



eCHN Privacy Policy

Document Identification Table

Department: Privacy Office	
Posting Date: November 9, 2018	Document Number: PSO - 100
Document Classification: Public	
Approved By: Privacy & Security Leadership Committee	Date of Approval: November 6, 2018
Date of Next Review: November 9, 2019	Version: 6.0
Document path: http://seraph.echn.ca/policyandprocedure/Policy%20Documents/Forms/AllItems.aspx	

Table of Contents

1. Objective	3
2. Scope	3
3. The electronic Child Health Network	3
3.1. Services	3
3.2. Reporting Obligations	4
4. Personal Health Information Protection Act, 2004	4
4.1. Health Information Custodian	4
4.2. PHIPA Agent	4
4.3. Health Information Network Provider	5
5. Fair Information Practices	5
6. Personal Health Information at eCHN	5
6.1. Accountability for Personal Health Information	5
6.1.1. <i>Organizational Accountability</i>	5
6.1.2. <i>Policies and Procedures</i>	6
6.1.3. <i>Breach and Incident Management</i>	6
6.1.4. <i>Training and Awareness</i>	6
6.1.5. <i>Agreements</i>	7
6.2. Identifying the Purpose for the Collection of Personal Health Information.....	7
6.3. Consent for the Collection, Use and Disclosure of Personal Health Information.....	8



6.4.	Limiting Collection of Personal Health Information.....	8
6.5.	Limiting Use, Disclosure and Retention of Personal Health Information	9
6.5.1.	<i>eCHN Use of Personal Health Information</i>	<i>9</i>
6.5.2.	<i>eCHN Disclosure of Personal Health Information</i>	<i>9</i>
6.5.3.	<i>eCHN Retention of Personal Health Information.....</i>	<i>10</i>
6.6.	Accuracy of Personal Health Information.....	10
6.7.	Safeguards for Personal Health Information	11
6.7.1.	<i>Assessing Privacy Risk at eCHN</i>	<i>11</i>
6.8.	Openness about the Management of Personal Health Information	12
6.9.	Individual Access and Amendment of Personal Health Information.....	12
6.10.	Challenging Compliance.....	13
7.	Compliance	14
8.	Terms & Definitions.....	14
9.	References and Associated Documents	16
10.	Version Table.....	16

1. Objective

The Ontario privacy legislation, the *Personal Health Information Protection Act, 2004* (PHIPA), establishes rules concerning the collection, use and disclosure of Personal Health Information by Health Information Custodians and those persons that provide services to support the delivery of health care services.

The purpose of the eCHN Privacy Policy is to outline the privacy practices undertaken by eCHN for the collection, use and disclosure of the Personal Health Information stored and managed by eCHN.

2. Scope

This Privacy Policy is applicable to all eCHN employees, contractors, vendors, healthcare partners and eCHN Clients that use the eCHN Portal or those that support operations for the various eCHN services.

3. The electronic Child Health Network

The electronic Child Health Network (eCHN) was established in 1997 as a not-for profit, government funded organization, dedicated to using modern technology to promote the sharing of pediatric health data, information and knowledge among health care providers. It is designed to deliver a communication infrastructure which supports children's health services in Ontario.

eCHN assembles data that it receives from Data Contributing Clients, as a result of pediatric patients' interactions with the health care system, in the form of a single, longitudinal, medical chart. eCHN maintains key areas of information, such as: admission, discharge and transfer data; lab reports; clinic notes; consultant's letters and surgical notes; X-ray images and reports.

eCHN is founded on the principle that up-to date, accurate and comprehensive patient information is exchanged in a secure and portable manner to assist with timely medical decision-making.

3.1. Services

eCHN Provides the following services

WebChart – an electronic health record (EHR), which is used to facilitate the sharing of pediatric patient data from Health Information Custodian contributors to authorized users, through the eCHN System.

e-Referral – allows licensed healthcare practitioners and their support staff to seamlessly access the external electronic referral applications of authorized eCHN Clients directly from the eCHN Portal using Single Sign-On functionality.

