding to inquiries or complaints related to BORN Ontario privacy practices • Any and all related privacy and security oversight The Privacy Officer works in collaboration with the CHEO Chief Privacy Officer to ensure alignment between BORN Ontario privacy policies and any applicable CHEO privacy policies. The following committees and roles also form part of the privacy and security accountability framework. The Privacy and Security Review Committee has responsibility for: • Developing, reviewing and approving BORN Ontario policies and procedures • Overseeing implementation of the procedures • Conducting annual reviews of privacy and security policies and procedures (or more frequently as needed to ensure safeguards remain effective and to determine whether modifications are warranted) • Reviewing annually the collections, uses and disclosures of Personal Health Information to ensure adherence to the provisions and principles of the Personal Health Information Protection Act, 2004 and its regulation The Data Dictionary Review Committee has responsibility for conducting

	annual reviews of data holdings to ensure that the need for each data element has been identified and that BORN Ontario does not collect more Personal Health Information than is reasonably necessary to meet its purposes. The Disclosure of Personal Health Information Review Committee also reviews all requests for use and disclosure of Personal Health Information for research purposes and for disclosure to a prescribed entity. The Scientific Manager has responsibility for reviewing all research requests to ensure that they comply with the requirements of the *Personal Health Information Protection Act, 2004* and its regulation. The Manager of Health Informatics has responsibility for the technology leveraged to collect and store the Personal Heath Information used by BORN Ontario. *See* HR-08 and HR-09 Job Description for Position(s) Delegated Day-to-Day Authority to Manage the Privacy and Security Programs*.* **Collection of Personal Health Information** BORN Ontario collects Personal Health Information to improve the quality of health care services provided to mothers, infants and children in Ontario. 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 period). This information is collected from health information custodians involved in the care of both newborns and their mothers, in particular those providing pre- and post-natal care to pregnant woman across Ontario such as hospitals and patient practitioners like family physicians or midwives. BORN Ontario 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 Ontario collects only those data elements that have been identified through the rigorous review process undertaken by the Data Dictionary Review Committee as per P-04 Collection of Personal Health Information and P-06 Statements of Purpose for Data Holdings Containing Personal Health Information*.* The Data Dictionary Review Committee process ensures that each identified collection is consistent with the Act and it's regulations. The Data Dictionary Review Committee has responsibility for determining: • The nature of the Personal Health Information required to enable

	BORN Ontario to fulfill its mandate • List of data elements to be collected, and any sub-elements, as applicable • The health information custodians from whom the data elements will be collected • The rationale or statement(s) of purpose for each data element in relation to the identified purpose of the Registry The list of data holdings is reviewed annually by the Data Dictionary Review Committee as per P-04 Collection of Personal Health Information and P-06 Statements of Purpose for Data Holdings Containing Personal Health Information and is posted on the BORN Ontario website (http://www.bornontario.ca/privacy/statement-of-information-practices) along with the name, address and phone number of the Privacy Officer from whom further information may be obtained in relation to the purposes, data elements and data sources for each data holding of Personal Health Information. **Use of Personal Health Information** BORN Ontario uses the Personal Health Information that it collects to: • Identify 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) • Facilitate continuous improvement of screening thresholds to minimize missed cases • Raise alerts where maternal and/or newborn outcomes are clinically or statistically discrepant with accepted norms • Identify strategies to improve the quality and efficiency of care for mothers, infants and children • Create reports that can be used to provide the Ministry of Health and Long-Term Care, Local Health Integration Networks (LHIN) and Public Heath Units with comprehensive and timely information to support effective planning and management of health care delivery for mothers, babies and children in the province Information provided in reports to the Ministry, Local Health Information Networks and Public Health does not contain Personal Health Information or identify individuals; they only present an overview of aggregated health care data. The reports are carefully reviewed to ensure there is no risk of re-identification through small cell counts or other forms of possible residual disclosure *as per* P-24: De-Identification and Aggregation. The reports are made available through the BORN Ontario website at www.BORNOntario.ca. BORN Ontario 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 Ontario does not use Personal Health Information if other information will serve the purpose and does not use more Personal Health Information than is reasonably necessary to meet the purpose, using de-identified or aggregate information wherever possible. BORN may use Personal Health Information to conduct research only when the strict requirements of the *Personal Health Information Protection Act, 2004* are adhered to, including review by a Research Ethics Board as per P-10: Use of Personal Health Information for Research. BORN Ontario remains responsible for Personal Health Information used by its Agents. Access and use by BORN Agents is strictly controlled. Agents are trained on their privacy obligations and sign a Confidentiality Agreement acknowledging the requirements to use only the information necessary for their work, to keep Personal Health Information secure at all times, and to notify BORN Ontario 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 Agreement by Agents **Disclosure of Personal Health Information** BORN Ontario 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 the *Personal Health Information Protection Act, 2004* and its regulation: • To health care providers, when facilitating access for mothers, babies and children for care and treatment; for example, to ensure appropriate screening is offered in a meaningful timeframe • To a prescribed entity for the management, evaluation, monitoring or planning for the health system • To researchers for research purposes as defined in the *Personal Health Information Protection Act, 2004*. Personal Health Information is provided to researchers only if de-identified information is not sufficient to conduct the research. The research plan must be approved by a Research Ethics Board, meet the requirements set out in the Personal Health Information Protection Act, 2004, and be approved by the Scientific Manager who ensures that the minimum amount of Personal Health

Information and the least identifiable information is disclosed. The Scientific Manager is assisted by assessments conducted by the Electronic Health Information Laboratory

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 BORN Ontario Scientific Manager 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 BORN Ontario Scientific Manager is assisted by assessments conducted by the Electronic Health Information Laboratory that determine the risk of re-identification.

De-identified and aggregated Personal Health Information may be disclosed to the following groups and for the following purposes including:

- To Public Health Units to facilitate the appropriate planning, monitoring and provision of health care.
- To Researchers for research purposes
- To the Ministry of Health to inform policy and planning

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

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

BORN Ontario ensures that both **paper** and **electronic** records are kept safe and secure as follows:

- **Where Paper** records exist, they are to be considered transitory; they will be converted to electronic records at the earliest opportunity and destroyed as per S-08 Secure Disposal of

	Records of Personal Health Information • **Electronic** records will be maintained in identifiable form within the transactional database for 28 years and then converted to a de-identified format as per S-05 Secure Retention of Records of Personal Health Information and S-06 Secure Retention of Records of Personal Health Information on Mobile Devices. The reporting database will only include de-identified information to protect Personal Health Information from the broader BORN Ontario report user community • Records of Personal Health Information in both paper and electronic format will be 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 Ontario 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 annually, at a minimum, 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 Ontario and BORN Ontario's compliance with the *Personal Health Information Protection Act, 2004* and its regulation must be directed to: BORN Ontario Privacy Officer Suite 106-1785 Alta Vista Drive Ottawa ON K1G 3Y6 E-mail: privacy@BORNOntario.ca Phone: 613-523-3781 Fax: 613-523-9057

	See the BORN Ontario website at www.BORNOntario.ca Individuals may also direct complaints regarding the compliance of BORN Ontario to the Information and Privacy Commissioner of Ontario : Information and Privacy Commissioner of Ontario 2 Bloor Street East Suite 1400 Toronto, Ontario 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 available on the BORN website at www.BORNOntario.ca/Privacy the P01- Privacy Policy in Respect of CHEO's Status as a Prescribed Person and the Statement of Information Practices. The privacy policies can also be obtained by contacting the Privacy Officer as per above.
Responsibility	**Privacy Officer**

P-02 Ongoing Review of Privacy and Security Policies and Procedures

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-02 and S-02
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario has in place an effective policy to enable ongoing review of its privacy and security policies and procedures.
Policy	BORN Ontario undertakes a review of its privacy and security policies and procedures on an annual basis or more frequently if required. The purpose of a review is to determine whether amendments are needed or whether new policies and procedures are required to ensure that BORN Ontario meets or exceeds industry standards and best practices. BORN Agents who become aware of areas where the BORN Ontario privacy and security policies and/or procedures are inadequate, inoperable or for any other reason could be improved are encouraged to report those concerns or suggestions to the Privacy Officer. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits and S-15: Security Audits.
Responsibility	Privacy Officer

