



Thunder Bay District
Health Unit

THUNDER BAY DISTRICT HEALTH UNIT CORPORATE POLICY MANUAL

SECTION:	GENERAL ADMINISTRATION	NUMBER:	GA-03-05
SUBJECT:	Privacy of Personal Information	PAGE:	1 of 4
DATE:	November 1, 2004	APPROVED BY:	Senior Management
SUPERCEDES:	March 2003	SIGNATURE:	

DEFINITIONS

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) is legislation that provides for public access to government records and the protection of privacy respecting “personal information” held by municipal institutions. It ensures that individuals have the right to access their own personal information and to request correction of the information if they believe it to be inaccurate. It also regulates the collection, use, retention and disposal of personal information to ensure that it is protected from unauthorized disclosure.

Personal Health Information Protection Act (PHIPA) is legislation that regulates the collection, use and disclosure of “personal health information” held by health information custodians. It gives individuals the right to access and correct their own personal health information.

Personal Information is information about an identifiable individual, including: name, race, age, sex, education, employment history, address and telephone number.

Personal Health Information is identifying information about an individual which relates to: the individual’s physical or mental health, the provision of health care, health card number, family history, or identifies the individual’s substitute decision-maker.

PURPOSE:

The Thunder Bay District Health Unit is responsible for the protection of “personal information” and “personal health information” in our custody and control, and must ensure that information practices are in place that comply with applicable legislation.

The purpose of this policy is to set out guidelines with respect to the collection, use, disclosure, and security of personal information” and personal health information contained in our records, and to set out the process for receiving and responding to requests for information.

In this policy, personal information and personal health information will be hereinafter referred to as “personal information”, unless otherwise noted.

POLICY

Personal information held by the Health Unit will be collected, used, and disclosed in accordance with the applicable legislation.

1. *Accountability*

- The Medical Officer of Health is designated as the Head for purposes MFIPPA. The Policy and Privacy Officer shall be the designated contact person under PHIPA, and is responsible for facilitating organizational compliance with the legislation and responding to access requests.
- Management shall be responsible for ensuring that reasonable measures are in place to prevent unauthorized access to the records in their programs, as well as ensuring that a Directory of Records and if applicable, a listing of Personal Information Banks, exists for their Divisions and/or Programs.
- All requests for access to records will be processed through the Health Unit's Privacy Officer, according to the attached procedure.

2. *Identifying Purposes*

- Health unit clients will be advised of the purpose for which their personal information will be used, and such purpose shall be identified at or before the time the information is collected. All forms used in the collection of personal information shall contain a notice outlining the purpose for which the information will be used.
- The primary purpose for collecting information is for the provision of health care, the prevention of disease or injury or the promotion of health care,
- When personal information is used for a purpose not previously identified to the client, and for purposes not required by law, the new purpose must be discussed with the client.

3. *Consent*

- The Health Unit will rely on implied consent, where appropriate, or obtain express consent from clients when collecting, using and disclosing their personal health information, unless otherwise exempt by the legislation.

4. *Collection of personal information*

- The Health Unit will only collect personal information from clients that is needed to administer its programs and services.
- Such information must be collected directly from the individual unless otherwise authorized by the legislation.

5. *Use and Disclosure*

- The use and disclosure of personal information will be limited to the purpose identified at the time of collection, unless further consent is obtained or the disclosure is permitted or required by law.
- Personal information shall be as accurate, complete and up to date as is necessary for the purpose for which it is used.

6. *Retention and Destruction*

- Personal information must be retained long enough to give the individual opportunity to access it and check for accuracy (at least one year).
- Personal information contained in Health Unit records, shall be retained according to time periods identified in the Directory of Records and Retention Schedule for the applicable Program.
- Disposal of personal information shall be authorized, documented and carried out in a manner that protects the privacy of the individual, and according to Health Unit Policy on Records Management (GA-03-07). Records containing personal information must be destroyed in such a manner that they cannot be read, reconstructed or retrieved.

7. *Security*

- Personal information will be held in confidence and access to the information will be limited to employees who need to know this information in the performance of their duties.
- Personal information must be secure from accidental or unauthorized disclosure, copying, modification or destruction.
- Protection methods will include:
 - "Clean desk policy" where desks are locked when unattended
 - Locking file cabinets when unattended, and key distribution is limited and documented
 - Implementation of computer passwords and screen savers for electronic records (See also GA-03-11 Electronic Medical Records)
- As a condition of employment, all employees must sign a "Statement of Confidentiality". (See HR-08-02-4 Confidentiality of Information)

8. *Access*

- Upon request, an individual may be provided access to their personal information, provided they meet the requirements of the legislation. Certain exceptions to access may apply such as: where a physician has confirmed that the information may be detrimental to the client's health; where the information cannot be disclosed for legal reasons or where the record relates information pertaining to other individuals.
- An individual may also be able to challenge the accuracy and completeness of the information and have it amended as appropriate. Refer to procedure for access below.

PROCEDURE FOR ACCESS*Staff*

1. Have the requester complete Form A-2 Access Request whenever possible, or put their request in writing. This includes direct requests from clients, clients' solicitors, or requests from law enforcement or other agencies. See descriptions of additional forms below. If in doubt about a request, contact the Health Unit's Privacy Officer or your immediate Supervisor.
2. Ensure the request is dated or date stamped, retrieve the records and forward to the Privacy Officer as soon as possible (time limits may apply).

Privacy Officer

3. The Privacy Officer will review the records in question, communicating with the applicable Director/Manager, and if necessary, make a determination whether the request falls under MFIPPA or PHIPA.
4. Privacy Officer will provide guidance and recommendations as to the most appropriate method of processing the request, i.e., as a formal or informal request. The request may be processed by the Privacy Officer or returned to the applicable program area for processing.
5. For formal requests under MFIPPA or PHIPA, the Privacy Officer will open a file, send the appropriate acknowledgement letter, calculate and process payment of the fee if applicable, and initiate time tracking of the request.
6. Requests made by a Law Enforcement Agency may be released through this process or may require a subpoena.

FORMS

1. **Access Request Form A-2** - Use when requesting access to general records, access to own information, or correction to own information.
2. **Consent to Release Information A-3** - Use when an individual is consenting to the release of personal information or personal health information that is not otherwise authorized for disclosure.
3. **Notice of Requirement to Provide Information A-4** - Use when a request is made by an outside agency having legal authority under another Act or Statute to obtain personal information on individuals that is contained in our records. (i.e. Children's Aid Society)