Privacy of Information at OSMH

PHIPA & FIPPA

Orillia Soldiers' Memorial Hospital

Privacy Office

October 2023

Soldiers'
MEMORIAL HOSPITAL Orillia

Overview

- Information found in Ontario's Privacy Acts: PHIPA and FIPPA
- Privacy and security practices at OSMH

Please review the "Privacy Breach Management" and other privacy policies/procedures that are found on the OSMH Intranet. These are great resources for all OSMH employees, volunteers, and associated staff.

Carefully read and understand the Confidentiality Agreement! Employees are responsible to understand their obligations as it relates to privacy and confidentiality at OSMH.

If you have any further questions about the Confidentiality Agreement seek out clarification from your manager or the Privacy Office.

Personal Health Information Protection Act

PHIPA, 2004

Personal Health Information Protection Act

PHIPA, 2004

PHIPA sets out to:

- Establish rules for the collection, use and disclosure of personal health information (PHI)
  - Key aspects
    - Maintain confidentiality
    - Protect privacy
- Provide individuals with a right of access to PHI about themselves
- Provide individuals with a right to correct or disagree with the PHI about themselves

OSMH Privacy Office

- Provides educational documentation and policies
- Manages potential privacy threats or breaches
- Conducts privacy audits to ensure appropriate access to records
- Works with the Release of Information office to execute patient requests for access / correction of PHI
- Provides input towards privacy related matters
- Reports annual statistics of breaches and access requests to the Information and Privacy Commissioner of Ontario (IPC)
- Reports to the OSMH CEO on matters related to Privacy

Access to Information Systems at OSMH

- Access to information systems used at OSMH are based on the employees roles for the organization and their job requirements.
- Employees will have varying degrees of access granted to them
  - This is determined by what is needed for an employee to perform their day-to-day responsibilities.

Security - PHIPA

- OSMH will take reasonable steps to ensure that PHI is protected against theft, loss and unauthorized use or disclosure
- OSMH will ensure that records containing information are protected against unauthorized copying, modification or disposal.

Examples of Security Practices

(Including but not limited too)

- Keep documents out of reach and out of sight
- Ensure documents are secured
- Turn computer screens away from public view
- Lock workstations when not in use
- Keep conversations professional
- Who and what you see at OSMH is **private** and may not be disclosed to anyone

Authorized Access

Authorized access is an individual who is **permitted** to access PHI as required by their role and to perform their job responsibilities.

What does "Authorized Access" mean?

Examples:

- Providing health care
- Quality of Care practices
- Release of Information

Unauthorized Access

Access to any PHI outside of an employees scope of responsibilities is considered an **unauthorized** access**.**

- I.e., accessing PHI for non-work related purposes

Examples of unauthorized access:

- Accessing ones own record
- Accessing the record of a family member or friend
- Accessing the record of someone they are not providing care to

Unauthorized access to PHI is subject to disciplinary action.

To ensure all employees at OSMH are accessing records to which they are authorized, audits are conducted regularly.

Employees Requesting Access to their PHI

"Employees will not attempt to gain access to information in which they are not specifically authorized".

How do I request access to my records?

- MyChart
  - Free patient portal where patients of OSMH can view certain records
- Contact Health Records - Release of Information (ext. 3513)
  - Your personal health records will be prepared and provided at no cost
- PocketHealth
  - Full access to all imaging performed at OSMH (cost associated)

Patients Requesting Access to their PHI

- MyChart and Pocket Health
- Health Records - Release of Information (ROI)
  - Form filled out and submitted online or in person
- A patient may request to view their record in hospital
  - Request must be submitted to the ROI office
  - The most responsible physician is consulted
  - The patient is accompanied while viewing the records
- Employees may only release records owned by OSMH

Employee Access Audits:

(Breach of Information or breach of Regulatory College Standards)

Employees found to have unauthorized access will be;

- Investigated with the employees manager, Privacy Officer, Human Resources and Union (if applicable)
- Reenrolled into privacy eLearning or training documents
- Have a letter placed on their employee file
- Discipline up to and including dismissal
- Notification of the privacy breach to one or all of:
  - The employee's regulatory college (if applicable)
  - The IPC
  - The affected patient(s)

Breach

A breach is the unauthorized collection, use or disclosure of an individuals PHI.

Classified according to Breach levels:

Level 1: Accidental or unintentional

- Employee carelessly accessed, reviewed or disclosed PHI to themselves without a legitimate need to know

Level 2: Intentional or Non-malicious

- Employee accessed, used or disclosed PHI for reasons other than providing care

Level 3: Intentional and Malicious/Personal Gain

- Employee knowingly breaches policies and/or legislation with malicious intent to harm

Implied Consent vs. Expressed Consent

Implied Consent

Is consent that one understands has been given by the patient based on what the patient does or does not do.

Expressed Consent

Provided either verbally or in writing to collect, use or disclose their PHI.

Circle of Care

- The Circle of Care is used to describe the ability of certain health information custodians (HIC's) to assume an individual's implied consent to collect, use or disclose their personal health information for the purpose of providing health care.
- There may be non health custodians (Non-HIC's) who are also in the Circle of Care. You will be required to obtain expressed consent to share a patients PHI.

Connecting Ontario

- Access to the Connecting Ontario portal is granted to employees based on their roles and responsibilities
  - Employees may only view/handle patient's PHI in the portal if it is required within the scope of their duties
- Privacy Office audits access to Connecting Ontario
  - Same rules apply in terms of permitted access and consequences for breaching privacy

Patients Requesting Correction of Health Records

If a patient believes their record contains incorrect information:

- Patient must submit a formal request, in writing, to the OSMH Privacy Office to ask for the Correction.
- If it is determined that the correction cannot be made (discretion of the Clinician), a Notice of Disagreement will be offered.

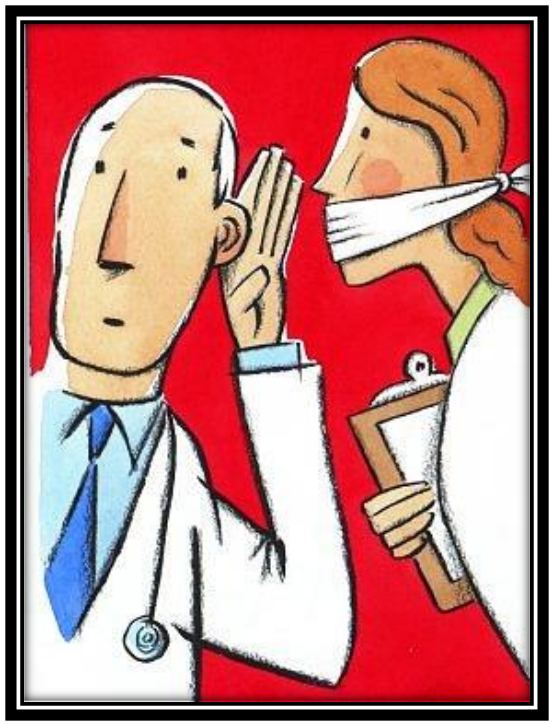
Emails

- PHI can be emailed to internal recipients (OSMH email addresses) to complete necessary job duties
  - PHI should be limited - Use MRN or FIN instead of name or HCN
- PHI can only be sent using approved methods. E.g. (password protected files, Onedrive access)
- OSMH recognizes that all electronic communication is considered to be a “record” and may be disclosed in an information request.
- All electronic mail communicated by OSMH email is the property of the hospital
  - OSMH reserves the right to audit and monitor email usage and content.

Mobile Devices

- All communication must respect the hospital's policy on confidentiality and all applicable laws
- Mobile devices are not to be used to communicate confidential information
- Photos or videos of patients, visitors, volunteers or staff is **prohibited**
  - Require express permission

Remember:



- Only collect, view, use or discuss patient information in the provision of care and as authorized for your role at OSMH
- **"What happens here, stays here"** even when you know the person.
- Anything mentioned to anyone outside the Circle of Care (even a colleague) will be considered a breach.

Freedom of Information and Protection of Privacy Act

FIPPA, 1990

FIPPA

1990

The purposes of this Act are,

(a) to provide a right of access to general records and personal information (non-PHI) under the control of institutions; and

(b) To protect the privacy of personal information contained in those records.

As a public institution information should be available to the public and any exemptions from this should be limited and specific.

FIPPA

Non-health record related information requests

- These requests could be for:
  - **Personal Information**
  - **General Records**
- Directed to the OSMH Privacy Office
- Remember: print, audio or electronic form **is a record**
  - This includes: emails, paper files, electronic files, video tapes, audiotapes, notebooks, sticky notes, handwritten notes etc.
- **Create records with access in mind**
  - Records should be factual, objective (no personal thoughts) and include only what is relevant
  - Write as if you will publish it in the newspaper.
  - **Anything recorded could be made public one day**