ICHA | Inner City Health Associates

Privacy and Security Practices

The following set of procedures has been developed by Inner City Health Associates (ICHA) to be compliant with privacy regulations and best practices as established by the physician regulatory bodies. This document reflects ICHA's responsibility under the regulations as both a Health Information Custodian (HIC) and as a Health Information Network Provider (HINP).

A. Type of information collected by ICHA

1. Identification/Contact information including: name, date of birth.
2. Billing information including provincial/territorial health insurance plan, and interim federal health program.
3. Health information, which may include medical history and presenting symptoms.

B. Security of information

ICHA provides administrative, physical and technical safeguards for the information in its custody and control.

1. Administrative safeguards:
    a. ICHA grants access to information on a 'need to know basis'.
    b. Only authorised users have access to personal health information (PHI). The level of access is based on the role of the individual user as described in Appendix A. The ICHA Privacy Officer will ensure that an up-to-date list of authorised users is maintained.
    c. All authorised users will sign a confidentiality agreement, which will be filed by the Virtual Office Assistant and the Inner City Family Health Team (ICFHT) Administrator.
    d. Contractual agreements with third parties (e.g. EMR service providers, IT support) will include privacy clauses/agreements.
2. Physical safeguards:
    a. ICHA has a contract with St Michael's Hospital to host the servers and firewall for the EMR. They will promptly report identified security risks to ICHA.
    b. Where paper records are used, they will be stored in a secure location, which in most settings will be a locked cabinet in a room that can be securely locked.
    c. Transport of paper records will only be done in exceptional circumstances and in a secure fashion.
3. Technical safeguards:
    a. Each authorised user will be assigned a two level password along with a unique user name.

b. Passwords:

   i. Must be unique and contain at least 8 characters with both letters and numbers or characters.

   ii. Must never be shared.

   iii. Users are responsible for changing their passwords at least once a year.

c. Any physical device (computer, USB stick, phone) that stores PHI must be encrypted and password protected.

d. All computers used to access the EMR must have up-to-date virus protection and spyware. Where the Site supplies the computer, it is their responsibility to ensure these programs are up to date.

e. Automatic log-off: The EMR will be set to automatically log off the user if there is no activity for more than 60 minutes.

f. All computers when left unattended must be locked by the user such that a password is required to re-open the computer.

C. Communications Policy

1. Telephone:

   a. Patient preference with regards to phone messages will be taken into account.

   b. Unless authorised, ICHA will leave only our name and phone number on messages for patients.

2. Fax:

   a. Faxes sent to ICHA are received electronically and directly inputted to the EMR.

   b. At the sites, faxing will only be done if the fax is located in a secure or supervised area.

   c. Pre-programmed numbers will be used to ensure the fax is received by the proper recipient.

3. Email:

   a. Communication of PHI will only be done through secure channels with sufficient levels of encryption.

   b. In the case of patients requesting email communication, they will be informed of the security risks and asked to give explicit consent to the use of email communication. This consent will be fully documented in the chart, ideally on the basis of a signed consent form scanned to the chart.

   c. Wherever possible, the messaging feature in the EMR will be used to communicate PHI amongst the circle of care providers.

4. Post/Courier:

   a. All correspondence including PHI will be sent in a sealed envelope marked “Confidential”.

D. Transparency

All ICHA sites are responsible for ensuring a copy of the privacy statement is posted prominently. In addition the ICHA privacy policy will be available on the public website and upon request at all sites.

Any client or site may request additional information on ICHA's privacy and security policies from their provider or from the ICHA Privacy Officer.

E. Retention of health records

All records will be retained for a period consistent with the latest CPSO guidelines. Currently this means at least 10 years or 10 years past age of majority (Medicine Act, 1991 Regulations) from the date of last entry.

Once retention has expired, effective destruction of electronic records requires that the records be permanently deleted or irreversibly erased. When destroying information, ICHA will also consider whether it is necessary to destroy any copies, including back-up files.

Before destroying records, it is recommended that a list be made of the names of the patients whose records are to be destroyed, and that this list be kept permanently in a secure location. The purpose is to be able to later determine at a glance that a medical record has been destroyed and has not simply been lost or misplaced.

F. Procedures for secure disposal/destruction of PHI

1. Disposal of any paper containing PHI which is no longer needed will be done securely using a cross cutting shredder.
2. Conversion of paper to electronic records will be carried out according to the ICHA protocol which can be accessed here: http://www.icha-toronto.ca/sites/default/files/Paper_Record_to_EMR_0.pdf
3. We will seek expert advice on how to dispose of electronic records and hardware. At a minimum, we will ensure that all information is wiped clear where possible prior to disposal of electronic data storage devices (e.g. computers, hard drives, DVDs).

G. ICHA as a Health Information Network Provider[1]

ICHA's commitment as a Health Network Information Provider (HINP) to the Health information custodians using the ICHA EMR:

1. Confidentiality: The ICHA Information Infrastructure will provide logical access controls, encryption, and other safeguards to protect the confidentiality of data.
2. Integrity: The ICHA Information Infrastructure will provide system logging and other safeguards to ensure the integrity of data.

[1] See O. Reg. 329/04, s. 6 (3).

3. Availability: The ICHA Information Infrastructure is located in a robust data centre and will maintain reasonable availability.

In addition:

4. Breach Notification: ICHA shall notify every applicable participating agency at the first reasonable opportunity of a privacy breach as outlined in our Privacy Breach Protocol which can be accessed here: http://www.icha-toronto.ca/sites/default/files/Privacy%20Breach%20Protocol_Feb2015.pdf

5. Description of Services: ICHA shall provide to each participating agency a plain language description of the services that ICHA provides to the agency (the 'privacy statement'), which is to be posted prominently in the clinical space for all clients to read.

6. Public Notice:

   ICHA shall make available to the public:

   a. The description of services referred to above;

   b. Copies of the ICHA privacy and security policies and guidelines on the ICHA website;

   c. Information about ICHA to ICHA agencies to make available to their clients; and

   d. A general description of the ICHA safeguards.

7. Risk Management:

   ICHA shall perform, and provide to each ICHA site, a written summary of the results of an assessment of the services provided to the health information custodians, with respect to:

   a. Threat Risk Assessments: threats, vulnerabilities and risks to the security and integrity of the personal health information; and

   b. Privacy Impact Assessments: how the services may affect the privacy of the individuals who are the subject of the information.

Version 1: July 2015