CEHC Regional Epic Instance Privacy Training

EpicCare Link / Third Party Access

- 2022/23

Central East
Clinical Information System
AN EPIC TRANSFORMATION

Objectives

After completing this module, you will have a better understanding of:

the regional nature of the CEHC Epic instance

relevant privacy legislations

the definition of PHI

what constitutes a privacy breach & its potential consequences

what a Private Encounter is and the expectations of Health Care Providers

what Break-the-Glass (BTG) is and the expectations of Health Care Providers

what a Release Restriction is and the expectations of Health Care Providers

what privacy resources are available to you and how to locate them

Central East
Clinical Information System
AN EPIC TRANSFORMATION

CEHC Regional Epic Instance

Partners of the Central East Hospital Cluster (CEHC) have adopted a shared, regional clinical information system. In practice, this enables clinical end users of the system to access and use personal health information across all Partner sites for authorized purposes (such as the provision of healthcare to patients).

When accessing Epic, clinical users will gain access to patient-level and encounter-level information collecting or occurring at all seven Partner organizations.

Training Rationale

To provide external users with information on how to best safeguard our patients' personal health information (PHI) against lost, theft, and unauthorized access, collection, use, and disclosure

To ensure all users have access to education/training around matters relating to PHI and privacy

To address common incidents identified through electronic health record (EHR) audits, near misses, and privacy breaches

To meet Information and Privacy Commission of Ontario (IPC) guidance, expectations, & in alignment with previous IPC Orders

To support all team members of the CEHC community with information regarding privacy legislation, and CEHC Regional policies

Key Terms

Agent: A person that acts for or on behalf of a health information custodian with authorization of the custodian

Breach: Personal Health Information that is lost, stolen, or accessed, collected, used or disclosed without authorization

Circle of Care: Enables HICs to rely on an individual's assumed implied consent for the   purpose of providing health care (not defined under PHIPA)

FIPPA: *Freedom of Information and Protection of Privacy Act*, 1990

HIC: Health Information Custodian. Person or organization who has control or custody of PHI as a result of performing the duties of a hospital or practice of health care providers

IPC: Information and Privacy Commissioner of Ontario

PHI: Personal Health Information (see slide #6 for PHIPA's definition)

PHIPA: *Personal Health Information Protection Act*, 2004

Privacy Legislation

There are two main privacy Acts that apply to hospitals:

    i.   *Personal Health Information Protection Act, 2004* (PHIPA)

    ii.   *Freedom of Information and Protection of Privacy Act*, 1990, (FIPPA)

PHIPA applies to all personal health information

FIPPA applies to all organizational & personal information (non-health)

- This training session will discuss items covered by PHIPA.

PHIPA:
- Balances the privacy right of patients with the legitimate need of HICs to access, collect, use and disclose PHI in order to deliver effective and timely health care
- Governs the way PHI may be accessed, collected, used and disclosed.

Personal Health Information

Any health information pertaining to an identifiable individual, or that could reasonably be used with other information to identify an individual

PHI must be protected in any form, verbally or recorded, and in any medium (written, print, photographic, audio, video, electronic or otherwise)

PHI includes, but is not limited to:
*   the physical or mental health of an individual (incl. family health history)
*   identification of a person as a health care provider of an individual
*   payments or eligibility for health care services
*   a health number (i.e., an Ontario Health Card Number alone is considered PHI)
*   the substitute-decision maker (SDM) of an individual

What is a Breach of Privacy?