Diabetes Dashboard – a tool which provides a consolidated view of clinically relevant data available within the eCHN Portal, including associated indicators for clinical decision-making. In addition, the Diabetes Dashboard integrates alerts of required clinical events according to Canadian and local best-practice guidelines and facilitates graphical representation of information.

POGO Shuttle Sheet – a tool which provides seamless coordination of visits to Pediatric Oncology Group of Ontario (“POGO”) treatment sites between various professionals working with cancer patients, including historical visit details when required.

3.2. Reporting Obligations

eCHN, as a government-funded organization, has mandatory reporting obligations to the Ministry of Health and Long-Term Care. eCHN may use the business information of eCHN users and de-identified patient keys to generate aggregated reports and statistics for internal reporting functions and to fulfil its mandatory reporting obligations. eCHN does not collect, use or disclose Personal Health Information as part of these reporting obligations.

4. Personal Health Information Protection Act, 2004

The *Personal Health Information Protection Act, 2004* (PHIPA) establishes rules concerning the collection, use and disclosure of Personal Health Information by Health Information Custodians, agents of those Custodians, and other persons prescribed in the legislation. The Act was developed to balance the privacy rights of individuals with the need for the effective provision of health care.

4.1. Health Information Custodian

In general, health care organizations, individual health care practitioners or other entities which are prescribed in PHIPA¹ are defined as Health Information Custodians in respect of Personal Health Information within their custody and control. Health Information Custodians that participate in eCHN include:

- Hospitals
- Local Health Integration Networks
- Group based health care practices (e.g. Children’s Treatment Centres, Family Health Teams, etc.)
- Public Health Units
- Independent health care practitioner offices
- Ministry of Health and Long-Term Care (as the custodian of the Ontario Laboratories Information System)

4.2. PHIPA Agent

In relation to Personal Health Information within the custody and control of a Health Information Custodian, a PHIPA agent² may be a person or organization that:

- Acts on behalf of a Health Information Custodian
- With the authorization of the Health Information Custodian

¹ PHIPA, s.3(1)

² PHIPA, s.2

- For the purpose of the Health Information Custodian.

eCHN acts as an “agent” for each Health Information Custodian that contributes patient data to eCHN for the relevant services.

4.3. Health Information Network Provider

eCHN provides and maintains an electronic communications platform which allows health care providers to securely disclose Personal Health Information to one another, specifically for the provision of care to pediatric patients. eCHN operates these electronic services as a “Health Information Network Provider”³.

5. Fair Information Practices

eCHN complies with the requirements and spirit of PHIPA and aligns its privacy practices with the ten *Fair Information Principles* outlined in the *Model Code for the Protection of Personal Information* (CSA Model Code). eCHN applies the CSA Model Code through its commitment to:

- **Accountability** for Personal Health Information
- Identifying the **Purpose** for the collection of Personal Health Information
- **Consent** for the collection, use and disclosure of Personal Health Information
- Limiting the **Collection** of Personal Health Information
- Limiting the **Use, Disclosure and Retention** of Personal Health Information
- **Accuracy** of Personal Health Information
- **Safeguards** for Personal Health Information
- **Openness** about the management of Personal Health Information
- **Individual Access** and amendment of Personal Health Information
- Ensuring that individuals have the right to **Challenge Compliance** practices at eCHN

6. Personal Health Information at eCHN

6.1. Accountability for Personal Health Information

6.1.1. Organizational Accountability

eCHN is committed to safeguarding and handling the Personal Health Information in the eCHN system in compliance with PHIPA and its accompanying regulation. Overall accountability for eCHN compliance with its privacy obligations rests with the eCHN Board of Directors. The Director of eCHN is responsible for reporting all privacy and security matters to the eCHN Board of Directors

Day-to-day oversight of privacy is delegated to the eCHN Privacy Office, which is responsible for providing leadership on all privacy matters that effect the organization. The eCHN Privacy Office aligns

³ O.Reg. 329/04, s.6(2)

privacy compliance efforts with the eCHN Security Office. This coordinated effort ensures a holistic approach to the protection and management of Personal Health Information at eCHN.