P-03 Transparency of Privacy Policies and Procedures	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-03
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario's privacy policies and procedures are transparent for the public and stakeholders.
Policy	As required by its status as a Prescribed Person under *Personal Health Information Protection Act, 2004*, BORN Ontario makes available P01 – Privacy Policy in Respect of it's Status as a Prescribed person through the BORN Ontario website at www.BORNOntario.ca/Privacy. A brochure is also available for download from the website.
Responsibility	Privacy Officer

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

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-04 Policy No. P-06
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario limits the collection of Personal Health Information in accordance with the requirements set forth by *Personal Health Information Protection Act, 2004* and best practices for privacy protection.
Policy	BORN Ontario only collects Personal Health Information if the collection is permitted by *Personal Health Information Protection Act, 2004* and its regulation. BORN Ontario collects only the minimum amount of Personal Health Information required to achieve the purpose of the Registry. BORN Ontario does not collect Personal Health Information if other information will serve the purpose of the Registry. BORN Ontario collects only those data elements that have been identified through the rigorous review process set out below. The purpose of the review process is to identify the minimum data elements necessary to achieve the Registry's purpose of facilitating and improving the provision of care to mothers, infants and children. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Data Dictionary Review Committee, Privacy Officer

P-05: List of Data Holdings Containing Personal Health Information

The BORN System, when complete, is a single data holding that is comprised of Personal Health Information collected from the following health information custodians:

1. Prenatal and Newborn screening providers
2. Hospitals
3. Midwives
4. Outpatient clinics

The unique data collections that are provided by various health information custodians for specific maternal-newborn encounters with the healthcare system are:

- Prenatal screening laboratory, ultrasound and results information
- Prenatal screening follow-up
- Antenatal specialty for congenital anomalies information
- Antenatal general for pregnancy status and care information
- Labour information
- Birth information
- Postpartum information
- Neonatal intensive care unit information for the sickest babies
- Newborn screening laboratory and results information
- Newborn screening follow-up for diagnosis information

P-07 Evidence: Statements of Purpose for Data Holdings Containing Personal Health Information

Children's Hospital of Eastern Ontario (CHEO) in respect of BORN Ontario is listed in the Regulation made under the *Personal Health Information Protection Act, 2004 (PHIPA)*, s. 39(1)(c), as a "prescribed registry" in respect of its data holding. Prescribed registries are a specific class of organizations that are permitted under PHIPA to collect Personal Health Information from health information custodians (without individuals' consent) for the purposes of facilitating and improving health care. In turn, prescribed registries are permitted to use and disclose Personal Health Information received from health information custodians (without consent) for the same purposes as permitted under s. 49(1) of the *Act*.

CHEO and the Ministry of Health and Long-Term Care established BORN Ontario:

- To build and manage the maternal/child Registry
- To build a source of accurate and timely maternal-infant information for facilitating and improving the provision of health care to pregnant women and children in Ontario
- For analysis of maternal-newborn data to support decision making by health care providers and planners

The core uses of the registry are:

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

B. Facilitating continuous improvement of healthcare delivery tools to minimize adverse outcomes. For example, improvement of screening algorithm and cut-offs to minimize missed screens.

C. Raising alerts where maternal and/or newborn outcomes are statistically discrepant with accepted norms. For example, an increase in congenital anomalies associated with a specific geographic region suggesting a toxic exposure or a provider being identified as performing too many episiotomies as compared to peers, leading to poor maternal outcomes.

D. Enabling health care providers to improve care by providing them the information and tools to compare themselves with peers and/or benchmarks.

E. Knowledge translation to improve the quality and efficiency of care for mothers, infants and children. For example, identifying strategies for health information custodians for continuous quality improvement.

F. Creating reports that can be used to provide the Ministry of Health and Long-Term Care, LHINs and Public Heath Units with comprehensive and timely information to support effective planning and management of health care delivery for mothers, babies and children in the province.

The BORN System, when complete, is a single data holding that is comprised of Personal Health Information collected from the following health information custodians:

1. Prenatal and Newborn screening providers
2. Hospitals
3. Midwives
4. Outpatient clinics

In deciding the data elements to include in the BORN dataset, each element is reviewed to ensure it is required to be collected in order to achieve the purposes of the BORN Registry. The following framework outlines the five types of information that are required.

1. Identifiers
2. Health Status
3. Health Risk Factors
4. Care Provided
5. Health Outcomes

The combination of all of these data types is required for the successful operation of the registry. Details and examples of each …

Identifiers

When instances of insufficient care are identified it is critical that BORN Ontario have in place a mechanism by which to alert the mother or care provider of the opportunity to improve care in a timely way. The identifiers must also allow the mother and child data to be augmented with additional health information to allow the health status, care provision and outcomes to be combined as outlined in the subsequent sections. Identifiers that allow the woman to be uniquely identified and appropriately contacted are required to meet the purposes of the Registry. We will regularly review identifiers to determine if fewer data elements would be sufficient for these purposes.

Examples

1. **Missed Screen**. Newborn Screening Ontario tests for 28 rare diseases in newborns. Test results can lead to early identification and proper, life-saving treatment. By capturing every birth in the province and then cross-referencing to every baby tested by Newborn Screening Ontario, BORN Ontario can promptly identify the babies that have not been tested and inform the primary care provider to ensure the test is offered.
2. **Missed Case**. A child screens negative for PKU in prenatal screening. Several months later the child is diagnosed with PKU by other means. It is critical that the identifiers on the two records allow the two to be linked, such that Newborn Screening Ontario learns that there are problems with the screening test.

Health Status

The health outcome of both mother and child is dependent upon the current health status of each. A complete understanding of the current health status of the mother and the child is needed to identify situations where additional care may be required.

Examples

1. **Gestational diabetes screening reminder**. Mothers testing positive for gestational diabetes require follow-up as they are at increased risk for Type 2 diabetes and its many resultant complications later in life. The Registry can gather this health status information from a number of antenatal providers (family doctor, midwife, obstetrician, birthing hospital) and alert the primary care physician to ensure appropriate follow-up care is offered. This can prove to have important long-term benefits for the woman and the system resources.
2. **Antenatal 1 and 2 Forms**. Complete pregnancy history and documentation of care is tracked across providers using the provincially mandated Antenatal 1 and Antenatal 2 forms. These forms should be sent to the birthing hospital at 35 weeks' gestation. A survey by BORN Ontario suggests that women frequently deliver without their providers having access to the information – either they deliver unexpectedly, early, or the forms cannot be located. Providing access to these forms in emergent situations ensures that providers have key clinical information available and also reduces the duplication of tests used to facilitate care (ultrasounds and laboratory).

Health Risk Factors

The health outcome of both the mother and the child can be impacted by the demographics of both. BORN Ontario must understand the current status of the woman and child to identify situations where additional care may be required.

Examples

1. **Unexplained poor outcomes, such as increased anomalies**. As an authoritative source of maternal-child health outcomes information, BORN Ontario is the only organization in the province with timely access to health trends in the population. Previously, a cluster of congenital anomalies was suspected in south western Ontario. It was through detailed analysis of the data entry, outcomes, risk factors and interventions that the signal was found to be in error. Should a legitimate signal be found, prevention of further congenital anomalies is possible by identifying women from the registry and offering them (through their health provider) further screening, diagnostic testing or therapy.
2. **Linking Risk to Outcomes**. Women who develop preeclampsia during pregnancy are at increased risk for cardiovascular disease later in life. The outcomes cannot be studied if the overall pregnancy environment is not understood.

Care Provided

The Registry must know what care has been provided for two reasons:

1. To quickly identify situations where care is insufficient (e.g. baby born, but no newborn screen completed).
2. To link 'Care Provided' to 'Outcomes' to develop the knowledge required to improve care to the maternal/child population.

Examples

1. **Missed Screen**. A baby was born in the community but was not offered newborn screening. Whether newborn screening was or was not offered must be captured in the system to identify the newborns not yet screened.
2. **NTQA.** Nuchal translucency (NT), a measurement on the neck of the fetus during ultrasound, is a key component in the prenatal screening algorithm. With values smaller than a millimetre being an important differentiation, it is critical that sonographers measure it accurately. Much work has been done internationally on quality assurance of NT measurements that involve plotting all measurements done by a single sonographer and comparing the distribution to accepted norms. BORN Ontario is able to collect these key measurements from labs across the province and report back to sonographers and their managers on the quality of their work. By minimizing errors in NT measurements, prenatal screening results will be much more accurate, reducing false positives and false negatives and the associated repeat tests and analysis.
3. **Discrepant Practice**. Evidence associated with labour, birth and newborn care in the province shows significant variation in key indicators such as caesarean section rates and other labour interventions. Tracking, reporting and addressing these variations will ensure women in the province are offered consistent, high-quality and appropriate care. Once data are available, BORN coordinators will work with the hospital or individual provider to understand why their rates are discrepant and develop and implement quality improvement strategies.

