



electronic  
CHILD HEALTH NETWORK

# eCHN Health Care Provider Guide

Version 1.0

eCHN Document: PSO 304 – eCHN Health Care Provider Guide

## Reference Guide

This guide will assist the users of the electronic Child Health Network (eCHN) with information around processes and contacting eCHN for support.

## Version Table

Version	Date	Author	Comments
0.1	May 29, 2015	S. Petrelli	1 <sup>st</sup> Draft – Partially Complete
0.2	June 25, 2015	S. Petrelli	Complete Draft/Updates based on changes to agreement templates
1.0	September 30, 2016	S. Patrelli, V. Hascalovici, E. Renz	Final draft

# Table of Contents

<b>Introduction</b>	<b>5</b>
Purpose and Scope of Guide .....	5
Audience .....	5
<b>The Electronic Child Health Network (eCHN)</b>	<b>6</b>
Overview .....	6
Benefits .....	7
eCHN Agreements with Health Information Custodians and their Agents .....	7
Who May Access eCHN and for what purpose .....	7
Applying for an eCHN Account .....	7
Acceptable Use of eCHN Information and Information Systems .....	8
The eCHN Help Desk .....	8
How to contact the eCHN Help Desk .....	9
Response Times from eCHN Help Desk .....	9
Privacy and Security Considerations .....	9
Patient Consent Management and Audit Capabilities.....	9
eCHN Support for Consent Management and Conducting Audits .....	10
eCHN Audit Reporter Tool.....	10
Access Requests and Correction of Patient Information in the eCHN Portal EHR .....	11
Security Incident and Privacy Breach Management.....	11
General Security Safeguards in Place at eCHN.....	13
Security Privacy Complaints and Inquiries.....	13

## **NOTICE AND DISCLAIMER**

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the electronic Child Health Network (eCHN).

eCHN and all persons involved in the preparation of this document disclaim any warranty as to accuracy or currency of the document. This document is provided on the understanding and basis that none of eCHN, the author(s) or other persons involved in the creation of this document shall be responsible for the accuracy or currency of the contents, or for the results of any action taken on the basis of the information contained in this document or for any errors or omissions contained herein. No one involved in this document is attempting herein to render legal, privacy, security, or other professional advice.

## **Introduction**

The guide is a comprehensive document outlining various processes which were created to assist electronic Child Health Network (eCHN) users with the eCHN Portal Applications, specifically WebChart and eReferral.

### **Purpose and Scope of Guide**

The eCHN Health Care Provider Guide describes the functions and associated benefits provided by the eCHN Portal Electronic Health Record (EHR) solution and the related privacy and security considerations, which health care providers and organizations must adhere to when using the eCHN Portal EHR applications. The guide provides information regarding support and maintenance, as well as general acceptable use obligations for users of the eCHN portal EHR solution.

### **Audience**

The primary audience for this document includes health care providers and organizations across the health care sector using the eCHN Portal EHR solution to view their patients' records and results.

# The Electronic Child Health Network (eCHN)

The electronic Child Health Network is a crucial innovation that revolutionizes the sharing of patient health information among medical professionals. eCHN is Canada's first province-wide integrated electronic health record. It is a secure electronic network that enables authorized care providers across Ontario to access health information about paediatric patients, instantly, from many different sources. The eCHN Portal EHR solution manages data from patient interactions within the health care system and consolidates them into the form of a single medical WebChart. eCHN provides a coherent, accurate and up-to-date patient record that is available wherever and whenever needed for patient care.