The eCHN Privacy Office and the eCHN Security Office oversee:

- Day-to day privacy compliance
- The development and maintenance of privacy and security policies as well as operational procedures
- Breach and incident management
- Privacy and security risk management activities
- Privacy and security awareness training of all eCHN personnel

eCHN has also appointed a Privacy and Security Leadership Committee to ensure alignment of the privacy framework with eCHN business objectives and to provide governance and oversight for the eCHN Privacy Office and eCHN Security Office. The Privacy and Security Leadership Committee reviews information handling and data safeguards, approves privacy and security related artefacts (such as Privacy Impact Assessments, Threat and Risk Assessments and resulting Risk Treatment Plans), and approves new privacy and security policies.

6.1.2.Policies and Procedures

eCHN has developed a comprehensive set of privacy and security policies which outline the rules and guiding principles by which eCHN ensures compliance with PHIPA and fair information practices, as found in the CSA Model Code.

A suite of procedures has been operationalized throughout the organization for the collection, use, disclosure, security and retention of Personal Health Information in paper and electronic form. These governing documents for privacy and security are updated according to internal review schedules.

6.1.3.Breach and Incident Management

An eCHN Privacy Incident Management Procedure and an eCHN Security Incident Management Procedure are in place to outline the required steps where a privacy risk, potential breach or breach has been identified. These procedures define how to identify, contain, report, investigate and escalate incidents and breaches.

6.1.4.Training and Awareness

Privacy and security training of all new personnel is conducted as a part of onboarding activities at eCHN and in accordance with the *eCHN Privacy & Security Training Policy and Procedure*. eCHN also provides an annual privacy and security training refresher to staff and a review of the confidentiality responsibilities they assume when managing patient information.



6.1.5. Agreements

Client, User and Other Contributing Health Information Custodian Agreements

eCHN enters into a written agreement with each Health Information Custodian that is contributing and/or accessing Personal Health Information from the eCHN system. An eCHN application form must be completed by each Health Information Custodian registering as an eCHN Client

Each individual user of a registered Client must request access to the eCHN system by completing and submitting the relevant access application form. All users must be authorized by the sponsoring Health Information Custodian Client and undergo an eCHN validation process before gaining access to eCHN.

Vendor Agreements

Vendors of eCHN that have access to Personal Health Information must agree to adhere to the privacy and security terms outlined within third party agreements. These agreements require that vendors manage and secure the Personal Health Information to which they have been given access, in a manner that meets industry best practices and allows eCHN to comply with its PHIPA obligations.

eCHN Personnel Agreements

All eCHN personnel are required to sign a Non-Disclosure Agreement and must abide by eCHN's policies and procedures, including eCHN's privacy and security policies, as conditions of their employment or other engagement / provision of services to eCHN.

6.2. Identifying the Purpose for the Collection of Personal Health Information

Before any Personal Health Information is shared with eCHN, and before it becomes available for consumption by authorized users on the eCHN Portal, the contributing Health Information Custodian and eCHN will outline the purpose and scope for the sharing of patient data within a set of formalized documents. The primary purpose for the transmission of data from a contributing Health Information Custodian to eCHN is to facilitate the delivery of the electronic services defined in section 3.1 of this Policy. eCHN does not use the Personal Health Information from contributing Clients for any other purpose than to fulfill its obligation to those Clients, in relation to the services.

Documenting the purpose for which eCHN receives Personal Health Information allows eCHN and the Health Information Custodian Client to determine the type and amount of information necessary for transfer, to fulfill the identified purpose.

eCHN does not directly collect Personal Health Information from the patient but rather accepts an electronic copy of the patient record from the Health Information Custodian. eCHN may make corrections to minor errors in data to preserve data quality and integrity. eCHN consults with the contributing Health Information Custodian to confirm all changes. At all times, the Health Information Custodian remains in possession of the original patient health record, with eCHN storing a copy of the custodian record in the eCHN system.

In the context of eCHN eReferral, eCHN may transmit a patient identifier (e.g. health card number) to eCHN eReferral Clients. The patient identifier is transmitted for the sole purpose of facilitating a referral for that patient to the eCHN eReferral Client, when the referral is initiated by an authorized eCHN user.

