

# TBRHSC Privacy/Personal Health Information Policy

## **POLICY:**

Thunder Bay Regional Health Sciences Centre (TBRHSC) is responsible for personal information under its control. As a provider of healthcare services, TBRHSC collects, uses and discloses personal health information and is a personal health information custodian under the Ontario Personal Health Information Protection Act (PHIPA).

TBRHSC is committed to protecting the privacy, confidentiality and security of all personal health information to which it is entrusted. The ten principles, which form the basis of TBRHSC's data protection, are interrelated, and TBRHSC will adhere to the ten principles as a whole.

Further information will be available in Frequently Asked Questions "FAQ" and in related policies.

<b>Index:</b>	<b>Page</b>
Principle 1 – Accountability for Personal Health Information	1
Principle 2 – Identifying Purposes for Personal Health Information	2
Principle 3 – Consent for the Collection, Use, and Disclosure of Personal Health Information	2
Principle 4 – Limiting Collection of Personal Health Information	4
Principle 5 – Limiting Use, Disclosure, and Retention of Personal Health Information	4
Principle 6 – Ensuring Accuracy of Personal Health Information	4
Principle 7 – Ensuring Appropriate Safeguards for Personal Health Information	4
Principle 8 – Openness Concerning Policies and Practices	5
Principle 9 – Individual Access to and Amendment of Personal Health Information	5
Principle 10 – Challenging Compliance with TBRHSC's Privacy, Confidentiality and Security Policy	6

## **Principle 1 – Accountability for Personal Health Information**

Accountability for TBRHSC compliance with the principles rest with the Chief Executive Officer, although other individuals within the Centre are responsible for the day to day collection and processing of personal information. In addition, other individuals within TBRHSC are delegated to act on behalf of the Chief Executive Officer, such as the Privacy Officer.

TBRHSC is responsible for any personal health information that has been transferred to a third party for processing. TBRHSC will use affiliation agreements or other means to provide a comparable level of protection while personal health information is being processed or accessed by a third party.

TBRHSC will implement corporate policies and practices to give effect to this policy. These include:

- Implementing procedures to protect personal health information
- Establishing procedures to receive and respond to complaints and enquiries
- Training staff and communicating to staff information about TBRHSC policies and practices
- Developing information to explain TBRHSC's policies and procedures

## **Principle 2 – Identifying Purposes for Personal Health Information**

TBRHSC will identify the purposes for which personal information is collected at or before the time of collection. The primary purposes are:

- To provide clinical care to patients
- To monitor and evaluate the quality of care and the outcomes resulting from that care
- To assess resource utilization in the delivery of care; to plan for the development and delivery of care and services
- To support and promote research and education
- To support and promote fundraising in relation to TBRHSC
- To meet legal and regulatory requirements

Identifying the purposes for which personal information is collected at or before the time of collection allows TBRHSC to determine the information it needs to collect to fulfill these purposes.

Depending on the way in which the personal health information is collected, the purposes will be provided orally or in writing. A patient pamphlet will give notice of the purposes. A patient who presents for treatment is also giving implicit consent for the use of his or her personal health information for authorized purposes.

When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless law requires the new purpose, the consent of the individual is required before information can be used for that purpose.

Persons collecting personal health information on behalf of TBRHSC shall be able to explain to individuals the purposes for which the information is being collected.

### **Principle 3 – Consent for the Collection, Use, and Disclosure of Personal Health Information**

The knowledge and consent of the individual are required for the collection, use or disclosure of personal health information, except when inappropriate.

**Note:** In certain circumstances personal health information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, TBRHSC will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when a hospital wants to use information for a purpose not previously identified).

This principle requires knowledge and consent. TBRHSC will make a reasonable effort to ensure that the individual is advised of the purposes for which personal health information will be used (e.g. through notice and patient information brochures). To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

TBRHSC will not, as a condition of the supply of a service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

A consent to the collection, use or disclosure of personal health information about an individual may be express or implied.

A health information custodian that receives personal health information for the purpose of providing health care, or assisting in the provision of health care, is entitled to assume they have the individual's implied consent to collect, use or disclose the information for those purposes, unless the custodian that receives the information is aware that the individual has expressly withheld or withdrawn the consent.

If a health information custodian discloses personal health information about an individual to another custodian, and if the disclosing custodian does not have the consent of the individual to disclose all the personal health information considered reasonably necessary for the purpose, the disclosing custodian will inform the other custodian of that fact.

Consent to the disclosure of personal health information about an individual must be express, and not implied, if:

- A health information custodian makes the disclosure to a person that is not a health information custodian
- A health information custodian makes the disclosure to another health information custodian and the disclosure is not for the purposes of providing health care or assisting in providing health care
- 

Typically, TBRHSC will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when TBRHSC wants to use information for a purpose not previously identified). In obtaining consent, the reasonable expectations of the individual are also relevant. Consent will not be obtained through deception.

