eCHN Privacy Policy

Document Identification Table

Department: Privacy and Security Office	
Posting Date: April 25, 2016	**Document Number:** PSO - 100
Document Classification: Public	
Approved By: R. Dhami	**Date of Approval:** March 7, 2016
Date of Next Review: February 28, 2017	**Version:** 5.5

Table of Contents

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 managed by the organization.

2. Scope

This Privacy Policy is applicable to all eCHN employees, contractors, vendors, healthcare partners and participating member (hereafter call "client" in this policy) site 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 pulls together the data resulting from your child's interactions with the health care system in the consolidated form of a single medical chart. It supplies such key areas of information 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 provided in a secure and portable manner is vital to medical decision making.

3.1. Services

eCHN Provides the following services via the eCHN Portal:

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 – a tool which allows a Client to refer a patient along with the patients' health information to another eCHN Client that the patient is being referred to.

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 includes functionalities such as alerts of required clinical events according to Canadian and local best-practice guidelines, as well as 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.

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 PHIPA[1] are defined as health information custodians in respect of personal health information within their custody and control. Health information custodians that participate in eCHN are:

- Hospitals
- Community Care Access Centres
- Group based health care practices (e.g. Children's Treatment Centres, Family Health Teams, etc.)
- Public Health Units
- Independent health care practitioners offices

[1] PHIPA, s. 3(1)

- 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 agent[2] may be a person or organization that:

- acts on behalf of a health information custodian;
- with the authorization of the health information custodian; and
- 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 with 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 also 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:

1. ***Accountability*** for personal health information
2. Identifying the ***Purpose*** for the collection of personal health information
3. ***Consent*** for the collection, use and disclosure of personal health information
4. Limiting the ***Collection*** of personal health information
5. Limiting the ***Use, Disclosure and Retention*** of personal health information
6. ***Accuracy*** of personal health information
7. ***Safeguards*** for personal health information
8. ***Openness*** about the management of personal health information
9. ***Individual Access*** and amendment of personal health information
10. Ensuring that individuals have the right to ***Challenge Compliance*** practices at eCHN

[2] PHIPA, s. 2
[3] O. Reg. 329/04, s. 6(2)

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 Officer, who is responsible for providing leadership on all privacy matters that effect the organization. The eCHN Privacy Officer aligns privacy compliance efforts with the eCHN information security program, overseen by the eCHN Sr. Manager, Business Continuity and Technical Infrastructure. This coordinated effort ensures a holistic approach to the protection and management of personal health information at eCHN. Together the eCHN Privacy Officer and the eCHN Sr. Manager, Business Continuity and Technical Infrastructure function under the umbrella of the eCHN Privacy and Security Office.

The eCHN Privacy and Security Office oversees:

- 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 and
- privacy and security awareness training of all eCHN personnel.

eCHN has also appointed a Privacy and Security Committee to ensure the alignment of the privacy framework with the eCHN business objectives. The Privacy and Security Committee reviews information handling and data safeguards, risk remediation activities 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 will ensure 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 on an annual basis, at a minimum.

6.1.3. Breach and Incident Management

An *eCHN Privacy Breach Management Procedure* and an *eCHN Security Incident Management Procedure* are in place to outline the steps to follow 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 the 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. A signed *eCHN Client Application* must be completed by each health information custodian organization or independent provider's office in order to begin registering authorized users for their facility.

Each individual user of a registered client must request access to the eCHN system, by completing and submitting the relevant access application. 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 practice and allows eCHN to comply with its PHIPA obligations.

eCHN Personnel Agreements

All eCHN personnel are required to sign a Confidentiality Acknowledgment and agree to abide by the eCHN Confidentiality Policy as terms of their employment.

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 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. 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.

Data from the eCHN system is not to be used for research purposes. The eCHN Terms and Conditions and the eCHN Portal Access Application Form, both prohibit use of the 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 should fully comply with any consent directive expressly given by their patient with regards to whether the applicable data may or may not be shared with eCHN.