4. **Access to Aggregate data**. Health care providers collect key clinical information for an individual as part of every visit, for example, the clinical details associated with labour including the indications for interventions, the timing of the labour, the medications and analgesia administered and final outcome for mother and baby. It is only once this data are aggregated that the information highlights important trends in the care being provided, for example, many women having emergency c-sections, many women being induced rather than labour starting spontaneously. Providers are willing to invest the time required to enter the information into the BORN system because it provides them great value for program planning and management of care to analyse their data in aggregate.

Health Outcomes

By connecting 'Health Status' and 'Care Provided' to maternal/newborn 'Outcomes', BORN can improve the provision of health care to pregnant women, babies and children in Ontario.

Examples

1. **Improving Screening Algorithms**. Screening is a mechanism to assess and report risk and as such, involves false-positive and false-negative results. While this is expected, the anxiety for families upon receiving a positive screen is significant, and the impact on individuals with a false negative result can be catastrophic. By gathering all screening results and all associated follow-up and outcomes information, trained analysts can review the information to identify triggers for the false results. Once analyzed, the screening thresholds can be adjusted to reduce false-positive and false-negative results. The costs of false negative can be significant – from lifelong disability to potential death. Reduction in the false positives will reduce the number of families impacted by the anxiety associated with a positive result.
2. **Effectiveness.** Providing feedback to public health units and health promotion agencies on the effects of their campaigns around smoking cessation, breastfeeding promotion, prenatal class attendance and the relationships between these and newborn and childhood outcomes will help improve the care provided to mothers and children.
3. **Reports.** The Ontario health care system is dependent on high quality information for decision making. Public Health Units and LHINs regularly request reports from the BORN founding members to plan the delivery of services in their region. Using aggregate information from the BORN System, we can inform regions and populations of key trends that need to be addressed.

The BORN Data Dictionary document maps each data element collected by the BORN System to one of the examples included in this document to illustrate the requirement for the data element to be collected. In many cases, data elements are required for multiple examples but only one is identified.

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

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-08
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario limits access to and use of Personal Health Information by BORN Ontario Agents.
Policy	An Agent is defined as a Children's Hospital of Eastern Ontario (CHEO) employee or consultant, contractor or seconded employee to BORN Ontario who has authority to provide services to or on behalf of BORN Ontario. For further certainty, for the purposes of these policies and procedures, the BORN System Hosting Provider is an Agent of BORN Ontario. Access to Personal Health Information by BORN Ontario Agents is based on the "need to know" principle, embodied in role-based access. Duties of Agents with access to Personal Health Information are segregated in order to avoid a concentration of privileges that would enable a single Agent to compromise Personal Health Information. BORN Ontario prohibits Agents from accessing and using Personal Health Information except as necessary for his or her employment or contractual responsibilities. BORN Ontario requires Agents to access and use the minimum amount of identifiable information reasonably necessary for carrying out their day-to-day employment, contractual or other responsibilities with BORN Ontario. BORN Ontario prohibits access to and use of Personal Health Information if other information, such as de-identified and/or aggregate information, will serve the identified purpose. BORN Ontario prohibits Agents from using de-identified and/or aggregate information, either alone or with other information to identify an individual, including attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in

	accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

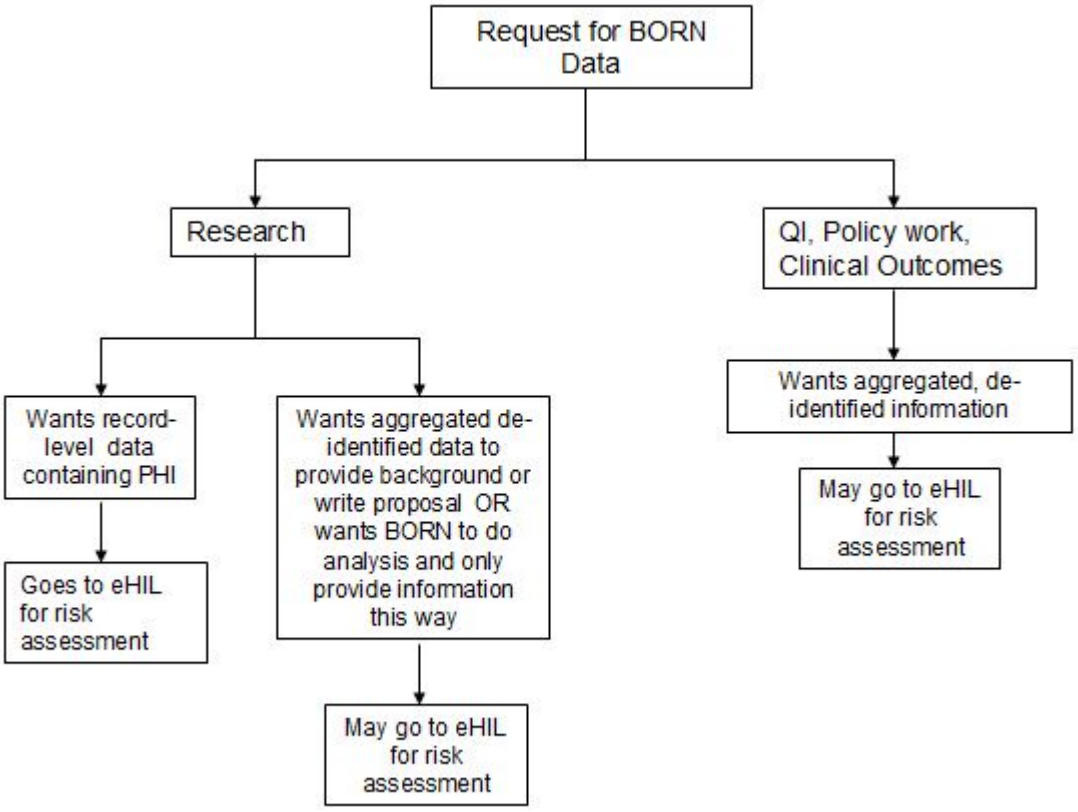
P-10: Use of Personal Health Information for Research

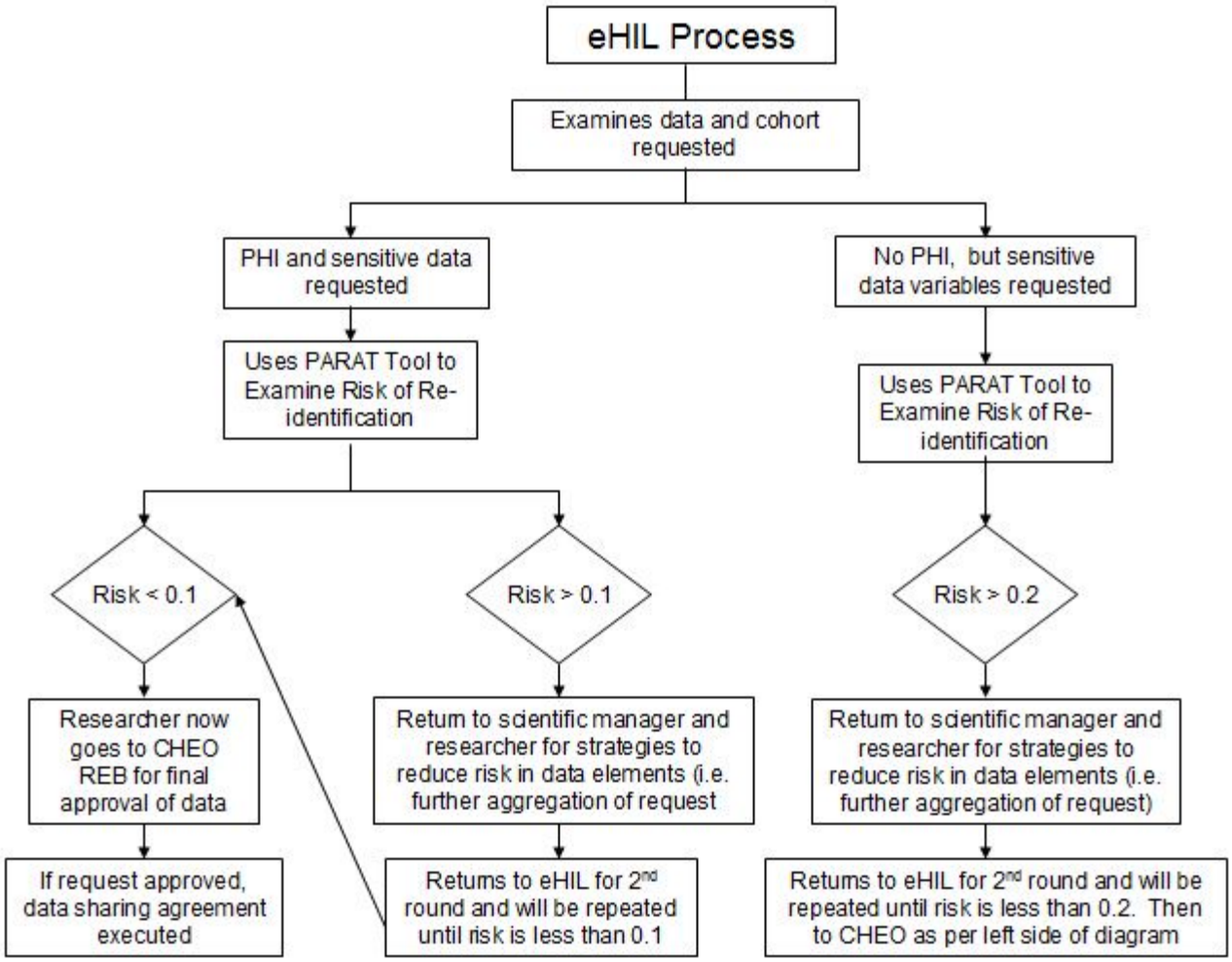
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-10
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To identify BORN Ontario policies and procedures on the use of Personal Health Information by BORN Agents for research purposes.
Policy	**General** BORN Ontario limits the use of Personal Health Information to those purposes authorized by *Personal Health Information Protection Act, 2004* and its regulation. BORN Ontario permits use of Personal Health Information for research purposes as authorized under *Personal Health Information Protection Act, 2004* where • BORN Ontario Agents meet the requirements for research provided in *Personal Health Information Protection Act, 2004* section 44 and associated regulations. • The purpose for the use is in accordance with the stated purpose for the Registry BORN Ontario will not use Personal Health Information for research purposes if other information will serve the research purpose. BORN Ontario will not use more Personal Health Information than is reasonably necessary to meet the identified research purpose. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate. In accordance with HR-11: Discipline and Corrective Action, where the Privacy Officer finds a BORN Agent in contravention of this policy and procedures and/or where there has been a breach of Personal Health Information, the Privacy Officer determines appropriate discipline and

	corrective action and provides the determination to the Agent's supervisor and Human Resources, as the case may be. Disciplinary and corrective action may include: • Additional privacy and awareness training in cases where the non-compliance was inadvertent • Termination of employment, contractual or other relationship and/or legal action where the nature of the non-compliance appears to be of malicious intent
Responsibility	Privacy Officer, Scientific Manager

P-10E: Data Request Review Process




eHIL Process
Examines data and cohort requested
PHI and sensitive data requested
No PHI, but sensitive data variables requested
Uses PARAT Tool to Examine Risk of Re-identification
Uses PARAT Tool to Examine Risk of Re-identification
Risk < 0.1
Risk > 0.1
Risk > 0.2
Researcher now goes to CHEO REB for final approval of data
Return to scientific manager and researcher for strategies to reduce risk in data elements (i.e. further aggregation of request
Return to scientific manager and researcher for strategies to reduce risk in data elements (i.e. further aggregation of request)
If request approved, data sharing agreement executed
Returns to eHIL for 2nd round and will be repeated until risk is less than 0.1
Returns to eHIL for 2nd round and will be repeated until risk is less than 0.2. Then to CHEO as per left side of diagram

P-12: Disclosure of Personal Health Information for Purposes Other Than Research

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-12
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario only discloses Personal Health Information for those purposes authorized by the *Personal Health Information Protection Act, 2004* and its regulation.
Policy	BORN Ontario limits the disclosure of Personal Health Information to those purposes permitted under the *Personal Health Information Protection Act, 2004* and its regulation. BORN Ontario will not disclose Personal Health Information if other information will serve the purpose and will not disclose more Personal Health Information than is reasonably necessary to meet the purpose. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Scientific Manager, Privacy Officer

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

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-13
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario only discloses Personal Health Information for research purposes in accordance with the *Personal Health Information Protection Act, 2004* and its regulation.
Policy	BORN Ontario permits disclosure of Personal Health Information for research purposes as authorized under *Personal Health Information Protection Act, 2004* and its regulation. Researchers must meet the requirements for research disclosure provided in section 44 and associated regulations. BORN Ontario will not disclose Personal Health Information for research purposes if other information will serve the research purpose. BORN Ontario will not disclose more Personal Health Information than is reasonably necessary to meet the identified research purpose. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Scientific Manager

P-16 Data Sharing Agreements	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-16
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario effectively executes data sharing agreements.
Policy	BORN Ontario requires the execution of a data sharing agreement when BORN Ontario is: • Collecting Personal Health Information from health information custodians (hospitals, midwifery practice groups and laboratories, clinics) for the purposes of BORN Ontario • Disclosing Personal Health Information for purposes other than research (e.g. to a prescribed entity, midwifery program at Ministry of Health and Long-Term Care for billing purposes) **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer, Privacy Administrator

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

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-19
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario executes agreements with third party service providers in respect of Personal Health Information.
Policy	A written agreement (**Error! Reference source not found.***)* must be entered into with third party service providers prior to permitting access to and use of Personal Health Information including: • Those that are contracted to retain, use, transfer or dispose of records of Personal Health Information, and • Those that are contracted to provide services to use electronic means to collect, use, modify, disclose, retain or dispose of Personal Health Information (electronic service providers) BORN Ontario does not provide Personal Health Information to a third party service provider if other information, namely de-identified and/or aggregate data, will serve the purpose and will not provide more Personal Health Information than is reasonably necessary to meet the purpose. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

P-22: Linkage of Records of Personal Health Information

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-22
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario appropriately links records of Personal Health Information.
Policy	Data linkage refers to the act of connecting an individual person's information from at least two sources for a specific purpose. BORN Ontario permits linkage of Personal Health Information for the following purposes: • Identifying where appropriate care has not been received and facilitating access to care and treatment for mothers, infants and children • Facilitating continuous improvement of healthcare delivery tools to minimize adverse outcomes • Raising alerts where maternal and/or newborn outcomes are statistically discrepant with accepted norms • Looking across the continuum of care of an individual or population (pregnancy to birth to young childhood) to improve the quality and efficiency of care for mothers, infants and children. For example, linking health outcome information to interventions allows for the analysis of the quality of the care being provided • Creating reports that can be used to provide the Ministry of Health and Long-Term Care, Local Health Integration Networks and Public Health Units with comprehensive and timely information to support effective planning and management of health care delivery for mothers, babies and children in the province. BORN Ontario permits the following types of record linkages: • Linkage of records of Personal Health Information solely in the custody of BORN Ontario for the exclusive purposes of BORN Ontario • Linkage of records of Personal Health Information in the custody of BORN Ontario with records of Personal Health Information to be collected from another person or organization for the exclusive purposes of BORN Ontario

	• Linkage of records of Personal Health Information solely in the custody of BORN Ontario for the purposes of disclosure to another person or organization • Linkage of records of Personal Health Information in the custody of BORN Ontario with records of Personal Health Information to be collected from another person or organization for the exclusive purposes of that other person or organization **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