A privacy breach refers to any;

- unauthorized access, collection, use, or disclosure
- loss
- theft

of any:

- personal information (PI), or
- personal health information (PHI)

Unauthorized Access/Disclosure

Unauthorized Access:

Accessing anyone's PHI <u>without</u> a work-related **NEED-TO-KNOW,** including accessing more information than is necessary

Unauthorized Disclosure:

Sharing patient information (within or outside of LH) to people who <u>do not</u> have a work-related **NEED-TO-KNOW**

Need-to-know considers:

      consent

      circle of care

      significant risk of serious bodily harm, or

      use for other permitted purposes under *PHIPA 37(1)*, *for example:*

            Planning or delivering programs or services

            Risk or error management, quality of care

            Educating agents to provide health care (formal)

Privacy Breach Implications

As a result of unauthorized access, collection, use, disclosure, loss, or theft of PHI, the following consequences can occur:

Mandatory reporting to:
        Regulatory colleges
        the IPC
        the patient/SDM/Executor

IPC's investigation can lead to penalties, including:
        Fines for Agents up to $200,000 and/or imprisonment of 1 year
        Fines for HICs up to $1,000,000

Disciplinary action can include loss of access and/or privileges

Legal action including criminal charges and/or civil lawsuits

Reputational damage & loss of patient/community trust

Most Common Incidents:

1.Giving information to wrong patient

When releasing prescriptions, referrals, discharge summaries or other PHI, ensure the correct documents are given to the correct patient (check name on all documents PRIOR to release) – particularly if using a shared printer and/or computer.

2.   Snooping

All agents of a CEHC Partner are permitted access to PHI for the purposes of completing their job functions and aligned to accountabilities expected of them by the sponsoring Partner (and for no other purpose).

3.Disclosing information without proper consent

When releasing information, ensure that informed consent has been obtained, or confirm that you are releasing with circle-of-care implied consent.
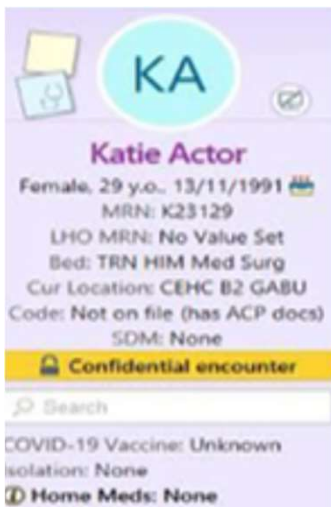
Only release what is necessary for the purpose.

Each User, Site Administrator and Sponsoring CEHC Partner are responsible for the information accessed through the shared Epic instance.

Private Encounter Patients

Under PHIPA, HICs are permitted (not mandated) to confirm that a patient is:

      i.in the facility

      ii.the patient's location

      iii.their general health status (critical, poor, fair, stable or satisfactory)

Patients have the right to opt-out of this disclosure and have their visit confidential.

If a patient has a Private Encounter, you will see a banner on the storyboard in Epic.

Katie Actor
Female, 29 y.o., 13/11/1991
MRN: K23129
LHO MRN: No Value Set
Bed: TRN HIM Med Surg
Cur Location: CEHC B2 GABU
Code: Not on file (has ACP docs)
SDM: None
🔒 Confidential encounter
🔍 Search
COVID-19 Vaccine: Unknown
Isolation: None
Home Meds: None

If a patient is not capable, a SDM can request a Private Encounter status; if no SDM is available, **a clinician can make the patient Private until a SDM is located**

For Private Encounter patients:

    <u>**NO information**</u> should be shared about the patient

    The patient's name should not be written on any boards, bedrooms, etc.

    If someone calls or shows up looking for this patient, they will be told, "***I have no information for that <u>person</u>***"; this includes police unless they have a warrant, consent, require the information due to a "significant risk of serious bodily harm" or produce an Urgent Demand for Records under the *Missing Persons Act, 2018*

Break-The-Glass (BTG) Patients

Under PHIPA, patients have the right to place a restriction on the **access** and/or disclosure of their PHI.
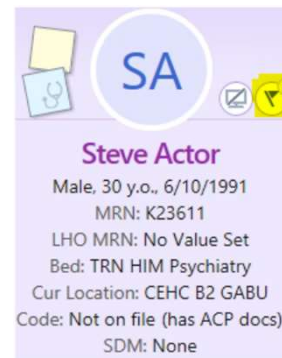
All BTG requests are processed by the Privacy Offices of CEHC partners.

The restriction can be applied at the patient level or at the encounter level.

When accessing, you will be prompted for a password.