TBRHSC can assume that an individual's request for treatment constitutes consent for specific purposes. The ways in which TBRHSC seeks consent for other activities may vary, depending on the circumstances and the type of information collected. TBRHSC will generally seek express consent when the information is likely to be considered sensitive (e.g., genetic testing). Implied consent would generally be appropriate when the information is less sensitive. An authorized representative (such as a legal guardian or a person having power of attorney) can also give consent.

Individuals can give consent in many ways. For example:

- An information sheet may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses
- Consent may be given orally when information is collected over the telephone, or
- Consent may be given at the time that individuals receive a service or treatment

If an individual is incapable of providing consent, they may designate a secondary decision maker to act on their behalf for the collection, use and disclosure of personal health information.

If the individual is incapable of designating a secondary decision maker, the following schedule will be used to make the designation:

1. The individual's guardian of person or guardian of property.
2. The individual's attorney for personal care or attorney for property.
3. The individual's representative appointed by the Consent and Capacity Board under section 26, if the representative has the authority to give consent.
4. The individual's spouse or partner.
5. A child or parent of the individual, or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent. This does not include a parent who has only a right of access to the individual.
6. A parent of the individual with only a right of access to the individual.
7. A brother or sister of the individual.
8. Any other relative of the individual.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. TBRHSC will inform the individual of the implications of such withdrawal.

#### **Principle 4 – Limiting Collection of Personal Health Information**

The collection of personal health information will be limited to that which is necessary for the purposes identified by TBRHSC. Information will be collected by fair and lawful means.

TBRHSC will not collect personal health information indiscriminately. Both the amount and the type of information collected will be limited to that which is necessary to fulfill the purposes identified. TBRHSC shall specify the type of information collected as part of its information-handling policies and practices.

TBRHSC shall not collect personal health information by misleading or deceiving individuals about the purpose for which information is being collected.

### **Principle 5 – Limiting Use, Disclosure, and Retention of Personal Health Information**

Personal health information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. When personal health information is to be used for new purposes, this policy will be updated to reflect these changes. Information will be retained only as long as necessary for the fulfillment of those purposes or as legislated. Disposal of personal health information will be done in a secure and confidential manner.

#### **Limiting Use:**

Access to personal health information will be limited to only those staff with a need to know such information for their job purposes (the “need to know” rule). Authorization is required before accessing, collecting, using, or disclosing personal health information. If an employee is unsure of whether they have authorization to access, use or disclose personal health information, they will seek clarification from their Manager/Coordinator or Privacy Officer.

Personal health information is to be maintained in the strictest of confidence and is not to be shared with unauthorized persons. For example, staff must avoid engaging in discussions about personal health information in public areas such as hallways, elevators, washrooms, cafeterias, etc.

#### **Limiting Disclosure:**

Personal health information may not be disclosed to a third party such as a pharmaceutical company without the express consent of the subject (e.g. the patient or his or her substitute decision maker).

However, information is released for:

- Providing ongoing clinical care to patients
- Contacting a relative or friend of a patient
- Confirming the patient is in the facility
- Confirming the death of a patient
- Supporting and promoting fundraising as it is related to TBRHSC
- Supporting approved research initiatives
- Approved audits and accreditation activities
- Professional colleges and other regulatory bodies
- The Public Guardian and Trustee, Children’s Aid Society, or lawyer representing a child
- Meeting other legal and regulatory requirements

### **Principle 6 – Ensuring Accuracy of Personal Health Information**

Personal health information should be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

The extent to which personal health information shall be kept accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

TBRHSC shall not routinely update personal health information, unless such a process is necessary to fulfill the purposes for which the information was collected, such as updating addresses.

Personal health information that is used on an ongoing basis, including information that is disclosed to third parties, shall generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

### **Principle 7 – Ensuring Appropriate Safeguards for Personal Health Information**

Personal health information shall be protected by security safeguards appropriate to the sensitivity of the information, regardless of the format in which it is stored.

The security safeguards will protect personal health information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage.

The methods of protection will include:

- *Physical measures*, for example, locked filing cabinets, restricted access to offices, ensuring terminals are turned away from public view, or video surveillance
- *Administrative measures*, for example, limiting access on a "need-to-know" basis; and
- *Technical measures*, for example, the use of passwords, encryption, auto-logging off the system when a session is finished or after a period of inactivity, and audits on the electronic patient record system.

Personal health information is not to be left in written form or displayed on computer terminals in areas or locations where unauthorized individuals may access it. Personal health information is not to be left unattended where there is no one to receive the information (e.g. fax machines).

Reproduction or copying of any personal health information should be limited and should not interfere with the integrity of the information. Staff reproducing or copying documents are responsible for ensuring that the documents are not left behind and that any discarded copies are to be disposed of securely.

### **Principle 8 – Openness Concerning Policies and Practices**

TBRHSC will make readily available to individuals specific information about its policies and practices relating to the management of personal health information under its custody or control.

TBRHSC will be open about its policies and practices with respect to the management of personal health information. Individuals will be able to acquire information about its policies and practices without unreasonable effort.