P-24: De-Identification and Aggregation

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-24
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario implements appropriate data de-identification and aggregation practices.
Policy	BORN Ontario prohibits the use or disclosure of Personal Health Information if other information, namely de-identified and/or aggregate information, will serve the identified purpose. Where information is aggregated, but includes information about individuals in groups of five (5) or less, the information will not be released. This restriction is contained in all Research Agreements and data sharing agreements. Agents are prohibited from using de-identified and/or aggregate information, alone or in combination with other information, to identify an individual. This requirement is contained in all Research Agreements and data sharing agreements. De-identified information refers to records that have had enough personal information removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information alone can be used to identify an individual. Aggregate information refers to summed and/or categorized data that is analyzed and placed in a format that precludes further analysis (e.g. tables or graphs) to prevent the chance of revealing an individual's identity. Individual records cannot be reconstructed. Identifying information refers to information that identifies an individual or that it is reasonably foreseeable in the circumstances could be used either alone or with other information to identify an individual. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first

	reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer and Scientific Manager

P-25: Privacy Impact Assessments

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-25
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario has in place effective policies to assess the impact of new or modified activities that involve the collection, use or disclosure of Personal Health Information
Policy	A privacy impact assessment is a detailed assessment undertaken to identify the actual or potential effects that a proposed project will have on the privacy of those whose personal information is included in the proposed project. A privacy impact assessment also identifies ways in which privacy risks may be mitigated. BORN Ontario undertakes privacy impact assessments: • On existing programs, processes and systems when there are significant changes relating to the collection, access, use or disclosure of Personal Health Information • In the design of new programs, processes and systems involving Personal Health Information • On any other programs, processes and systems with privacy implications, as recommended by the Privacy Officer Privacy impact assessments are updated in the following circumstances: • During the detailed design and implementation stage, where a conceptual PIA was done during the design stage • Significant changes to purposes, data collection, uses or disclosures • Significant changes to functionality of the service technology • Change in vendor/technology partner • Implementation of a new service delivery or management technology that stores, transmits, or retrieves Personal Health Information • When the Privacy Officer determines that an update is required • Every three years, at a minimum Privacy impact assessments are not required where existing programs,

	processes and systems are changed or new programs, processes, and systems are implemented, if no personal information or Personal Health Information is involved. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

P-27: Privacy Audits	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-27
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario conducts regular privacy audits and appropriately manages findings and recommendations resulting from these audits.
Policy	The Privacy Officer conducts regular privacy audits to: • Assess organizational compliance with privacy policies and procedures to ensure that they continue to reflect the requirements of the *Personal Health Information Protection Act, 2004* and its regulation as well as privacy best practices • On external parties to assess compliance with Research, Data Sharing and Third-party agreements • Assess compliance of Agents permitted to access and use Personal Health Information as per P-08: Limiting Agent Access to and Use of Personal Health Information **Compliance Audit and Enforcement** Agents responsible for conducting privacy audits are required to notify the Privacy Officer, at the first reasonable opportunity, of a privacy breach or suspected privacy breach or a security breach or suspected security breach as per P-29 Privacy Breach Management and S-17 Security Breach Management.
Responsibility	Privacy Officer

P-29 Privacy Breach Management	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-29
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario addresses the identification, reporting, containment, notification, investigation and remediation of privacy breaches as defined in this policy.
Policy	A privacy breach is: • The collection, use and disclosure of Personal Health Information that is not in compliance with the Personal Health Information Protection Act, 2004 and its regulation • A contravention of BORN Ontario privacy policies, procedures or protocols • A contravention of a BORN Ontario Confidentiality Agreement or the terms and conditions in data sharing agreements, Research Agreements, and Agreements with Third Party Service Providers retained by BORN Ontario • Circumstances where Personal Health Information is stolen, lost or subject to unauthorized use or disclosure or where records of Personal Health Information are subject to unauthorized copying, modification or disposal Agents must notify the Privacy Officer **as soon as reasonably possible**, and do whatever is reasonably possible to contain a breach or suspected breach, whether internal or external, and mitigate its effects immediately as per to HR-01 and HR-03 Privacy and Security Training and Awareness. **Contact Information for the BORN Ontario Privacy Officer** BORN Ontario Privacy Officer Suite 106-1785 Alta Vista Drive Ottawa ON K1G 3Y6 E-mail: privacy@BORNOntario.ca Phone: 613-523-3781 Fax: 613-523-9057 BORN Ontario website: www.BORNOntario.ca

	Compliance Audit and Enforcement BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17: Security Breach Management as appropriate.
Responsibility	Privacy Officer

P-29 A: Breach Management Protocol

A privacy breach occurs when there is unauthorized access to, or collection, use, disclosure or disposal of Personal Health Information whether done deliberately or inadvertently. Such activity is unauthorized if it occurs in contravention of the Ontario *Personal Health Information Protection Act, 2004* (*PHIPA*) or BORN Ontario policies and procedures.

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

Examples of privacy breaches include instances where Personal Health Information is lost, stolen, or mistakenly provided to the wrong person, such as when a computer is stolen.

Responding to a Privacy Breach

- It is important for all BORN Ontario staff to respond *immediately* when faced with a breach or a potential breach.
- The following steps should be carried out simultaneously or in quick succession.

Step 1: Contain the Breach to the extent possible

As a BORN Agent who discovers a potential breach you should act quickly to limit the breach.

- You must ensure that no further breaches can occur through the same means (e.g., change passwords, identification numbers, and or temporarily shut down a system)
- You must determine what (if any) Personal Health Information has been stolen, lost or

accessed, used, disclosed, copied, modified or disposed of in an unauthorized manner

- You must securely retrieve or destroy as much as possible of the breached information. In other words, if the information can be retrieved in a secure fashion, do so, otherwise confirm that as much of the information as is possible has been destroyed, and you have written confirmation of that action including date, time and method of secure disposal
- You must ensure that no copies of the Personal Health Information have been made or retained by the individual who was not authorized to retrieve or receive the information
- You must determine whether the breach or potential breach would allow unauthorized access to any other data (e.g. passwords being disclosed that could provide access to systems or databases) and take whatever steps are necessary and appropriate to shut down that access (e.g. disable the password)

Step 2: Get Help to Evaluate the Situation

As a BORN Agent who discovers a potential breach you are required to support the evaluation of the situation.

- You must notify the Privacy Officer at the first reasonable opportunity
- You must complete and Breach Reporting Form which includes the following:
  - Name and position of the individual who discovered the breach
  - Date and time of discovery
  - Estimated time and date the breach occurred
  - Type of breach (loss, theft, inadvertent disclosure)
  - Cause of breach, if known
  - Description of information involved in the breach
  - Actions taken by Agent reporting the breach to contain the breach
  - Any other individuals or organizations involved in the breach (or its notification) and contact information for relevant individuals
- The Breach Reporting Form should be completed and forwarded to the Privacy Officer as soon as reasonably possible.
- The Privacy Officer will work with you and other appropriate BORN staff or external resources to determine the extent of the breach:
  - What data elements have been breached?
  - Is there a risk of further exposure of the information?
  - Is the information encrypted or otherwise non-accessible?
  - How many individuals are affected by the breach?
  - Who are the individuals affected by the breach?
  - What is the cause of the breach?
  - What organizations are involved in the breach?
- The Privacy Officer, together with you and other appropriate BORN staff or external resources must determine harm that may result from the breach, including:
  - Security risk
  - Identity theft or fraud
  - Hurt, humiliation, damage to individual's reputation
  - Risk to public health

3. Consider Notification

The Privacy Officer will consider broader notification of the breach.

- The Privacy Officer must consider the advisability of notifying other organizations such as:
    - Information and Privacy Commissioner of Ontario
    - Police
- Whenever personal health information is or is believed to be stolen, lost or acessed by unauthorized perons and whenever required pursuant to the agreement with the health information custodian or organization, the Privacy Officer must send written notification to the heath information custodians or organization who provided the information at the first reasonable opportunity in order that they may notify individuals whose privacy was breached.

4. Prevent further breaches

The Privacy Officer is responsible for preventing further breaches.

- The Privacy Officer must review existing policy for necessary changes to BORN polices and procedures to avoid any further breaches
- The Privacy Officer must undertake any required educational campaign within BORN (and associated organizations as necessary) to educate employees on how to avoid further breaches
- The Privacy Officer must review BORN Ontario Breach Management Protocol for potential improvements
- The Privacy Officer must take appropriate action regarding the individual responsible for the breach

P-31: Privacy Complaints	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-31
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario effectively manages privacy complaints.
Policy	BORN Ontario responds to all privacy complaints including: • Complaints relating to the privacy policies and procedures implemented by BORN Ontario • Complaints related to the compliance of BORN Ontario to the *Personal Health Information Protection Act, 2004* and its regulation **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

P-32 A: Complaint Form

BORN Ontario Complaint Form

Your Information

Full Name: _____

Address: _____

Daytime Telephone Number: _____

E-mail address*: _____

* I consent to being contacted at this e-mail address. I acknowledge that sending e-mail over the Internet is not secure, in that it can be intercepted and/or manipulated and retransmitted. Please initial _____

Complaint Information

Please provide a detailed description of your privacy complaint covering the *what, when, who, how, where and why* of what happened. Please be sure to describe the nature of the occurrence and any subsequent contacts you have had with BORN Ontario and the outcomes. (If you need additional space, please attach as many pages as necessary.)