Notwithstanding eCHN's *Reporting Obligations*, as outlined in section 3.2, data from the eCHN system is not to be used for research or any secondary purposes. The eCHN Terms and Conditions prohibit use of patient data from the eCHN system for research purposes.

6.3. Consent for the Collection, Use and Disclosure of Personal Health Information

The Health Information Custodian, as the owner of contributed Personal Health Information, will determine the preferred consent method (express or implied) that is applied by the custodian organization. Each Health Information Custodian that contributes Personal Health Information to eCHN must fully comply with any consent directive expressly given by their patient with respect to the contributed Personal Health Information.

Patients who wish to revoke consent, or reinstate previously withdrawn consent, must make their consent request to the relevant contributing Health Information Custodian. eCHN provides a tool for contributing health information custodians to record patient consent directives in the eCHN system. Once notified by the contributing Health Information Custodian, eCHN will process all consent withdrawals or reactivations in a timely manner. Additionally, eCHN will permanently retain an audit log of all consent status changes requested from a Health Information Custodian.

eCHN recommends that each Health Information Custodian discuss and inform individuals of the implications of consent withdrawal and/or reinstatement.

Emergency Access

A locked patient record or chart can be overridden in the WebChart application in two situations:

- By a physician user in the case of an emergency which requires access to the restricted information to reduce a significant risk of serious bodily harm to the patient⁴, or
- By a physician user in the case where a patient or substitute decision-maker (i.e. parent or legal guardian) has given express consent to override a previously applied access restriction.

A consent override by any physician will trigger an immediate notification to the eCHN Privacy Office and a subsequent audit of the circumstances for the override. Emergency override audits will be conducted in cooperation with the Privacy Officer from the site where the event occurred.

6.4. Limiting Collection of Personal Health Information

eCHN receives only that Personal Health Information necessary to fulfill its responsibilities as a PHIPA Agent of the relevant contributing Health Information custodian. Each Health Information Custodian

⁴ PHIPA section 40(1)



that contributes data to the eCHN system determines which Personal Health Information is submitted to eCHN.

6.5. Limiting Use, Disclosure and Retention of Personal Health Information

6.5.1. eCHN Use of Personal Health Information

eCHN does not use Personal Health Information for purposes other than those which are noted in the *eCHN Terms and Conditions*, the *eCHN Portal Access Application Form* and any formalized services documentation developed with each contributing Client.

6.5.2. eCHN Disclosure of Personal Health Information

As a Health Information Network Provider, eCHN supplies its Clients with services that allow Health Information Custodians to disclose Personal Health Information with one another. eCHN will not disclose any Personal Health Information for its own purpose or for any secondary purpose, unless required by law. Furthermore, Personal Health Information from the eCHN system is not available to any government body or insurance company.

eCHN shall provide access to Personal Health Information contained in the eCHN system to authorized Health Information Custodian users and their agents in accordance with the *eCHN Terms and Conditions*.

All access to the eCHN Portal is logged and such logs are retained permanently. User access logs are made available to Privacy Officers from Health Information Custodian organizations via the eCHN Audit Reporter tool. The eCHN Audit Reporter tool allows appointed users from a Client organization to conduct their own user audits. The eCHN Audit Reporter tool provides information on all access to patient information, including the name of the user(s) that accessed patient data along with the date and time of the access.

Personal Health Information in the eCHN system is not to be accessed, viewed, collected, used or disclosed for research purposes. All eCHN users are advised in the *eCHN Portal Access Application Form* and in the *eCHN Terms and Conditions* that they must not use any data from the eCHN system for research purposes. Each user must agree to provisions in the application form and Terms and Conditions, prior to gaining access to the eCHN system.

In cases where eCHN has identified that there has been an unauthorized access, collection, use or disclosure of the Personal Health Information in the eCHN system, eCHN will notify the appropriate Health Information Custodian(s) in accordance with the *eCHN Privacy Incident Management Procedure* and/or the *eCHN Security Incident Management Procedure*.

6.5.3. eCHN Retention of Personal Health Information

The eCHN System is not intended to be a long-term archive for patient data. Data may be purged from the eCHN system from time-to-time, in accordance with the *eCHN Retention of PHI Policy* for Personal Health Information.