The information made available will include:

- The name and the address of the Privacy Officer, who is accountable for TBRHSC policies and practices and to whom complaints or inquiries can be forwarded
- The means of gaining access to personal health information under TBRHSC custody or control
- The process of requesting a change to your personal health information
- A description of the type of personal health information held by TBRHSC, including a general account of its use
- The contact information for the Office of the Information and Privacy Commissioner of Ontario
- A copy of any information that explains TBRHSC's policies, standards or codes
- A list of personal health information that may be made available to other agencies and health care professionals

### **Principle 9 – Individual Access to and Amendment of Personal Health Information**

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal health information and may access, inspect, or copy (upon payment of cost recovery fee) his or her personal health information, subject to legal restrictions. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

**Note:** In certain situations, TBRHSC may not be able to provide access to all the personal health information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

Upon request, an individual has a right of access to a record of personal health information about themselves that is held at TBRHSC. TBRHSC will seek to indicate the source of this information and will

allow the individual access to this information. If reasonably practical, TBRHSC will provide an explanation of any term, code or abbreviation used in the record.

An individual can receive a copy of their personal health information by submitting a written request to Health Records, TBRHSC or by visiting the Health Records Department and completing an Authorization For Release of Information form. The request must be an original in order to complete the request. Requests must include name, date of birth and mailing address as well as the type of information requested. The request must be dated, witnessed and signed by one other person.

To have records released to a relative, friend, family doctor or another institution, a signed Authorization For Release of Information must be submitted to TBRHSC giving the hospital authorization to release the information.

An individual may be required to provide sufficient information to permit TBRHSC to provide an account of the existence, use, and disclosure of personal health information. The information provided will only be used for this purpose.

In providing an account of third parties to which it has disclosed personal health information about an individual, TBRHSC will attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, TBRHSC will provide a list of the organizations to which it may have disclosed information about the individual.

TBRHSC will respond to an individual's request within 30 days and at a reasonable cost to the individual. The requested information will be provided or made available in a form that is generally understandable. For example, if TBRHSC uses abbreviations or codes to record information, an explanation will be provided.

When an individual successfully demonstrates the inaccuracy or incompleteness of personal health information, TBRHSC will amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information will be transmitted to third parties having access to the information in question.

If an individual believes their record is inaccurate or incomplete, they may submit a written request for a correction to their record. A request will be granted if the individual demonstrates the record is incomplete or inaccurate, and the information necessary to correct the record is given to TBRHSC. TBRHSC may not grant a request for correction if the record consists of a professional opinion made in good faith.

If a request is refused TBRHSC will provide a written Notice of Refusal to the individual explicitly stating the reason for the refusal. The individual has the right to make a complaint to the Office of the Information and Privacy Commissioner of Ontario, if a request is refused.

When a challenge is not resolved to the satisfaction of the individual, TBRHSC will record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

### **Principle 10 – Challenging Compliance with TBRHSC's Privacy, Confidentiality and Security Policy**

An individual shall be able to address a challenge concerning compliance with TBRHSC's Privacy, Confidentiality and Security to the Privacy Officer. All formal complaints must be submitted in writing to the Privacy Officer. All complaints will be investigated and remedial action taken when appropriate including, if necessary, amending its policies and practices.

Any individual who collects, uses, or discloses personal health information under the custody or control of TBRHSC can be the subject of a question, complaint or breach of this policy.

All breaches are taken very seriously. In the event of a breach, a consultation with the Manager, Privacy Officer, and Human Resources will take place to ensure a consistent and unbiased viewpoint. Penalties for breaches will be assigned on a case-by-case basis. Depending on the facts of each case, disciplinary action may include verbal or written warnings, counselling, suspension, termination of user privileges, and

termination of employment, hospital privileges or affiliation with TBRHSC. Staff of professional colleges will be reported to their respective college in accordance with the College's protocols for reporting data protection breaches. Breaches that are criminal in nature may involve the police.

Documentation on all breaches will be retained in an individual's personnel file under the custody of Human Resources. The manager of an employee who has committed a breach will report all breaches to the Privacy Officer.

TBRHSC will put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal health information.

**REFERENCE:**

Bill 31: An Act to enact and amend various Acts with respect to the protection of health information. Royal Assent, May 20, 2004, 38<sup>th</sup> Parliament, 1<sup>st</sup> Session, 2003-2004. Toronto: Legislative Assembly of Ontario, 2004. Available: [http://www.ontla.on.ca/documents/Bills/38\\_Parliament/Session1/b031ra.pdf](http://www.ontla.on.ca/documents/Bills/38_Parliament/Session1/b031ra.pdf) . [October 22, 2004]

"Personal Health Information Protection Act" Toronto: Legislative Assembly of Ontario, 2004. Available: [http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03\\_e.htm](http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm) [October 22, 2004]

Ontario Hospital Association, Ontario Hospital eHealth Council, Ontario Medical Association, Office of the Information and Privacy Commissioner. 2004. Hospital Privacy Toolkit: Guide to the Ontario Personal Health Information Protection Act. (Publication # 314). Ontario: Queen's Printer for Ontario.

Ontario Hospital Association. 2003. Guidelines to Managing Privacy, Data Protection and Security for Ontario Hospitals. Ontario: