

POLICY, PRACTICE AND PROCEDURE

NAME: Collection, Use and Disclosure of Personal Health Information	MANUAL: General
CODE #: WE-MI-07	# OF PAGES: 3
EFFECTIVE DATE: June 11, 2014	LAST REVISION DATE: December 2, 2013

1. PURPOSE

To ensure compliance with legislative requirements, ethical obligations and professional standards of practice when collecting, using or disclosing personal health information.

2. SCOPE

This policy applies to all employees, contractors, sub-contractors, students and volunteers.

3. POLICY

- 3.1. WECHC complies with the Personal Health Information Protection Act (PHIPA), 2004.
- 3.2. Refer to the Resource Guide – Privacy and Confidentiality for more detailed information.
- 3.3. Client records are confidential.
- 3.4. PHIPA allows for the disclosure of personal health information without client consent in certain circumstances including treatment in emergency situations, duty to warn and criminal offense. (Refer to #4.4 below). In addition, employees may be required by law to disclose personal health information without the consent of the client (mandatory reporting).
- 3.5. If personal health information is being transmitted by fax, a Fax Cover Sheet must be used. Successful transmission of the information will be verified by the sender by reviewing the Fax Confirmation.

4. PROCEDURE

4.1. New Client

During their initial visit new clients and/or substitute decision-makers must be informed about the collection, use and disclosure of their personal information:

- The **Statement of Personal Health Information Practices for Clients** is shared/discussed and the client initials the registration form indicating that they have read and understand.
- The registration form is placed/scanned in the client's health record. If the client's health record is divided the form must be maintained in the current, active record.

4.2. Lock Box

A client/substitute decision-maker has the right to refuse disclosure of all or part of the personal health information on the record, including another custodian (healthcare provider/institution) which is known as the "lock box" provision. If a client or substitute decision-maker refuses to disclose all or part of the personal information on the health record:

- discuss the potential health risks for creating a "lock box" and not disclosing the information;
- document the details of the discussion in the client's health record;
- inform others of the information that has been withheld at the direction of the client. If the "lock box" request cannot be honoured in Nightingale, the information will be captured on paper and "locked".

4.3. Disclosure Related to Duty to Warn and Criminal Offense

If disclosure is necessary in relation to a Duty to Warn or Criminal Offense:

- advise the Director of the situation and discuss the steps to be taken to address the situation:
 - advise the client of the decision to disclose the information,
 - contact the police, and/or,
 - contact the intended victim(s).
- document all information related to the process used in the client's health record.
- Advise the Privacy Officer of the situation and consultation as needed.

4.4. Disclosure Required for Litigation

In the event an employee(s) receives a summons, subpoena or court order:

- discuss the matter with the Director and/or ED to develop an appropriate plan;
- refrain from making any statements with respect to the case except under oath, or unless directed to by the Court.

4.5. Access to Personal Health Information

If a client requests access to their health record or a substitute decision-maker requests access on a client's behalf:

- acknowledge the individual's request for information by telephone or form letter (within one (1) business day);
- notify your Director and the Privacy Officer of the request.
- review the request (should be in writing with enough detail to reasonably find the record or the part(s) of the record specific to the request and must include the reason for the request). If more information is required to find the record, work with the individual to obtain the information required;
- process the request within 30 days (or 60 days in the case of complex searches) and at minimal or no cost to the individual:
 - notify the individual in writing if the record cannot be found after a reasonable search;
 - notify the individual if access cannot be provided to all of the information requested, i.e., information that is prohibitively costly to provide, contains references to other individuals, cannot be disclosed for legal, security, or commercial proprietary reasons or is subject to solicitor/client or litigation privilege;
 - provide the individual with access specific to the request - review the information requested with the individual to answer any questions, to clarify medical terms or abbreviations used in the record and to ensure that the record is not altered in any way;
 - provide the individual with a copy of the information if requested.
- Document all information related to the request, acknowledgment and processing of the request in the client's health record.

4.6. Challenging the Accuracy of the Information

In accordance with PHIPA, an individual can challenge the accuracy and completeness of the information in their health record and have it amended as appropriate (correction, deletion, or addition of information).

- When an individual successfully demonstrates the inaccuracy or incompleteness of personal information:
 - complete the required amendment;
 - document the details of the request and the actions taken in the client's health record;

- transmit amended information to third-parties having access to the information if appropriate.
- When an individual is unable to successfully demonstrate the inaccuracy or completeness of personal information:
 - provide the individual with the reason(s) for denial of their request to amend the record;
 - document the details of the request and discussion with the individual in the client's health record.

4.7. Unauthorized Theft, Loss, Access, Use or Disclosure of Client Information

When knowledge of theft, loss, unauthorized access, use or disclosure of client information is identified:

- notify the Director and Privacy Officer;
- complete an Incident/Concern Report form;
- complete an investigation to gather the information related to the incident including the specific client records and personal health information involved;
- the Director will send to the client(s) a letter to inform them of the theft, loss, unauthorized access, use or disclosure, what personal health information was affected and what measures have been taken to rectify the breach;
- document the details of the process followed in the client's health record.

5. RELATED DOCUMENTS

- Confidentiality Agreement - Form# - WE-MI-05-001
- Fax Cover Sheet - Form# - WE-MI-07-008
- Information Practices (English and French)
- Resource Guide – Privacy and Confidentiality
- Statement of Personal Health Information Practices for Clients (English - Form# - WE-MI-01-002 and French - Form# - WE-MI-01-002FR)
- WECHC policy WE-MI-05 - Confidentiality
- WECHC policy WE-MI-01 - Privacy Policy
- Regulated Health Professions Act (RHPA), 1991

Original Policy Approval Date: December 2, 2013					
POLICY REVISIONS SUBSEQUENT TO ORIGINAL APPROVAL					
Number	Initiator	Reason	Who	Date	Approver
1	Dir Clinical Practice	EMR Update	Dir Clinical Practice	June 11, 2014	Privacy Officer