

## ***eCHN Architecture and Safeguards***

**Section 12. (1) of PHIPA<sup>1</sup>** “A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.”

eCHN as an “**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, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated.

The eCHN architecture is separated into two components – the “data contribution” and the “HiNet Application”.

The **data contribution** consists of sending a copy of Personal Health Information<sup>2</sup> (PHI) data elements, as specified in a formal contractual agreement between the eCHN Member Site and eCHN, over encrypted channel.

The **HiNet Application** is administered centrally at eCHN’s secure data centre and populated through a secure data feed of Admission Discharge Transfer (ADT), Diagnostic Imaging (DI), Electronic Reports (e-reports) and Laboratory Results (LAB) information from the registration systems at the Health Information Custodian’s site participating in eCHN.

Access to the **HiNet Application** is administered through a user authentication database centrally maintained by eCHN. All HiNet users are authorized and authenticated by the eCHN Member Site/HIC.

### **Monitored Access to Personal Health Information**

To assure that Health Information Custodian is able to review access to its patient’s records, online audit tool is integral part of the HiNet application. Every access to the patient’s data is recorded in the audit log file. The audit log can be accessed through HiNet Application by authorized HiNet users at the eCHN member site/HIC with the permission to see the audit information. The HIC can access this log file at any time.

### **Security Safeguards for Personal Health Information (PHI)**

All data communication occurs over the encrypted channel.

All communication with the **HiNet Application** is utilizing end-to-end encryption.

---

<sup>1</sup> Personal Health Information Protection Act, November 2004

<sup>2</sup> A copy of the demographic and clinical data of a patient that is in the custody of the Agent (eCHN), stored in HiNet data repositories for access to authorized users of eCHN.

**Technical Safeguards for eCHN internal network:** Access to the HiNet application is guarded by layered system at eCHN.

eCHN employs advanced security measures such as:

- Enterprise class firewall;
- Centralized antivirus and operating system updates;
- Enterprise class Backup system;
- Comprehensive audit logs;
- End-to-end encrypted channels for all data communication:

### **Administrative Safeguards: eCHN Member Site/HIC**

The HIC's participating in eCHN must sign "Memorandum of Understanding" and subsequent "Privacy Addendum" documents that outline both Health Information Custodian's and eCHN's obligations and responsibilities with respect to the collection, use and disclosure of Personal Health Information via the HiNet Application. These documents are signed on the HIC organizational level.

All HiNet users are authorized and authenticated by the eCHN Member Site/HIC. During the user authentication process, each individual that is required to access PHI is required to sign the "HiNet Access Application Form" and "HiNet User Access Agreement" documents. These documents outline on an individual basis, for all HiNet users, conditions and restrictions of accessing patient's Personal Health Information.

### **Administrative Safeguards: eCHN**

All eCHN Personnel are required to sign a mandatory "Non Disclosure Agreement" that outlines their obligations with respect to all confidential information (including but not limited to PHI). eCHN Personnel are also provided with Privacy and Security training. Training is part of orientation process and refreshed on annual basis.

**Physical Safeguards:** all systems as part of **HiNet Application** and data repositories are physically located in the eCHN's data centre. This secure data centre can be accessed by eCHN Personnel only via restricted and controlled access.

## **Security Incidents Reporting**

<p><b>Section 17 (3) of PHIPA:</b> An agent of a health information custodian shall notify the custodian at the first reasonable opportunity if personal health information handled by the agent on behalf of the custodian is stolen, lost or accessed by unauthorized persons.</p>
--

eCHN has implemented an Information Security Incident Reporting process aimed at satisfying the reporting, recording, response, tracking, resolution and management reporting of information security and privacy incidents.

The security incident reporting process is governed by the eCHN Privacy Policy and eCHN Security Policy, and their corresponding procedures.

The confidentiality of information related to Personal Health Information is maintained at all times.

## **Incident Reporting Flow**

All electronic information (privacy) and/or information systems security incidents MUST initially be reported to the eCHN Business Continuity and Technical Infrastructure team.

eCHN Business Continuity and Technical Infrastructure team will assess the incident and for any incident involving a breach of privacy, they will assign the highest level of importance – Severity One. In the unlikely event of a Severity One Incidents involving PHI, The eCHN Privacy Breach Incident Reporting Procedure is evoked and the eCHN Privacy Officer is immediately notified. eCHN Privacy Officer is responsible for advising the eCHN executives and CEO of the Severity One incident. The relevant eCHN Member Site/HIC who sent eCHN a copy of suspected breached electronic health record is also contacted by the eCHN Privacy Officer.

Facilitated by the eCHN Privacy Officer, a Severity One level incidents would be handled jointly between eCHN and the relevant eCHN Member Site/HIC who sent eCHN a copy of suspected breached electronic health record.. As eCHN does not provide direct clinical support, direct contact with patients, as deemed necessary by the HIC, shall be subsequently handled by the internal Incident processes of the applicable HIC.

All information security and privacy incidents MUST be reported by the eCHN Personnel through completion and submission of the Incident Report form.