Children’s Treatment Network		Children’s Treatment Network of Simcoe York	
Section:	Privacy	Review Period	Annual
Title:	**Security of the Shared Electronic Record Policy**	Effective Date:	December 8, 2008
		Revision Date:	January 5, 2015
Page :	Page 1 of 11	Approved By:	

Purpose

Children’s Treatment Network of Simcoe York (“CTN” or “the Network”) is committed to protecting the privacy and security of personal health information (“PHI”) and personal information (“PI”) of Network Clients, while at the same time facilitating the sharing of information necessary to provide integrated service planning and delivery.

This Policy and related procedures ensure that CTN’s security processes and systems relating to the Shared Electronic Record:

- safeguard the availability and integrity of the Shared Electronic Record; and
- adequately protect confidential and sensitive data within the Shared Electronic Record from unauthorized access, disclosure or loss.

Recognizing that security and privacy must both be in place to protect confidentiality, this Policy is intended to work in tandem with CTN’s **Information Sharing and Management Policy** and related Procedures.

CTN Roles and Responsibilities

As set out in the **Information Sharing and Management Policy**, CTN assumes different roles under PHIPA depending on the circumstances, including the role of Health Information Custodian (“HIC”), Health Information Network Provider (“HINP”), and Network Administrator.

As the HINP and Network Administrator of the Shared Electronic Record, CTN takes reasonable steps to ensure the physical, administrative and technological security of the PHI and PI relating to the Shared Electronic Record and to ensure that records within the Shared Electronic Record are retained/stored, transferred and disposed of in a secure manner.

CTN also enters into any necessary agreements for third party vendor services relating to the Shared Electronic Record which will include contractual provisions for the safeguarding of PHI.

Network Participant Roles and Responsibilities

Each Network Participant is responsible for:

- Ensuring the integrity and good working order of its own infrastructure, hardware and software systems so as not to compromise the security, system functionality or availability of the Shared Electronic Record.

Policy:

- Ensuring adequate safeguards for PHI and PI from the Shared Electronic Record when it is in its own custody or control

- The privacy, confidentiality and security of any PHI or PI relating to the Shared Electronic Record on any local or mobile devices.

Scope

This policy applies to CTN, Network Participants and their Agents (Authorized Users) in respect of the Shared Electronic Record. It governs security of PHI/PI relating to the Shared Electronic Record, including hardware and software operation, physical and electronic media, remote access, and local and mobile devices.

Guiding Principles

CTN and Network Participants rely on the standard ISO principles[1] for the security of PHI/PI as follows:

1. Authentication
   Ensuring the accurate and positive identification of individuals accessing the Shared Electronic Record via password

2. Authorization
   Appropriate and approved access to PHI/PI relating to the Shared Electronic Record is granted based on role-based access controls

3. Encryption
   Information relating to the Shared Electronic Record is protected from being accidentally or intentionally reviewed by encoding files or disclosed to third parties

4. Integrity
   Ensuring that PHI/PI in the Shared Electronic Record is accurate for purposes for which it is collected and used, and protected from unauthorized alteration

5. Accountability
   Accurate auditing to validate proper usage, access and disclosure of information relating to the Shared Electronic Record

6. Non-repudiation
   Ensuring business transactions and information exchanges between multiple entities can be trusted and are legally compliant

7. Availability
   The system is operational and PHI/PI is accessible to system users when needed

8. Relationship of security and privacy
   Complementary responsibilities of security and privacy policies to protect confidentiality

[1] Canadian Health Informatics Association 2011 Guidelines for Protection of Health Information

Policy:

Implementation

1. Authorization, Access Control and Authentication

CTN's Shared Electronic Record is the primary mechanism for the documentation and sharing of PHI/PI relating to Network Clients. PHI/PI in the Shared Electronic Record will be securely retained/stored, transmitted, shared, received, and insofar as is reasonably practicable, protected from unauthorized or unlawful access or interception, accidental loss or damage.

Access to the Shared Electronic Record is restricted to Agents of CTN and current Network Participants:

- whose identity has been verified using standard procedures;
- who have undergone training on CTN policies, family-centered and integrated processes of care, and the Shared Electronic Record; and
- who have signed a confidentiality agreement in which s/he agrees to be bound by privacy laws, CTN policies and any user terms and conditions as may be determined by CTN and Network Participants from time-to-time.

Agents who have been granted access to the Shared Electronic Record are referred to as Authorized Users.

Each Network Participant shall designate a contact person, as required by the Information Sharing Agreement and the **Information Sharing and Management Policy**. The Network Participant's contact person shall provide CTN with the name, role and email address of each Network Participant Agent requiring access to the Shared Electronic Record. On an ongoing basis, the Network Participant's contact person shall promptly advise CTN of any changes (i.e. those who no longer require access to the Shared Electronic Record and whose authorization should consequently be revoked, Agents that will be away temporarily for a period longer than 3 months and whose access should consequently be suspended, those whose access level should be changed, etc.).