## Overview

eCHN is a non-profit, government-funded organization dedicated to providing an EHR solution that permits the secure sharing of personal health information between authorized health care providers.

eCHN is a production system that pulls together millions of records from patient interactions within the healthcare system to present a patient's health record which may contain:

- laboratory results and reports, including OLIS data at OLIS-authorized client sites
- admission, discharge and transfer data
- clinic notes
- radiology images and reports
- consultants' letters
- surgical notes
- scanned documents
- medication administration reports

The above listed records that are received from each contributing member site are made available, in read only format, to authorized health information custodian users of the eCHN Portal via the WebChart viewer.

eCHN's clinical data repositories contain the health information of Ontario patients from newborn to age 19. eCHN is intended for use by hospitals, other healthcare provider agencies and individual healthcare practitioners. Access to PHI is available to those who "need to know" in order to provide patient care - including physicians, nurses, technicians, therapists and other HIC's. eCHN data repositories are not available to any government or insurance organization and are not to be used for research purposes.

The eCHN Portals e-Referral application was developed specifically for the use of health care professionals, to allow them to refer patients that need specialized care, to the required health care provider. Currently the application facilitates referrals from health care providers to the Hospital for Sick Children, Toronto.

## **Benefits**

Authorized users of the eCHN Portal EHR solution realize the following benefits:

- Seamless integration of patient health information from multiple data sources into one electronic Health Record
- Instantaneous and secure web-based access available 24/7 to authorized eCHN users
- Better coordination of care for patients
- Reduced time spent of medical information gathering allowing more time for direct patient care.

## **eCHN Agreements with Health Information Custodians and their Agents**

All HICs that a) contribute data to eCHN, b) consume data which was provided by contributors or c) any agents of authorized HICs must first agree to the terms and conditions of use of the eCHN Portal. Terms and conditions for the eCHN Portal are found within Participation agreements, eCHN Portal Access Application Forms (ePAAF) and are also posted on the eCHN website. Only those HICs and their specified agents that have a written contract with eCHN may apply for access to the eCHN Portal.

## **Who May Access eCHN and for what purpose**

The eCHN Portal EHR is only made available to Ontario health information custodians<sup>1</sup>, and their authorized agents<sup>2</sup>, who provide health care services to paediatric patients.

Authorized users may only access the data and tools available on the eCHN Portal for the purpose of providing health care or assisting in the provision of health care to patients within their circle of care

Information available on eCHN must not use be used for any research purposes or any other secondary uses.

## **Applying for an eCHN Account**

Ontario health information custodians and their authorized agents may apply for eCHN portal access by:

- Calling the eCHN help desk at 416-813-7998 or 1-877-252-9900
- Emailing the eCHN help desk ([helpdesk@echn.ca](mailto:helpdesk@echn.ca))

---

<sup>1</sup> Health information custodians described in paragraph 1, 2, 3 or 4 of subsection 3(1) of PHIPA.

<sup>2</sup> As defined in section 2 of PHIPA.

- Visiting eCHN.ca and submitting the application request web-form

eCHN will send an ePAAF (eCHN Portal Access Application Form) to applicants for completion and signing. The completed form is then sent to eCHN for processing and to establish:

- If the applicant is a health information custodian, or an appointed representative of an existing authorized health information custodian;
- The position that the applicant holds within their respective health care institution; and
- That the applicant has signed the ePAAF and thereby agreed to the terms for access as well as the obligations they undertake if they are given user privileges for the eCHN Portal.

Applications are processed by eCHN within 2-3 business days.

## **Acceptable Use of eCHN Information and Information Systems**

eCHN has created an Acceptable Use of eCHN Information and Information Systems policy which must be read and accepted by all eCHN Users. The requirements outlined in the Acceptable Use of eCHN Information and Information Systems policy are intended to help protect the confidentiality, integrity, and availability of personal health information stored in or processed by the eCHN Portal EHR.

Some guidance for users on how to apply appropriate privacy and security protocols when collecting, using and disclosing the sensitive patient health information from the eCHN Portal EHR solution is included below:

- eCHN Portal users must only access personal health information for patients within their circle of care, for the purpose of providing health care
- The information available on the eCHN Portal may not be used for research or data mining
- eCHN accounts are for individual use only and eCHN Portal login credentials are to be kept private and confidential. Credentials sharing is in contravention of the eCHN Portal Access Application form signed by each user
- Health Information Custodians/authorized users are expected to also adhere to privacy policies of their organization

## **The eCHN Help Desk**

eCHN provides all users and potential users of the eCHN Portal with full telephone support from the representatives of the eCHN Help Desk. Representatives from the eCHN Help Desk team will be able to answer questions and provide general troubleshooting support to callers.



## How to contact the eCHN Help Desk

eCHN Help Desk – Monday to Friday 8am to 6pm

Tel: (416) 813 – 7998 Toll Free: 1-877-252-9900

Email: helpdesk@echn.ca

## Response Times from eCHN Help Desk

The eCHN Help Desk makes every effort to answer you call or email in a timely manner. Our average times for responding to support requests are within the same business day.

## Privacy and Security Considerations

eCHN complies with the requirements and spirit of the *Personal Health Information Protection Act, 2004*. The eCHN Privacy Policy and protocols are based on ensuring privacy and security compliance with that Act as well as the industry best practices found within the ten privacy principles outlined in the CSA Model Code for the Protection of Personal Information and the information security standards outlined in the ISO 17799.

The Personal Health Information Protection Act, 2004 (“PHIPA”) is Ontario’s health information privacy legislation and governs the collection, use, and disclosure of PHI by health information custodians (“HIC”s) as prescribed within the Act. PHIPA was drafted to balance the privacy rights of individuals with the need for the effective provision of health care. The Act applies primarily to health care providers that have custody or control of PHI along with the agent’s and service providers of those providers, when managing patient data.

HICs within Ontario gain their legal authority to collect, use and disclose PHI from PHIPA and relay their mandated obligations and responsibilities for compliance to their agents and service providers.

eCHN, by acting as a PHIPA agent and Health Information Network Provider (“HINP”) for various Ontario HICs is therefore subject to the Act in fulfilling its responsibilities to those HICs.

eCHN demonstrates its commitment to compliance with its privacy and safeguarding obligations for personal health information with the operation of a robust privacy and security program. The following sections of the health care provider guide outline some of the practices in place at eCHN and how they can be leveraged by authorized users to support the security of their patient data.

## Patient Consent Management and Audit Capabilities

Consent for the transfer of patient data to the eCHN Portal requires that the individual (to whom the personal health information pertains, their guardian or their Substitute Decision Maker) has given express, or implied permission to a contributing health information custodian for the transfer to eCHN of their (or their child’s) personal health information. A patient who has provided their consent for the transfer of their health information to the eCHN Portal may

withdraw consent to their patient chart or restrict access on specific records within a chart, at any time.

eCHN provides access to the eCHN Consent Management application to appropriate staff members at data-contributing client Sites. Step by step information on use of the Consent Management tools available at eCHN can be found within the eCHN Consent Management Guide.

Additionally, eCHN has developed an Audit Reporting Tool that is available to appointed individuals within a health information custodian organization. Appointed users have the ability to perform an audit on a patient chart which originated from their facility to see who has accessed that chart and also to determine which records have been accessed by any specified user from their organization.

### **eCHN Support for Consent Management and Conducting Audits**

Any questions about access restrictions, transaction restrictions, emergency overrides or the eCHN Audit Reporter tool can be forwarded to [helpdesk@echn.ca](mailto:helpdesk@echn.ca) or you may call 416-813-7998 or 1-877-252-9900.

For questions related to the application of a consent directive for a specific patient chart or record please call the eCHN Help Desk at 416-813-7998 or 1-877-252-9900. If you would prefer to send a written communication about a specific patient, please do not include any personal health information within the email communication.

### **eCHN Audit Reporter Tool**

## **Access Requests and Correction of Patient Information in the eCHN Portal EHR**

Individuals making a request for access or corrections to their personal health information can find information about the access and correction process on the eCHN public website at: <http://www.echn.ca/privacy-faq.php>.

Requests must be submitted to eCHN on the *eCHN PHI Inquiry Form* found at: [http://www.echn.ca/documents/SEPF-820\\_eCHN\\_PHI\\_Inquiry\\_Form\\_REVISED-July%2027.pdf](http://www.echn.ca/documents/SEPF-820_eCHN_PHI_Inquiry_Form_REVISED-July%2027.pdf).