6.6. Accuracy of Personal Health Information

Participation in the eCHN program/service is voluntary for Health Information Custodians in Ontario. eCHN Health Information Custodian Clients that contribute Personal Health Information to the eCHN system will identify which patient records to provide to eCHN. Clients that do not contribute data to the eCHN repository may authorize their registered users to view patient data from the system for the permitted purpose. As contributing sites determine which data they share with eCHN, and since patients in Ontario may receive care at contributing and non-contributing facilities, eCHN advises its users that the data available in the eCHN applications may not be a complete patient health record.

Patients can request, and eCHN may provide (upon verification of the requestor), a list of Health Information Custodians that have transferred a patient's Personal Health Information to the eCHN system. In order to initiate such a request, a requestor must complete the [eCHN PHI Inquiry Form](#) found on the eCHN public website.

Any inquiries regarding accuracy of Personal Health Information held in the eCHN system are directed to the relevant contributing Health Information Custodian for correction. eCHN updates Personal Health Information in the eCHN system as received from the contributing Health Information Custodian.

eCHN uses quality assurance processes, data analysis tools and data coding standards to facilitate the transfer, use and quality control of the Personal Health Information it receives. Health Information Custodians are responsible for ensuring the data they provide to eCHN is accurate, complete and up-to-date for the purposes specified. At times, eCHN may make corrections to minor errors in data to preserve data quality and integrity. eCHN collaborates with the contributing Health Information Custodian with respect to all changes.

As it relates specifically to eCHN WebChart services, data standardization⁵ may be applied by eCHN to data received from the contributing Health Information Custodian. It is the responsibility of the contributing Health Information Custodian to confirm and approve any mapping and standardization applied by eCHN. The standardized data remains under the ownership of the original contributing Health Information Custodian. For referential integrity and traceability, eCHN allows the original (as received) data to be accessible for viewing on the WebChart application.

⁵ LOINC: Logical Observation Identifiers Names and Code as updated.

6.7. Safeguards for Personal Health Information

Security safeguards appropriate to the quantity and sensitivity of the Personal Health Information on the eCHN system are in place to protect patient data from theft or loss, as well as unauthorized access, disclosure, copying or modification. eCHN implements privacy and security controls for the appropriate handling of Personal Health Information regardless of the format in which it is held (i.e. paper or electronic records).

The nature of the safeguards will depend on the sensitivity of the information, the amount of data, the distribution or audience for the data, along with the format and the method of storage for the data. Higher levels of safeguards are applied for more sensitive information.

eCHN identifies and applies administrative, technical and physical security controls from the point of data receipt up to the point of data access by users, or to the point of data destruction for Personal Health Information which is to be purged.

General administrative, technical and physical security controls employed by eCHN for the management of Personal Health Information are noted on the following page <http://www.echn.ca/privacy-safeguards.php> on the eCHN public website.

6.7.1. Assessing Privacy Risk at eCHN

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) assesses and identifies privacy risks and the level of privacy compliance with eCHN policy and legal requirements for an identified program or system. eCHN executes a PIA for all new programs or existing programs where there is a relevant change in the program that impacts privacy compliance and risk. PIAs are developed in accordance with the eCHN Privacy and Security Risk Management Procedure.

Threat and Risk Assessment

A Threat and Risk Assessment (TRA) of the eCHN system identifies the risks associated with the confidentiality, integrity and availability of all data, including Personal Health Information, which is managed and maintained on the eCHN system. eCHN conducts TRAs for new program initiatives and when a significant change is proposed for the eCHN architecture. TRAs are developed in compliance with the eCHN Security Policy and the eCHN Privacy and Security Risk Management Procedure.

Risk Treatment

A critical element of a PIA and TRA is the identification of risks and recommendations and the subsequent treatment of those risks. eCHN documents and monitors risk treatment activities in accordance with its eCHN Privacy and Security Risk Management Procedure.

eCHN will provide to Health Information Custodian Clients, upon request, the summary of any relevant security and privacy assessments conducted on the eCHN services.