CTN's Director of ACCESS and Health Records maintains an ongoing process for confirming the list of Authorized Users with each Network Participant and removing access as requested.

Access to Client PHI/PI relating to the Shared Electronic Record by Authorized Users is strictly on a "need to know basis" and shall only occur in accordance with CTN's **Information Sharing and Management Policy**, **Collection, Use and Disclosure of Personal Health Information Procedure** and **Information Consent Procedure**.

2. Role of the CTN System Administrator

CTN's System Administrator is responsible for the process of validating and authorizing role-based (user group) access to individuals, and assigning user identification and passwords.

The System Administrator removes authorization when notified by the Network Participant contact. The System Administrator may also remove authorization in other circumstances at CTN's instruction, such as in the event of an actual or potential Security Breach or Privacy Breach (see **Privacy Breach Management Procedure**).

Policy:

Additionally, CTN's System Administrator is responsible for:

- Maintenance of current system user log
- Password management
- Ensuring Agents have satisfied the requirements set out above to become Authorized Users
- Initial training on the Shared Electronic Record (in a training copy)
- Privacy training before access to the Shared Electronic Record is granted
- Managing levels of security, including when access is restricted (see below)
- Managing Clients' consent directions (see **Information Consent Procedure**)
- Monitoring the Shared Electronic Record for upgrades, downtime and impact on security
- Completing audit reports and advising users of the audit results
- Providing ongoing support to Authorized Users through an online HELPDESK.

3. Levels of Security

The levels of security for the Shared Electronic Record commensurate with the sensitivity and classification of the information that is stored, shared, transmitted and received by the Shared Electronic Record.

CTN recognizes that ensuring technological security requires that the privacy and security components of the Network work complementarily. CTN stays up to date on new developments in technological security, including the risks and opportunities within the Network related to security of PHI/PI.

The default setting for the Shared Electronic Record allows all Authorized Users to view all information in the Client records for which they are providing care. CTN's System Administrator can change levels of access/security, and has a procedure to manage this.

There are 3 levels of security:

- Default - an Authorized User is able to access all records and expected to access records of assigned Clients only
- Secondary Level – classes of documents and note types can be sequestered from view by specific Authorized Users or groups of Authorized Users
- Tertiary Level – access can be restricted to a specific Authorized User or group of Authorized Users

If a Client/SDM withdraws consent or places any restrictions on his/her PHI/PI (i.e. Consent Directive (lockbox)), the CTN Privacy Officer and/or System Administrator must be promptly notified and will change the level of access accordingly. For further information regarding Consent Directives, refer to the **Information Consent Procedure**.

Policy:

4. Physical Security and Encryption

The physical and technical environment relating to the Shared Electronic Record, including computers and other devices used to access the Shared Electronic Record, is a secure system.

Each Network Participant accessing the shared record will ensure that their staff is supported to access the shared record in an efficient and secure way. Each Network Participant is responsible to ensure that information contained and/or obtained from the shared electronic record is secure.

CTN and Network Participants will implement technical and physical means of protecting the security of the Shared Electronic Record, including:

- Use of strong encryption for all computers that have access to or hold information from the Shared Electronic Record
- Use of strong passwords
- A prohibition on sharing passwords with anyone
- Timing out of computers after 10-15 minutes of inactivity; personal identifying information must not be left on a screen, or a program left accessible while away from the computer
- Fax machines placed in a secure location, with a routine that ensures that faxes are directed to the appropriate person immediately
- Access to a shredder for secure destruction of paper records
- Secure storage, including the use of locked cabinets to store records relating to the Shared Electronic Record that are in paper form or on removal devices (e.g. USB, DVD etc.)
- Sufficient privacy of workstations and meeting places or conversation areas to maintain Client privacy and confidentiality

5. Acceptable Use of CTN Hardware, Software and Networks for Authorized Users

Appropriate Use

- Authorized Users will employ only those accounts for which they are authorized, and will take all necessary precautions to prevent others from obtaining access to their computers or passwords
- Authorized Users are guided by their professional practice standards, where applicable
- Personal use of CTN Hardware, Software and Networks is avoided or kept to a minimum
- Data is treated as confidential and shared based on appropriate consents (see **Information Consent Procedure**)
- If an Authorized User or other Agent inappropriately accesses a record, the Privacy Breach Management Procedure, including notifying the CTN Privacy Officer, will be initiated immediately (see **Privacy Breach Management Procedure**)
- Avoid removing PHI/PI from the Shared Electronic Record or from the secure workplace unless necessary
- Network Participants must keep portable equipment secure: Do not leave laptops or mobile devices providing access to the Shared Electronic Record unattended (e.g. in cars etc.)
- Safeguard privacy in all conversations and at all times
- Immediately report any equipment loss or damage