Upon receipt of the completed *eCHN PHI Inquiry Form* by the eCHN Privacy Office, a confirmation will be sent to the requestor with 24hrs. A response to the request will be made in an efficient and timely manner.

## **Security Incident and Privacy Breach Management**

eCHN defines a *Security Incident* as an adverse event or series of events that impact the security and therefore the ability of eCHN to conduct normal business.

Some examples of a Security Incidents may include the following:

- Hacker attack (Unauthorized access/modification to an account, system file or hardware, data theft/compromise from external network)
- Hardware/software malfunction that might jeopardise eCHN security
- Equipment theft/loss
- Breaches of physical security
- Confirmed or suspected disclosure of Personal Health Information

eCHN defines a *Privacy Breach* as the intentional or inadvertent unauthorized collection, use, disclosure, retention and/or disposal of personal health information.

Some examples of a Privacy Breach may include the following:

- Sharing of user credentials which leads to unauthorized users accessing the patient information on the eCHN Portal
- Accessing personal health information on the eCHN Portal for reasons other than the provision of clinical care to the patient (i.e. surfing the repository data, research, etc.)
- Improper disposal/destruction of personal health information from the eCHN Portal

If you become aware of a confirmed or suspected security incident and/or a breach of data from the eCHN Portal EHR, accessed, collected, used or disclosed by any of your organization's

staff members, including employees, agents or service providers, you MUST report the confirmed or suspected matter to the eCHN Help Desk at:

Telephone: (416) 813-7998 toll-free 1-877-252-9900

Email: [helpdesk@ech.n.ca](mailto:helpdesk@ech.n.ca) (Do not include any elements of specific patient health information within the communication email)

It is expected that you and your organization's staff will cooperate with any investigations conducted by eCHN in respect of any suspected or confirmed privacy or security breaches in relation to eCHN Portal EHR data. In the event of an incident investigation, eCHN may contact the primary privacy contact noted for your facility.

When reporting a confirmed or suspected privacy or security breach to eCHN, please have the following information ready, where possible:

1. A description of the situation and condition that led to the incident.
2. Who was involved (name and role)?
3. Where did the incident happen?
4. When and at what time was the incident noticed?
5. Describe how the incident was detected.
6. Provide information on the most likely cause – for example:
  - Human error;
  - Technical failure, caused by failure of an application or system to maintain privacy;
  - Process failure, caused by not following a process;
  - Wilful wrongdoing;
  - Etc.
7. Describe the type of PI/PHI involved in the incident.

**Note:** It is extremely important that you do not disclose any patient personal health information and/or personal information to the eCHN help desk agent when reporting a suspected or confirmed privacy breach. You are expected to cooperate in any containment activities or with any investigation undertaken by eCHN. During the investigation by eCHN, you may be required to provide additional information, which may include personal health information or personal information, in order to contain or resolve the breach.

8. List measures taken to contain the breach or any risks that could eventually result in a breach.
9. List any corrective measures taken or additional controls applied.
10. What services, if any, are impacted?

## **General Security Safeguards in Place at eCHN**

eCHN has developed and implemented policies and procedure for the security operation of the eCHN Portal. These guiding documents define baseline control measures called standards of due care controls that are required to prevent a variety of different negative security related scenarios from occurring.

For more information on the Security safeguards in place at eCHN you may go to <http://www.echn.ca>.

## **Security Privacy Complaints and Inquiries**

Any member organizations or authorized users that are concerned with the privacy and security practices at eCHN or that have an inquiry about the eCHN privacy program, may forward their inquiry and/or complaint to the eCHN Privacy Office by:

Telephone: 416-813-7998 toll-free 1-877-252-9900

e-mail: [privacy@ech.n.ca](mailto:privacy@ech.n.ca)

eCHN is committed to the protection of patient information entrusted to us by contributing member organizations and will respond to all concerns or questions in a timely manner.