Where to send this form

Mail:

BORN Ontario Privacy Officer

1785 Alta Vista Dr. Suite 106

Ottawa, Ont. K3G 3Y6

Fax : (613)523-9057

E-mail*: privacy@BORNOntario.ca

Signature

Your Signature: _____

Date: _____

P-33 Privacy Inquiries	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Privacy Policies and Procedures	Policy No. P-33
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario effectively manages privacy inquiries.
Policy	BORN Ontario responds to all privacy inquires, including: • Inquiries relating to the privacy policies and procedures implemented by BORN Ontario • Inquiries relating to compliance of BORN Ontario with the *Personal Health Information Protection Act, 2004* and its regulation **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with P-27: Privacy Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

Security Policies and Procedures

S-01 Information Security Policy	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-01
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario has in place a security framework to protect the Personal Health Information that it receives.
Policy	BORN Ontario securely maintains the Personal Health Information in its custody and protects the information against theft, loss and unauthorized use or disclosure, copying, modification and disposal. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

S-02 Ongoing Review of Security Policies and Procedures	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-02
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	See P-02 Ongoing Review of Privacy and Security Policies and Procedures.
Policy	
Responsibility	Privacy Officer

S-03 Ensuring Physical Security of Personal Health Information

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-03
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario provides appropriate physical security in order to protect Personal Health Information against theft, loss and unauthorized use, disclosure copying, modification or disposal.
Policy	The physical safeguards implemented by BORN Ontario to protect records of Personal Health Information include locked doors, locked filing cabinets, alarms and controlled access to premises where BORN Agents work and to secure locations within the premises where records of Personal Health Information are retained. Secure electronic devices, such as servers that store Personal Health Information, are held in protected areas with perimeters secured by entry controls that include tracked badge swipe cards or key locks, or both, to ensure that only authorized personnel are allowed access. There are three levels of access: 1. HID card access to elevator that accesses the Data Centre floor 2. HID card access to Data Centre entrance 3. Within Data Centre, access to BORN servers via key for the locked cabinet containing the servers The BORN System Hosting Provider provides a number of controls to protect the BORN System from environmental and man-made incidents including fire alarms, fire suppression (pre-action sprinkler and NOVEC 1230), HVAC redundancy, UPS redundancy, generator backup and dual power feeds. The environmental system is monitored through environmental sensors which send alerts to the physical plant and the Hosting Provider staff. When not in use, portable computers must be stored in secure locations such as a locked cabinet. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in

	accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

S-05 Secure Retention of Records of Personal Health Information

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-05
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario securely retains records of Personal Health Information in paper and electronic format.
Policy	BORN Agents are required to take steps that are reasonable in the circumstances to ensure that Personal Health Information is retained securely and is protected against theft, loss and unauthorized use or disclosure, copying, modification or disposal. Records of Personal Health Information in electronic format are retained only as long as necessary to fulfill the purpose for which the Personal Health Information is collected, to a maximum of 28 years in order to permit longitudinal analysis for the purposes of improving the provision of care to mothers, infants and children. Records of Personal Health Information held by researchers must not be retained for a period longer than set out in the research agreements. Disposal is monitored by BORN Ontario. Paper records held by BORN Ontario are only kept long enough to effect transfer to secure electronic format and are then destroyed as per S-08 Secure Disposal of Records of Personal Health Information. **Note**: This is an interim state pending full electronic adoption when there will be no collection, use or disclosure of Personal Health Information in paper format. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as

	appropriate.
Responsibility	Privacy Officer

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

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-06
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	The purpose of this Policy is to ensure that Personal Health Information stored on authorized mobile computing equipment is maintained securely and is protected against theft or loss and unauthorized use, access, copying modification, disclosure or disposal.
Policy	It is BORN Ontario policy that Personal Health Information **not** be removed from BORN Ontario secured premises for use by BORN Agents. Personal Health Information will not be stored on mobile computing equipment except in very specific and exceptional circumstances. **Mobile Computing Equipment** includes laptops, Universal Serial bus (USB) flash drives, external hard drives, CDs, DVDs and other mobile and mass storage devices as authorized in writing by the Privacy Officer. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

S-07 Secure Transfer of Records of Personal Health Information

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-07
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario securely transfers records of Personal Health Information regardless of format.
Policy	Records of Personal Health Information in electronic format must be transferred in a secure manner. Agents must use only the approved methods of transferring records of Personal Health Information in electronic format. Paper-based transfers of Personal Health Information are not permitted. Agents are not permitted to transfer Personal Health Information by fax. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Scientific Manager, Privacy Officer

S-08 Secure Disposal of Records of Personal Health Information

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-08
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario securely disposes of records of Personal Health Information in both paper and electronic format.
Policy	Records of Personal Health Information must be disposed of in a secure manner. **Disposed of in a secure manner** means that the records are destroyed in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstances. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

S-09 Passwords	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-09
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario maintains system integrity through appropriate password creation, security and administration.
Policy	Agents are required to develop and use strong passwords when accessing information systems, technologies, equipment, resources, applications and programs containing Personal Health Information, regardless of whether they are leased, owned or operated by BORN Ontario. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

S-10 System Control and Audit Logs	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-10
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario maintains system integrity through review of system control.
Policy	The access, use, modification and disclosure of Personal Health Information in the custody and control of BORN Ontario are monitored on an on-going basis. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer, Manager of Health Informatics

S-11 Patch Management

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-11
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that there are appropriate policies and procedures in place for patch management.
Policy	Software patches and other software upgrades are reviewed on an ongoing basis and implemented where appropriate in order to ensure that BORN Ontario provides a secure operational environment. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

S-12 Change Management

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-12
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure BORN Ontario has policies and procedures in place for receiving, reviewing and determining whether to approve or deny a request for a change to its operational environment.
Policy	Requests for changes to the operational environment are subject to a thorough review and approval process. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

S-13 Back-up and Recovery of Records of Personal Health Information

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-13
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN has the appropriate systems in place for the back up and recovery of records of Personal Health Information.
Policy	BORN Ontario maintains the security of records of Personal Health Information in its custody through the systematic back up and recovery of Personal Health Information in its custody. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Hosting Provider

S-14 Acceptable Use of Technology

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-14
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario Agents understand and abide by the acceptable use of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by BORN Ontario.
Policy	The following uses of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by BORN Ontario are prohibited *without exception:* • Using unencrypted mobile media such as USB keys • Removing from the premises computers containing Personal Health Information • E-mailing Personal Health Information • Faxing Personal Health Information • Attempting to gain access to any data or programs for which written authorization from the Privacy Officer does not exist • Use of information systems for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, harassment, intimidation, impersonation and computer tampering (e.g. spreading of computer viruses or other malicious software) • Creating, viewing, copying, altering, or deleting information systems data belonging to BORN Ontario without permission • Sharing information system account passwords with another person or attempting to obtain another person's information system account password. Information system accounts are only to be used by the registered user • Use of information systems in any way that violates BORN Ontario policies and procedures The following uses of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by BORN Ontario are permitted only with prior approval:

	• Use of mobile media such as USB key which contain Personal Health Information • Remote access Agents should have no expectation of privacy when using the BORN System as their activities related to Personal Health Information will be monitored. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

S-15: Security Audits	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-15
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario conducts regular security audits.
Policy	BORN Ontario conducts regular security audits to protect the security of the Personal Health Information in its custody and control. **Compliance Audit and Enforcement** Agents responsible for conducting the security audit are required to notify the Privacy Officer at the first reasonable opportunity of an information security breach or suspected information security breach as per S-17 Security Breach Management or P-29 Privacy Breach Management.
Responsibility	Privacy Officer