Policy:

Inappropriate Use

- Activity for personal gain, or that is in contravention of the Criminal Code, Canada's anti-spam legislation (CASL) or the Ontario Human Rights Code is prohibited
- Activity that contravenes CTN's policies and procedures regarding the privacy and security of the Shared Electronic Record is prohibited
- Accumulation of unnecessary, outdated or non-work related files on the network
- Activities that may compromise the integrity of the network, application or computer, such as installing unauthorized software, is prohibited
- Storing PHI/PI on unencrypted devices is prohibited

Sanctions for inappropriate use of network hardware and software are identified in the Information Sharing Agreement, and may include the withdrawal of the hardware, or suspension or revocation of access to the device, software and/or Shared Electronic Record.

6. Remote Access

The Shared Electronic Record has two applications: full client, and web-based. Providers accessing the Shared Electronic Record remotely from outside of their workplace (i.e. from a local or mobile device) must take specific precautions to ensure both physical and technological security.

Network Participants are responsible for ensuring that PHI/PI is not stored on the hard drive or any local or mobile device unless:

- the information or device is encrypted using strong encryption, and
- the device is password protected.

Authorized Users with remote access must take care to ensure that family members do not have access to the information; the computer is logged out when not in use; and the Home Office Security Checklist is followed.

7. **Transmittal of Information Outside the Shared Electronic Record**

- Mobile Devices
  Each Network Participant is responsible for determining if the use of mobile devices by its Agents (Authorized Users) will be permitted and assumes all risks associated with the use of such devices. If a Network Participant permits the use of mobile devices, it must ensure that minimum security obligations are met, including the following:

  - All mobile devices, including laptops and USB keys that provide access to the Shared Electronic Record or contain information from the Shared Electronic Record must be encrypted using strong encryption and password protection.
  - PHI/PI on devices and transferred to the Shared Electronic Record must be stored centrally.
  - Mobile devices should never be left unattended.
  - Information transmitted via a VPN network is encrypted and secure. If encryption software cannot be added to the device, the device shall not be used to store PHI/PI or other sensitive or confidential information.

Policy:

- PHI/PI should not be stored on mobile devices but should be transferred to the Shared Electronic Record.
- The information must be de-identified whenever possible.

Network Participants are responsible for ensuring compliance by their Agents.

- Cell Phones

  Wireless devices may have limitations with respect to secure communications, and health care professionals should be cautious in using them for communication of PHI and other sensitive communications. Cell Phones must be password protected.

- Telephone messages

  PHI/PI left on a voice mail is still considered PHI/PI and poses privacy and security risks. Therefore, caution must be used when leaving telephone messages. An appropriate example of a message that could be left is: "This message is for 'xyz', please ask them to call 'abc' at telephone number 'lmn'." Ensure that the mailbox where the message is left belongs to the person who is to receive the message. Leaving the name of the organization or the fact that the individual placing the call is a health care professional is not recommended. All Network Participants are expected to have secure voice mail systems for incoming messages.

- Email

  Internet-based email is not considered secure, confidential or reliable for the transmission of PHI/PI, as it may be intercepted between the sender and receiver. Email must not be used for urgent or highly confidential information.

  Communication with Network Clients and families via email may occur provided that the Client/SDM has provided express consent to receive communications by email. The consent shall be documented in the Shared Electronic Record. This includes emailing schedules and appointment bookings, as this information constitutes PHI/PI (i.e. it includes the person's name and the provider with whom the appointment is scheduled).

  If a Client or family initiates contact by email, express consent must be obtained before responding with any PHI or PI.

  All email communications by Authorized Users must include headers and footers in the email that put individuals on notice that:

  - The email is intended for the person(s) or entity to whom it is addressed;
  - It may contain confidential or personal information that is subject to privacy laws;
  - Delivery of the message to any person other than the intended recipient(s) is not intended in any way to waive confidentiality;
  - Unauthorized review, retransmission, dissemination or other use of the information by entities other than the intended recipient is prohibited;
  - If the email is received in error, the sender should be contacted immediately and the email should be deleted immediately; and

Policy:

- Provides the Client/family with contact information for follow up by other means.

The content of clinically relevant email communication to/from Clients or families should be contained in the Shared Electronic Record in a clinical note, along with a message that the Client/family has confirmed receipt of communication.

- Videoconferencing/Telehealth

  CTN adheres to the policies of Ontario Telemedicine Network (OTN) when using videoconferencing for clinical or other uses. Privacy@otn.ca. Health care provided through Videoconference/Telehealth will be documented in the Shared Electronic Record.
- eCHN -Electronic Child Health Network

  CTN adheres to the privacy and security policies of the Electronic Child Health Network for its read-only membership.