6.8. Openness about the Management of Personal Health Information

eCHN makes information about its policies and practices with respect to the management of Personal Health Information readily available to the public. The [eCHN website](#) provides the public with the following general information:

- An overview of eCHN
- A list of Clients and services
- The types of data collected by eCHN
- The eCHN Architecture and Safeguards which are in place to manage PHI
- The eCHN Privacy Policy
- Contact information for the eCHN Privacy and Security Offices
- Instructions on how to make an access request

Additional information on the eCHN privacy program can also be requested from the eCHN Privacy Office at privacy@echn.ca.

6.9. Individual Access and Amendment of Personal Health Information

PHIPA provides individuals with a right of access to their Personal Health Information which is in the custody or under the control of a custodian. eCHN acknowledges individuals' right of access and has implemented procedures to support individuals in making a request for access.

In order to initiate a request for access, an individual must complete the [eCHN PHI Inquiry Form](#) found on the eCHN public website. A requestor is required to provide sufficient information to permit eCHN to validate their identity as a patient, a parent, a guardian or a substitute decision-maker. The requestor will be required to provide any additional details necessary to confirm their association to a patient within the eCHN system. The information provided by the requestor is not used for any other purpose than to verify the requestors' identity and respond to the access request. eCHN responds to each request as soon as possible but no later than 30 days after receiving the request.

In processing an access request, eCHN may:

- Inform the requestor of the existence of the patient's health information in the eCHN system
- Identify which Health Information Custodian(s) contributed the patient's information to eCHN.

When an individual requires additional details about their records, challenges the accuracy and completeness of the Personal Health Information within those records, and/or requests to have it amended, eCHN refers the individual to the contributing Health Information Custodian(s) to make any necessary amendments.

Any updates to a patient record(s) are communicated to eCHN with the regularly scheduled data transmission from the data-contributing Health Information Custodian. Upon processing the data

transmission, the corrected copy of the patient record within the eCHN system is automatically updated.

6.10. Challenging Compliance

eCHN is committed to protecting the privacy of Personal Health Information within its custody or control, as required by Ontario's *Personal Health Information Protection Act, 2004*.

Any individual concerned with the privacy practices of eCHN can make an inquiry and/or register a complaint to the Director of eCHN and/or to the eCHN Privacy Office.

For further information about this policy, eCHN's privacy practices, or safeguards at eCHN, please contact the eCHN Privacy Office. All inquiries should be made in writing and be directed to eCHN by:

Mail: Electronic Child Health Network (eCHN)
180 Dundas Street West, Suite 2405
Toronto, Ontario M5G 1Z8

Phone: (416) 813-8807

Fax: (416) 813-8294

Email: echnmail@echn.ca

Website: www.echn.ca

An inquiry can also be made by completing and submitting the [eCHN Privacy Complaint Form](#) available on the eCHN public website.

All complaints and inquiries are responded to promptly and in accordance with eCHN's complaint procedures. Follow-up actions and updates to eCHN practices will be taken where required.

If an individual is not satisfied with the response from eCHN, the individual has the right to direct their concerns to the Information and Privacy Commissioner of Ontario.

The Ontario Privacy Commissioner's Office may be reached by:

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

Phone: 416-326-3948

Website: www.ipc.on.ca

7. Compliance

Those persons identified in the “Scope” section of this document are required to comply with this policy and any other supporting procedures related to safeguarding and proper handling of Personal Health Information at eCHN. In the event of non-compliance with this policy, appropriate action will be taken and may include removal of access rights to Personal Health Information on the eCHN system, termination of eCHN user accounts, and disciplinary action and up to and including termination of employment / provision of services to eCHN.