S-17 Security Breach Management

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Security Policies and Procedures	Policy No. S-17
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario addresses the identification, reporting, containment, notification, investigation and remediation of security breaches as defined in this policy.
Policy	A Security Breach includes: • Any act or incident in contravention of the security policies and procedures and practices implemented by BORN Ontario • Any act or incident, internal or external, that affects the confidentiality and integrity of information in the custody and control of BORN Ontario BORN Ontario requires every Agent to notify the Privacy Officer *as soon as reasonably possible*, and to do whatever is reasonably possible to contain a security breach or suspected security breach, whether internal or external, and to mitigate its effects *immediately* as per HR-01 and HR-03 Privacy and Security Training and Awareness. The Privacy Officer can be reached at: BORN Ontario Privacy Officer Suite 106-1785 Alta Vista Drive Ottawa ON K1G 3Y6 E-mail: privacy@BORNOntario.ca Phone: 613-523-3781 Fax: 613-523-9057 BORN Ontario website: www.BORNOntario.ca **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an ongoing basis by the Privacy Officer in accordance with S-15: Security Audits. Agents are required to notify the Privacy Officer at the first reasonable opportunity of a breach or suspected breach in accordance with P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

HR-01 and HR-03 Privacy and Security Training and Awareness

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Human Resources Policies and Procedures	Policy No. HR-01 and HR-03
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario Agents are provided with initial privacy and security orientation as well as ongoing privacy and security training.
Policy	Agents accessing Personal Health Information must complete an initial privacy and security orientation prior to being given access to Personal Health Information. All Agents must attend annual privacy and security training and additional training as required by the Privacy Officer. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an on-going basis by the Privacy Officer in accordance with P-27: Privacy Audits and S-15: Security Audits as appropriate. If an Agent breaches or believes there may have been a breach of this policy or procedures, the Agent must notify the Privacy Officer at the first reasonable opportunity, as per P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

HR-05 Execution of Confidentiality Agreement by Agents

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Human Resources Policies and Procedures	Policy No. HR-05
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario has all Agents sign a Confidentiality Agreement to protect the privacy, security and confidentiality of the information for which BORN is responsible.
Policy	BORN undertakes to ensure all Agents are aware of and confirm their obligations to protect the privacy and confidentiality of the Personal Health Information for which BORN is responsible. To this end, BORN Ontario Agents execute Confidentiality Agreements (as per ***Error! Reference source not found.***) at the commencement of their employment, contractual or other relationship with BORN Ontario and prior to being given access to Personal Health Information. Confidentiality Agreements are renewed annually on completion of annual privacy and security training. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an on-going basis by the Privacy Officer in accordance with P-27: Privacy Audits and S-15: Security Audits as appropriate. If an Agent breaches or believes there may have been a breach of this policy or procedures, the Agent must notify the Privacy Officer at the first reasonable opportunity, as per P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

HR-08 and HR-09 Job Description for Position(s) Delegated Day-to-Day Authority to Manage the Privacy and Security Programs

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Human Resources Policies and Procedures	Policy No. HR-08 and HR-09
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

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

DEPARTMENT: **BORN Ontario**

TITLE: **Privacy Officer** **Pay Band TBD**

Position # TBD (TBD)

REPORTS TO: The Privacy Officer will be expected to report to the Privacy and Security Review Committee on a regular basis about compliance with privacy and security policies and applicable legislation.

SUMMARY: The Privacy Officer is responsible to develop, oversee implementation and manage the BORN privacy strategy. Included is: manage BORN policies and procedures governing privacy and security, in compliance with the Personal Health Information Protection Act (PHIPA) requirements of Prescribed Registries and best practices; advance awareness of privacy and access to information programs and services; ensure processes are in place to enable knowledge and opt-out and manage privacy and access, monitoring and compliance activities.

RESPONSIBILITES:

The BORN Privacy Officer has overall responsibility for BORN privacy framework, including the following specific responsibilities:

1. **Manage the Privacy and Security Policies and Procedures**

a. Manage the development of the BORN privacy and security policies and procedures to comply with all applicable privacy legislation in Ontario, including detailed policies and procedures for specific areas of operations and activities.
b. Manage the implementation and administration of the BORN privacy and security policies and procedures to ensure that all collections, uses or disclosures of personal information comply with applicable legislation.
c. Manage, coordinate and conduct privacy and security monitoring activities.
d. Develop and deliver quarterly and annual privacy and security reports summarizing the Privacy and Security status of BORN
    i. Governance Structure
    ii. Training and Awareness
        1. Training
        2. Website
        3. Public engagement
    iii. Audits and Compliance
        1. Audits
        2. PIAs
        3. Schedules for audits and PIAs
    iv. Incident Management
        1. Breaches
        2. Complaints
        3. Inquiries
    v. Status of Recommendations
e. Coordinate, with the Legal advice as necessary, any agreements or contracts to ensure that personal information collected or processed on behalf of third parties by outside contractors is appropriately safeguarded and BORN interests are appropriately protected.

2. Build a Culture of Privacy within the organization

a. Act as the first point of contact for Privacy questions and concerns. Provide ongoing advice and guidance to other managers and employees, as required, about specific privacy issues and concerns.
b. Demonstrate privacy leadership and contribute in a significant way to the development of and continued maintenance of an environment in which employees, suppliers, contractors and others demonstrate awareness of privacy rights and obligations and act accordingly.
c. Promote awareness of privacy and access to information programs and services to internal and external stakeholders.
d. Participate as a key member of the BORN team.
e. Overall responsibility for employee training on privacy protection and for the provision of information, as required, to inform employees and others about BORN privacy policies.
f. Liaise with provincial stakeholders for the purpose of developing a high quality program in cooperation with POs in the community.
g. Monitor the external privacy environment and provide threat-risk analysis and guidance to the organization as appropriate about privacy issues that may impact upon BORN, including the status of current or future laws.
h. Develop or oversee development of communications materials, as required, for founding members, employees and others.

3. BORN Team Member

a. Monitor the external privacy environment on an ongoing basis and providing proactive advice and guidance to senior management on emerging privacy issues that could impact operations and activities.
b. Facilitate teams and committees required by Privacy Operations.
c. Coordinate and manage the interface between BORN and external organizations such as the Information and Privacy Commissioner of Ontario on any matter concerning compliance with privacy policies and legislation.
d. Work in collaboration with other program managers to ensure that program strategies are achieved.

Perform other related duties as assigned by supervisor.

Perform work in accordance with the provisions of the Children's Hospital of Eastern Ontario's Corporate Health and Safety Policies and Procedures.

A police record check is required of all potential candidates.

QUALIFICATIONS:

Education/Experience:

- University Degree in Law, Business, Administration, or Health Administration
- Masters Degree preferred
- Minimum five (5) years of related experience
- Experience working in a Privacy environment, preferably a Registry
- Experience in managing complex projects
- Computer literacy is essential. Proficient working knowledge of MS office is required
- Experience and formal training combined with demonstrated performance and ability may substitute for stipulated academic/experience requirements

Additional Competencies/Skills:

- Comprehensive use of computer technology
- Take steps to ensure timely completion of tasks by adjusting priorities as required
- Communicate effectively and concisely, both orally and in writing
- Deal effectively with internal and external partners
- Excellent presentation, teaching and group facilitation skills
- Evidence of sound change management skills with proven project management ability
- Working knowledge of applicable occupational health and safety legislation; general knowledge of corporate/departmental policies and procedures related to health and safety

EFFORT:

- Demand on energy as a result of lack of control over work

- Fatigue resulting from a very high degree of concentrated visual attention, focused thinking/analysis and a regular requirement to meet emergency or unexpected important deadlines

WORKING CONDITIONS:

- Travel within Ontario required; occasional national/international travel required
- Minor exposure to disagreeable conditions (e.g. lack of privacy, frequent interruptions)

Updated March 27, 2011

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

DEPARTMENT: **BORN Ontario**

TITLE: **Manager of Health Informatics** **Pay Band 4.3**

Position # 7257 (FT)

REPORTS TO: Director, BORN Ontario

SUMMARY: The Manager of health informatics is responsible for the development and maintenance of the technology systems required to deliver the knowledge required for the best possible beginnings for lifelong health. Responsible for the database architecture; application functionality; management of the technical support function; maintaining the vendor and hosting relationships; and providing relevant consulting services to various members as new data sources join BORN. The Manager of Health Informatics is also responsible for developing and monitoring operating budgets specific to the technology related to the BORN program, and for managing the human resources of the department including hiring, termination and managing the performance of staff as necessary.

RESPONSIBILITES:

4. Manage the technology

a. Define product specifications including the data, reporting and functionality of the BORN technology system.
b. Manage and approve all changes regarding the design, development, installation, documentation, testing, security, and maintenance of the BORN

technology system.

c. Work with a variety of hardware and application vendors to ensure that the system meets or exceeds user requirements.
d. Coordinate all technology activities to minimize any operational disruptions.
e. Provide technical evaluations and advise when new member data are being integrated.
f. Monitor vendor's adherence to specifications, quality and effectiveness of vendor support.

5. Represent BORN technology

a. Work with stakeholders and users to ensure the technology system is integrated with clinical and administrative processes.
b. Translate user needs into technology requirements.
c. Represent the program by participating in and presenting at meetings that focus on technology initiatives that may benefit BORN (e.g., Ottawa Centre for Research and Innovation).
d. Represent the interests of BORN and/or the Hospital by establishing networks and building partnerships.
e. Liaise with members and provincial stakeholders for the purpose of developing further data integration opportunities with other programs in the community.

6. Privacy Responsibilities

a. Member of the BORN Privacy and Security Review Committee.
b. Adhere to, represent and champion the BORN Privacy and Security Management Plan.
c. Build a culture of Privacy within BORN.
d. Manage physical access to PHI.
e. Execution of security audits.

7. BORN Team Member

a. Keep current with emerging technologies by consulting suppliers and technical documents.
b. Facilitate teams and committees required throughout technology development
c. Lead the planning, development, deployment, operation and maintenance of a technology work plan, resources and services consistent with the programs goals and priorities.
d. Understand the impacts of technology decisions on and of the broader environment – Privacy, Security, Ministry, Science, Policy.
e. Work in collaboration with other program managers to ensure that program strategies are achieved.

8. Management responsibilities

a. Responsible for developing and monitoring operating budgets, and for managing the human resources including hiring, termination and managing the performance of staff as necessary.

Perform other related duties as assigned by supervisor.

Perform work in accordance with the provisions of the Children's Hospital of Eastern Ontario's Corporate Health and Safety Policies and Procedures.

A police record check is required of all potential candidates.

QUALIFICATIONS:

Education/Experience:

- University Degree in Business, Administration, or Health Administration
- Masters Degree preferred
- Minimum five (5) years of related experience
- Experience working in a complex IT environment
- Experience in managing complex projects
- Computer literacy is essential. Proficient working knowledge of MS office is required
- Experience and formal training combined with demonstrated performance and ability may substitute for stipulated academic/experience requirements

Additional Competencies/Skills:

- Comprehensive use computer technology
- Take steps to ensure timely completion of tasks by adjusting priorities as required
- Communicate effectively and concisely, both orally and in writing
- Deal effectively with internal and external customers
- Excellent presentation, teaching and group facilitation skills
- Evidence of sound change management skills with proven project management ability
- Working knowledge of applicable occupational health and safety legislation; general knowledge of corporate/departmental policies and procedures related to health and safety

EFFORT:

- Demand on energy as a result of lack of control over work
- Fatigue resulting from a very high degree of concentrated visual attention, focused thinking/analysis and a regular requirement to meet emergency or unexpected important deadlines

WORKING CONDITIONS:

- Travel within Ontario required; occasional national/international travel required
- Minor exposure to disagreeable conditions (e.g. lack of privacy, frequent interruptions)

Updated March 27, 2011

HR-10: Termination or Cessation of the Employment or Contractual Relationship

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Human Resources Policies and Procedures	Policy No. HR-10
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To identify the BORN Ontario policy and procedures related to termination or cessation of employment or contractual relationship.
Policy	All BORN Ontario policies for voluntary and involuntary termination or cessation of the employment or contractual relationship are in alignment with Children's Hospital of Eastern Ontario (CHEO) Human Resources policies and requirements, and are in full compliance with current employment legislation. Agents must securely return all property on or before the date of termination of employment. Property includes records of Personal Health Information, identification cards, access cards, credit cards, computer equipment, books, materials, cell phones and mobile devices, keys and any other CHEO or BORN Ontario owned items as identified **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an on-going basis by the Privacy Officer in accordance with P-27: Privacy Audits and S-15: Security Audits as appropriate. If an Agent breaches or believes there may have been a breach of this policy or procedures, the Agent must notify the Privacy Officer at the first reasonable opportunity, as per P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	BORN Ontario Privacy Officer

HR-11: Discipline and Corrective Action	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Human Resources Policies and Procedures	Policy No. HR-11
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To identify the BORN Ontario policy and procedures for employee disciplinary and corrective action in respect of Personal Health Information.
Policy	BORN Ontario Agents must execute a BORN Ontario Confidentiality Agreement in accordance with ***Error! Reference source not found.*** at the commencement of their employment, contractual or other relationship with BORN Ontario and prior to being given access to Personal Health Information. 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. **Whistle Blower Protection** BORN Ontario Agents are protected from actions taken against them simply for reporting breaches or suspected breaches unless those reports are made in a frivolous or vexatious manner.
Responsibility	BORN Ontario Privacy Officer

O-01 and O-02 Privacy and Security Governance and Accountability Framework

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Organizational and Other Policies and Procedures	Policy No. O-01 and O-02
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	That BORN Ontario has a privacy and security governance and accountability framework in place to ensure compliance with the *Personal Health Information Protection Act, 2004* and its regulations, and to ensure compliance with BORN Ontario privacy policies and procedures.
Policy	Agents are required to comply with the BORN Ontario privacy and security governance and accountability framework. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an on-going basis by the Privacy Officer in accordance with P-27: Privacy Audits and S-15: Security Audits as appropriate. If an Agent breaches or believes there may have been a breach of this policy or procedures, the Agent must notify the Privacy Officer at the first reasonable opportunity, as per P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

O-04 Corporate Risk Management Framework

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Organizational and Other Policies and Procedures	Policy No. O-04
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario has a comprehensive and integrated corporate risk management framework in place.
Policy	BORN Ontario implements a corporate risk management framework to identify, assess, mitigate and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose Personal Health Information is received and to maintain the confidentiality of that information. All risks identified through the BORN Privacy & Security policies and procedures will be assessed using the framework including those identified through audits, PIA's and breach incidents.
Responsibility	Privacy and Security Review Committee

O-06 Maintaining a Consolidated Log of Recommendations

Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Organizational and Other Policies and Procedures	Policy No. O-06
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	To ensure that BORN Ontario maintains a consolidated log of recommendations.
Policy	BORN Ontario maintains a consolidated and centralized log of all privacy and security related recommendations. The log will be updated within a week of recommendations being received, and will be reviewed as required, at a minimum monthly. **Compliance Audit and Enforcement** BORN Ontario Agents must comply with this policy and procedures. Compliance is audited on an on-going basis by the Privacy Officer in accordance with P-27: Privacy Audits and S-15: Security Audits as appropriate. If an Agent breaches or believes there may have been a breach of this policy or procedures, the Agent must notify the Privacy Officer at the first reasonable opportunity, as per P-29 Privacy Breach Management or S-17 Security Breach Management as appropriate.
Responsibility	Privacy Officer

O-08 Business Continuity and Disaster Recovery Plan	
Manual/Section: BORN Ontario Privacy and Security Policies and Procedures/Organizational and Other Policies and Procedures	Policy No. O-08
Reviewed by/on: Privacy and Security Review Committee on April 11, 2011	

Purpose	BORN Ontario is working with CHEO and the BORN System Hosting Provider to develop a robust business continuity and disaster recovery plan that provides effective prevention and recovery procedures in the event of an incident.
Policy	
Responsibility	

Appendix A – Who's Who at BORN Ontario (Roles)

As of March 31st, 2011 the individuals with the responsibilities outlined in the document above are outlined here:

Role	Individual
BORN Privacy Officer	Pranesh Chakraborty
BORN Scientific Manager	Ann Sprague
BORN Scientific Director	Mark Walker
BORN Medical Director	Pranesh Chakraborty
BORN Executive Lead	Susan Richardson
BORN Director	Mari Teitelbaum (Acting)
BORN Manager of Health Informatics	Vacant (Mari Teitelbaum)
BORN Privacy Administrator	Joan Mongeon
BORN Quality Management Specialist	Barbara Chapman
BORN System Administrator	Barb Chapman (Acting)
BORN Communications Lead	Brittan Fell
CHEO Privacy Officer	Tyson Roffey