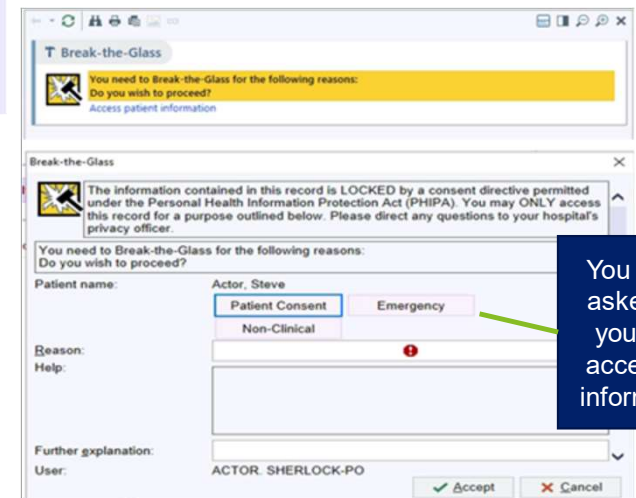**The password = your Epic log-in password.**

Your may only break the glass if you have patient consent or where the information is necessary to eliminate or reduce a significant risk of serious bodily harm.

SA

Steve Actor
Male, 30 y.o., 6/10/1991
MRN: K23611
LHO MRN: No Value Set
Bed: TRN HIM Psychiatry
Cur Location: CEHC B2 GABU
Code: Not on file (has ACP docs)
SDM: None

You will know a patient has a BTG on their chart by hovering over the flag on the patient's storyboard.

You will be asked why you must access the information.

The Privacy Office is notified of all Breaks

13

Release Restriction Patients

Under PHIPA, patients have the right to place a restriction on the access and/or **disclosure** of their PHI. All Release Restriction requests should be directed to the Privacy Office of your Sponsoring Partner for processing.

A banner will flag the Release Restriction when using the *Quick Disclosure Activity.*

A Tip Sheet (*Release Information Using the Quick Disclosure Activity*) is available on your Home Dashboard by clicking F1 or in Additional Resource section under 'Release Information.'

In Basket

Epic also includes a number of new electronic communication tools, including Secure Chat and In Basket

> Both solutions enable care team members to communicate quickly and safely with colleagues using secure instant messaging or email-like functions within Epic

> Secure Chat & In Basket messages do not form a part of the patient's legal health record, therefore any information from these messages that is used to inform care decisions or delivery must be copied into the legal health record (i.e., via a clinical note).

> While not a component of the legal health record, communication may be subject to disclosure in legal proceedings.

CEHC's Care Team Communication Guide (appendix a) provides additional information on the appropriate use of communication tools for different purposes

CEHC Privacy Office Contacts

If you become aware of a privacy breach or have a privacy concern, please immediately contact our team.

Campbellford Memorial Hospital:

- ekeogh@cmh.ca
- 705-653-1140 ext. 2147

Haliburton Highlands Health Services:

- kchurko@hhhs.ca
- 705-457-1392 ext. 2222

Lakeridge Health:

- privacy@lh.ca
- 905-576-8711 ext. 34367

Northumberland Hills Hospital:

- privacy@nhh.ca
- 905-372-6811 ext. 4827

Peterborough Regional Health Centre:

- privacy@prhc.on.ca
- 705-743-2121 ext. 3856

Ross Memorial Hospital:

- privacyofficer@rmh.org
- 705-328-6297

Scarborough Health Network:

- privacy@shn.ca
- 416-284-8131 ext. 7782

16

**Central East
Clinical Information System**
AN EPIC TRANSFORMATION

References & Resources

LH Care Team Communication Guide
Information & Privacy Commissioner of Ontario
Personal Health Information Protection Act (PHIPA)

Important and Influential IPC & Orders:
- *Unauthorized Access & Disclosure: IPC Ontario*
  - *H-013 Disclosure*
  - *H0-002, H0-010, Decisions 44, 74, 80 Snooping*
  - *Decision 102 Shared Electronic Health Records*
  - *Decision 110 Hospital EMRs & Private Practice Employees*
- *Transporting PHI & Encryption: IPC Ontario*
  - *H0-004*
- *Patient Access to Records: IPC Ontario*
  - *H0-009, H0-012*

