Privacy

Legislative References: Personal Health Information Protection Act, 2004 (PHIPA)

Purpose:

This policy is intended to provide an overview of the confidentiality and privacy requirements as specified under the Personal Health Information Protection Act, 2004 (PHIPA) and to address any other professional obligations or legislation relative to client confidentiality and the practice of healthcare. It also covers the protection of employee privacy and establishes acceptable behaviours for all staff of the HHC to uphold their legal and professional obligations pertaining to privacy and confidentiality.

The purpose of this policy is to ensure that personal identifiable and personal health information is protected at all times during the collection, use, disclosure, storage and destruction by HHC employees, contracted service providers, students, and volunteers to ensure patient confidence when they seek healthcare or disclose sensitive information to staff and to the facility. Protection of confidential information also includes minimizing the risk of theft, loss, and unauthorized use or disclosure of that information, regardless of the media, including information being transferred between locations or transferred to a third party.

Policy Statements:

The Harrow Health Centre (HHC) is committed to safeguarding the confidential information of patients, employees and other individuals associated with the workplace or its practices, as required to comply with all applicable legislation for the province of Ontario and pertaining to the practice of healthcare.

Procedure:

Confidentiality refers to the responsibility and accountability of an organization or person to protect information entrusted to its care for a specific purpose. Such information entrusted to the organization or person must only be used for the purpose it was originally intended and must only be accessible to those authorized to have access to it.

This means that all personal health and personal identifiable information related to a client must be kept in strict confidence for the use only by the identified “circle of care” providers, regardless of whether the information was gathered verbally, in written format, or recorded. Sensitive data must be maintained in a secure environment limited to an appropriate set of authorized individuals and organizations.

Breach of confidentiality is the sharing of personal health or personal identifiable information, in any form, regarding a patient with someone who is not identified in the circle of care for that individual or who does not have the appropriate consent for release of information.

Patient trust with regards to the security of confidential information is critical to the patient –provider relationship. In essence, the Act “balances the individual’s right to privacy with respect to their own personal health information with the legitimate needs of the health information custodians to collect, use and share the information.” In addition, this specific type of health or personal identifiable

information must have been received from the individual, their substitute decision maker or another health information custodian.

The HHC and affiliate will only use, disclose, and retain patient's personal health information in compliance with the law and for its intended purpose. The following safeguards have been implemented to prevent unauthorized use by authorized users:

i. All staff and affiliates with potential to access patient or staff personal information sign a confidentiality agreement prior to commencing employment with the HHC
ii. Staff have clearly outlined job responsibilities and scope of practice outlining their need to use personal health information
iii. Staff are informed that their access to personal health information will periodically be audited (EMR Audit run monthly)
iv. At no time are staff permitted to allow access for visitors to view computer-based information
v. All staff are to ensure that all information printed out is filed, scanned and/or discarded in a manner to ensure confidentiality
vi. All staff are to ensure that the transfer of any personal health information is done in a confidential manner to the intended recipient

The HHC as the Health Information Custodian and its agents will be held accountable and have an enforceable duty to keep personal health information secure by:

i. Limiting the use of personal identifiable or health information to the purpose it was provided
ii. Removing personal identifiable or health information where practical
iii. Implement and maintain physical, administrative, and technological security measures to reduce the risk of unauthorized use or disclosure
iv. Destroying or having an authorized person/provider destroy, personal health information after its purpose has been met, if permitted by law
v. Assuring members of a particular patients "Circle of Care" that they can confidently assume that they have consent to collect, use, and disclose the patient's personal health information for that care, unless knowledgeable that that patient has expressly withheld or withdrawn that consent
vi. Addressing a request for a patient or staff's personal health information by a patient or third party
vii. Outlining the retention periods of the patient's personal health information
viii. Taking every reasonable step to secure the personal and health information of the facility's patients and staff against theft, loss and unauthorized use or disclosure, as well as, protecting this information against unauthorized copying

All organizations that are designated as Health Information Custodians (HIC) are required to have a privacy officer. At the HHC the position with this accountability is the Executive Director. In the absence of the Executive Director, the delegate for the CPO is the Clinical Director.

All breaches of privacy/confidentiality are to be reported to the Privacy Officer, or delegate, and will be investigated promptly. Any breach proven to be deliberate or as the result of competency issues may result in disciplinary action, up to and including dismissal, and a report to the applicable College. Breaches are also reportable to the Privacy Commissioner.