8. Terms & Definitions

Term User in this Document	Acronym	Definition
Agent	n/a	As defined in PHIPA section 2: <i>“agent”, in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent’s own purposes...”</i>
Client	n/a	A health information custodian who has executed (by signing and/or clicking through) an agreement referencing and binding such Client and its users to comply with the eCHN Terms and Conditions.
Contributing Health Information Custodian		Health information custodian clients: <ul style="list-style-type: none"> - Are organizations whose systems are integrated with eCHN to transmit patient records to eCHN for standardization and posting in the WebChart EHR; or - Use eCHN services for the transmission of patient records to other health information custodians that provide health care services to that patient.
CSA Model Code for the Protection of Personal Information	n/a	The ten principles set out by the Canadian Standards Association that balance the privacy rights of individuals and the information needs of organizations within a “Model Code”.
eCHN Portal	n/a	The network accessible portal used to provide Clients and their users with access to the eCHN System
eCHN Portal User	n/a	An individual who has been authorized by a Client to access the eCHN System, for the relevant services, as the Client’s PHIPA Agent on behalf of the Client. For clarity, the term user also

		applies to a Client who is an individual health information custodian utilizing the eCHN System
eCHN Services	n/a	The Services listed in the “ <i>Background</i> ” section of this Privacy Policy.
eCHN System	n/a	The electronic system used by eCHN to provide the eCHN Services and includes the eCHN Portal.
Electronic Child Health Network	eCHN	Established in 1997 as a not-for profit, government funded organization to deliver the eCHN Portal services.
Health Information Custodian	HIC	A person or organization who has custody or control of PHI as a result of, or in connection with, the person’s or organization’s powers or duties; as defined in section 3 of PHIPA. Some Examples of Health Information Custodians which are users of the eCHN Portal are hospitals, CCAC’s, Independent Physician Offices and Children’s Treatment Centres.
Health Information Network Provider	HINP	As defined in the regulation which accompanies PHIPA, O. Reg. 329/04 section 6(2): <i>“...means a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an</i>
Personal Health Information	PHI	As defined in PHIPA ⁶ . <i>In general PHI is identifying information along with any information about health care status or history for an individual. The information can be in oral or recorded form.</i>
<i>Personal Health Information Protection Act, 2004</i>	PHIPA	The <i>Personal Health Information Protection Act, 2004</i> is the Ontario health privacy statute which governs the manner in which personal health information may be collected, used and disclosed within the health care system.

⁶ PHIPA 2004, section 4(1)



9. References and Associated Documents

- *Personal Health Information Protection Act, 2004*
- eCHN Privacy Incident Management Procedure
- eCHN Security Incident Management Procedure
- eCHN Acceptable Use Policy
- eCHN Non-Disclosure Agreement
- eCHN Confidentiality Policy for eCHN Portal Users
- Governing Principles for eCHN PHI Management
- eCHN Security Policy
- PHI Enquiry Policy
- Destruction of PHI Procedure
- Consent Management Procedure
- Procedure for the Management of Lost and Found eCHN Reports
- Retention of PHI
- eCHN Demo Patient Policy
- eCHN Email Policy
- eCHN Password Policy

10. Version Table

Version	Date	Author	Reviewer	Change Description
4.2	November 19, 2015	S. Petrelli		Revisions to Privacy Policy to align with new eCHN Terms and Conditions.
5.0	February 2, 2016	S. Petrelli		Finalize and submit draft revision for legal review.
5.1	February 18, 2016	S. Petrelli		Full revision of the Privacy Policy.
5.2	February 24, 2016	S. Petrelli		Minor updates
5.3	March 9, 2016	S. Petrelli		Revisions based on feedback from R. Dhami.
5.4	June 3, 2016	E. Renz		Revisions based on feedback re. consent mgt content
5.5	August 22, 2016	E. Renz		Revisions with respect to wording around data modification/correction
5.6	September 18, 2017	E. Renz	J. Forsyth	Revisions based on recommendations from project PIAs. Additional minor edits as



				needed to ensure that the policy is up-to-date.
5.7	October 3, 2017	E. Renz	R. Dhami	Incorporated edits and feedback from J. Forsyth
5.8	June 1, 2018	E. Renz	R. Dhami	Revisions based on recommendations from project PIAs and to ensure the accuracy of descriptions detailing eCHN's consent management practices.
5.9	June 15, 2018	E. Renz	N. Remtulla and A. Leahy	Additional revisions to consent management sections and additional revisions made to services descriptions.
6.0	November 11, 2018	E. Renz	N. Remtulla	Accepted and finalized all revisions and changes.