Central East
Clinical Information System
AN EPIC TRANSFORMATION

Care Team Communication Guide

Goals

Clinical communication should be:

Collaborative	with clinical team members sharing responsibility for the method, format and privacy of information sent while respecting recipient availability and capacity.
Appropriate	by ensuring that relevant communicated health information is documented in the chart and that communications reference, not replace, the health record.
Timely	by ensuring that communication senders and receivers have a shared understanding about how, when and where different types of communications will be received and acted upon.
Accountable	by recognizing that clinically important communications content should be documented within the permanent health record.
Secure	by using Epic clinical communication tools, when available, and organizationally approved tools when interacting with persons not using Epic.

Guides

Do	When Using Communication Tools	Don't
- Use for work purposes; not personal or social purposes. - Use to facilitate clinical care. - Respect people's time and availability, with reasonable response time expectations. - Communicate indirectly with the same professionalism expected of direct communication. - Limit communication recipients (copy, blind copy, group, etc.) to those with clear need and accountability. - Ensure coverage for communication responsibilities when away or unavailable. - Appropriately attribute or reference communication content.		- Use indirect communications when direct communications (face-to-face, telephone, telehealth, etc.) are needed. - Use to deliver health care (without documentation). - Compose essays… keep communications brief and relevant. - Use clinical communications for complaint, criticism or accusation; or use slang, inappropriate abbreviations or disrespectful or unprofessional language. - Use communication tools to request orders or other chart entries where the sender is able to self-order or self-enter in a safe manner. - Copy chart elements into a communication when a reference or link to the chart is possible.

Mode of communication	FYI	Routine	High	Urgent/ Emergent
Secure Chat	✓	✓	⚠	✗
In Basket* - staff message	✓	✓	⚠	✗
Sticky Note	✓	⚠	⚠	✗
Handoff Note	⚠	✓	⚠	✗
Verbal - in-person	✓	✓	✓	✓
Verbal - phone call	⚠	⚠	✓	✓
Page	⚠	⚠	✓	✓
Hospital email	✓	✓	⚠	✗
Personal email/text message	Not recommended for secure clinical communication			

✓ Recommended

⚠ Per User Preference/Per Local Practice

* Refer to the Regional Policy regarding In Basket use

Priority	Definition	Examples	Considerations
FYI	Informal communication not included in the medical record. Does not require a response from the recipient.	Sticky notes. For example: "If you have a minute, please call the patient's husband at 608-271-9000 to give him an update." "The patient is afraid of needles. To calm him down before shots and blood draws, ask him about his puppy at home."	If you would normally hold the information until shift change or physician rounds, do not send one-off messages.
Routine	All non-urgent patient situations, including informational content. Might not require a response from the recipient	Non-critical vitals or normal lab results. For example: "The patient has arrived in room 208." "The patient's temperature is 101.5, which exceeds 101.3 documented in the notify physician order – send a message to the attending provider."	Read receipts do not count for closed loop communication. If you expect a response, please ask the recipient to reply. If you would normally hold the information until shift change or physician rounds, do not send one-off messages.
High	Patient situations that need timely attention and response but does not yet require immediate decision-making or real-time action. Requires a response from the recipient for confirmation.	Abnormal lab values, abnormal vital signs, pending discharge. For example: "The patient has a gradual, persistent deterioration in vital signs – send a message to the attending provider."	Read receipts do not count for confirmation that recipient received the message. Requires specific training for escalation of care if the recipient does not respond.

| Urgent/ Emergent | Patient situations that need immediate attention and require real-time action. | Patient deteriorating, critical lab values, trauma, code, critical values. | Requires specific training for escalation of care if the recipient does not respond. |
| | Requires a response from the recipient for confirmation. | For example: "The patient has an intracranial bleed – send a message to the neurosurgeon on call." | The mode of communication depends on your organizational policy for urgent patient care requests. |