Policy:

8. Privacy Auditing and Accountability

CTN conducts privacy audits of the Shared Electronic Record, on both a regular and a random cycle, to monitor compliance with information practices and to improve the security of the Shared Electronic Record, which may include, upon providing reasonable written notice, conducting a site visit of the Participant's premises. CTN also conducts audits where necessary to investigate an actual or potential privacy or Security Breach.

An audit log will be maintained, and privacy metrics reported on a quarterly basis to the Quality Committee and Network Participants (clinical and privacy leads) as needed. CTN communicates regularly to Authorized Users about the audit policy, through the login screen each time they access the Shared Electronic Record, and through audit follow-up communications.

"VIPs" are defined as persons who might be of interest to a large number of people, such as sports celebrities or politicians, whose personal information may be at greater risk. "VIPs" may also include staff that has a family member with a shared electronic record. CTN will audit these records more frequently to monitor their security.

From time to time, CTN may also audit the privacy practices of Network Participants with respect to access and security of the Shared Electronic Record and obligations under the Agreement.

9. Security Breach Management

In conjunction with Network Participants, CTN conducts investigations into any actual or potential Security Incidents and Security Breaches associated with the Shared Electronic Record and co-ordinates any notifications and responses.

CTN, a Network Participant or their respective Agent (Authorized User) may become aware of a potential or actual Security Incident or Security Breach through a report or complaint, through an audit or review, or through self-reporting by an Agent.

All Security Incidents require investigation to determine if an actual or potential Security Breach has occurred and to review the circumstances surrounding the Security Incident.

Upon identifying a Security Incident, CTN, the Network Participant or Agent shall immediately notify CTN's Privacy Officer. The notification should include the reporting person's name, title, organization and contact information, along with a description of the actual or potential Security Incident.
Immediate steps will be taken to contain any Security Incident or Breach and to mitigate any potential deleterious effects.

CTN shall conduct an investigation of all Security Incidents, determine whether notification, reporting and/or remedial or preventative steps are required, and take appropriate steps to address the Security Incident and to make sure that similar incidents do not occur in the future.

Policy:

Privacy breaches that occur as a result of or relating to a breach of security in the Shared Electronic Record shall be handled in accordance with CTN's **Privacy Breach Management Procedure**.

All Security Incidents and Security Breaches are reported to CTN Quality Committee on a quarterly basis.

Management of the Shared Electronic Client Record

The CTN Director of Corporate Services and the Director of ACCESS and Health Records /Privacy Officer work together in with respect to the security and privacy of the Shared Electronic Record.

The CTN Director of Corporate Services has responsibility for the effective management of the Shared Electronic Record including: data integrity, backup and recovery, and other technical security functions such as the secure network infrastructure (firewalls, etc). This includes establishing and implementing procedures for system downtime (in collaboration with the System Administrator and Director of ACCESS and Health Records), regular threat and risk monitoring, and contacts with any information system vendors. CTN shall promptly communicate any issues, upgrades, improvements or changes to the Shared Electronic Record that impact upon the Network Participant.

Each Network Participant is responsible for its own information practices and systems. To the extent that a Network Participant intends to make significant changes to its information practices or systems that may affect the functioning of the Shared Electronic Record, the Network Participant shall ensure that such technical assessments or privacy impact assessments as are necessary or advisable in the circumstances are conducted, at its own cost. The Network Participant shall share the results of the assessments with CTN prior to making any changes to its information practices or systems and CTN shall have the right, acting reasonably, to refuse to permit such changes.

Review and Revision

This Policy will be reviewed annually and revised as needed. Any changes will be communicated as needed to all Network stakeholders.

Definitions

Authorized User
An Agent of CTN or a Network Participant who has been granted authorization to access the Shared Electronic Record relating to his/her role and responsibilities for CTN and/or a Network Participant.

Security Incident
Any situation where the security of the Shared Electronic Record or a Client's PHI/PI is called into question, including a Security Breach, 'near miss', or a complaint relating to the security of the Shared Electronic Record.

Security Breach

Policy:

Any act or omission by an Agent of CTN or a Network Participant or other individual that results in a negative impact or that causes interruption, disclosure, unauthorized access to or modification or destruction of PHI/PI relating to the Shared Electronic Record, or a any lack of availability of health information systems that adversely affect care provided to Network Clients.

Refer to the **Information Sharing and Management Policy** for further definitions.

References and Links

Information Sharing and Management Policy
Information Sharing Agreement

Procedures

- **Privacy Breach Management Procedure**
- **Process for restricting access to a client record (Levels of Security)**

Technical and Installation Guides for CTN Shared Electronic Record
Home Office Security Checklist
Confidentiality Agreement
Ontario Telemedicine Network Privacy Policy

Procedures in development/revision

- **User Authorization**
- **Privacy Auditing**