Additionally, inherent in the ability for an individual to consent is the ability of that patient to withdraw or withhold that consent for the collection, use or disclosure of their personal health information. eCHN provides the mechanism for a patient consent directive to be recorded in the eCHN system.

A patient may withdraw consent for *the transmission* of their data to eCHN by notification to the contributing health information custodian. The contributing health information custodian will process the patient transmission restriction in accordance with their organizational policies and procedures for consent management.

A patient may also withdraw consent *for access* to their patient data which is held in the eCHN system. A patient can initiate an access restriction by notification to a contributing health information custodian of their consent directive. eCHN will not process the withdrawal of consent, or access restrictions, directly from an individual, but will refer the individual back to the health information custodian(s) that contributed the relevant record(s). It is the responsibility of each health information custodian to notify eCHN of changes to a patients consent directive in cases where eCHN is required to apply a restriction or filter on that patients' personal health information.

Once notified by the contributing health information custodian, eCHN will process all consent withdrawals, or reactivations of previously withdrawn consent, in a timely manner.

eCHN recommends that each health information custodian discuss and inform individuals of the implications of consent withdrawal.

Emergency Access
Access to a patients locked record(s) 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 patient[4], or
- By a physician user in the case where a patient has given their express consent to override a previously applied access restriction.

A consent override by any physician will trigger an immediate notification to the eCHN Privacy and Security 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.

eCHN will permanently retain an audit log of all consent status changes requested from a health information custodian

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 that contributes data to the eCHN system shall determine which personal health information is provided.

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 that which is noted in the *eCHN Terms and Conditions*, the *eCHN Portal Access Application Form* and any formalized services documentation developed with each contributing client.

[4] PHIPA section 40(1)

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 in accordance with the *eCHN Terms and Conditions*.

All access to the eCHN Portal is logged and 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, 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 Condition* 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 Breach 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 and Procedure* 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 of the eCHN public website.

eCHN does not correct/change or modify the personal health information record maintained at the health information custodian's facility. 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.

As it relates specifically to eCHN WebChart services, data standardization[5] 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.

6.7. Safeguards for Personal Health Information

Security safeguards appropriate to the amount 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 upon 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.

[5] LOINC: Logical Observation Identifiers Names and Codes as updated.

eCHN identifies and applies administrative, technical and physical security controls from the point of data receipt to 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 in the *eCHN Portal – Architecture and Safeguards* which is posted 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 risk 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 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;
- Types of data collected by eCHN;

- The eCHN Architecture and Safeguards which are in place to manage PHI;
- The eCHN Privacy Policy;
- How to contact the eCHN Privacy and Security Office; and
- Making an access request

Additional information on the eCHN Privacy program can also be requested from the eCHN Privacy and Security 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 the individuals' right of access and has implemented procedures to support those 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 of 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 patients health information in the eCHN system; and
- Identify which health information custodian(s) contributed the patients' information to eCHN.

When an individual requires additional details about their records, challenges the accuracy and completeness of the personal health information 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. 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 Officer.

For further information about this policy, eCHN privacy practices or safeguards at eCHN, please contact the eCHN Privacy and Security Office. Any such inquiry should be put 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* as posted 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 can 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 the appropriate actions will be taken by eCHN which may include removal of access rights to personal health information on the eCHN system and up to termination of eCHN user accounts or employment.

8. Terms and Definitions

Term	Acronym	Definitions
Agent	n/a	As defined in PHIPA section 2: *""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…"*
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: - 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

Term	Acronym	Definitions
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 "*Background*" 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): *"…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 agent of any of the custodians."*
Personal Health Information	PHI	As defined in PHIPA[6]. 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.

[6] PHIPA 2004, section 4(1)

Term	Acronym	Definitions
Personal Health Information Protection Act, 2004	PHIPA	The *Personal Health Information Protection Act, 2004* 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.

9. References

Reference and Associated Documents:	• *Personal Health Information Protection Act*, 2004 • eCHN Privacy Breach 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