



Timmins and District Hospital

Policy Name: Privacy Policy			
Policy No.:	1.3.1.1.	Approved Date:	Nov 2004
Lead /Approving Director: Director of Clinical Services, CPO	Reviewed Date:		
	Revised Date:	August 2005, June 2006, August 2006	
Documents Replaced (if any)			

Preamble: Policies are related to the Hospital's mission, vision, values, philosophy and objectives. They make broad statements and aid in decision-making. They prescribe limits, pinpoint responsibilities and accountabilities and are interdisciplinary in nature.

Name of Policy: Privacy Policy

Purpose - Timmins and District Hospital privacy policy guides our compliance with the Personal Health Information Protection Act (PHIPA).

Distribution/Practice Setting -
TDH Health Care Team

Definitions –

Agent

Anyone authorized by the Hospital to collect, use or disclose of Personal Health Information (PHI) on behalf of the Hospital and not for the agent's own purposes; (for example, employees; persons contracted to provide services who have access to PHI (records management, copying or shredding records); health professionals with privileges; volunteers; directors; students

Circle of Care

Those Health Information Custodians (HIC) indicated under the definition of HIC with an asterisk (*HIC), for the purpose of providing health care or assisting in providing health care within the continuum of care

HIC (Health Information Custodian) includes:

- *the Hospital
- *health care practitioners
 - regulated health professionals; registered drugless practitioner; social worker; person whose primary function is to provide health care (acupuncturist, psychotherapy)
 - **NOT** aboriginal healers; aboriginal midwives; faith healer
- *service providers to CCAC

- *CCAC
- *public, private, or mental hospitals
- *psychiatric facilities under *Mental Health Act*
- *independent health facilities
- *homes for aged, nursing homes
- *pharmacies
- *laboratories
- *ambulance
- *community health or mental health centres whose primary purpose is providing health care
- evaluators under *Health Care Consent Act* or assessors under *Substitute Decisions Act* (capacity)
- medical officer of health and board of health under *Health Protection and Promotion Act*
- Minister and Ministry
- others as provided under the regulations

Hospital - Timmins and District Hospital

IPC – Information and Privacy Commissioner of Ontario

Patient information - means PHI as defined by PHIPA. See definition.

PHI (Personal Health Information)

Information, oral or recorded, about an individual that does or could identify that individual and that:

- relates to physical or mental health
- includes family history as it is reflected in record of PHI
- identifies the health care provider
- relates to payments or eligibility for health care
- relates to donation of body part or bodily substance
- includes the health number (replaces *Health Cards and Numbers Control Act*)
- identifies SDM
- includes any non-health info that is in record that is identifying

PHIPA – *Personal Health Information Protection Act, 2004* (Ontario)

Privacy Officer – Hospital employee identified at end of this Policy

SDM – substitute decision maker

Policy –

The Personal Health Information Protection Act is based on 10 privacy principles consistent with other international privacy legislation. Timmins and District Hospital is committed to upholding these principles in the way we handle personal health information

Principle 1 - Accountability for Personal Information

T&DH is responsible for personal information under its custody or control and has designated

an individual, the Chief Privacy Officer, who is accountable for the Timmins & District Hospital's compliance with the following principles.

Principle 2 - Identifying Purposes for the Collection of Personal Information

T&DHN, at or before the time personal information is collected, will identify the purposes for which personal information is collected. The primary purposes are the delivery of direct patient care, the administration of the health care system, to conduct research and statistics, to comply with legal and regulatory requirements.

Principle 3 - Consent for the Collection, Use, and Disclosure of Personal Information

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

Principle 4 - Limiting Collection of Personal Information

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

Principle 5 - Limiting Use, Disclosure and Retention of Personal Information

Personal 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. Personal information will be retained only as long as necessary for the fulfillment of those purposes.

Principle 6 – Ensuring Accuracy of Personal Information

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

Principle 7 – Ensuring Safeguards for Personal Information

Security safeguards appropriate to the sensitivity of the information will protect personal information.

Principle 8 - Openness about Personal Information Policies and Practices

T&DH will make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9 - Individual Access to their own Personal Information

Upon request, an individual will be informed of the existence, use and disclosure of his or her personal information and will be given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 - Challenging Compliance with T&DH's Privacy Policies and Practices

An individual will be able to address a challenge concerning compliance with the above principles to the Chief Privacy Officer.

Timmins and District Hospital recognizes the importance of privacy and the sensitivity of personal health information (“PHI”). The hospital is committed to protecting any information that belongs to the patients that we hold. This Privacy Policy outlines how Timmins and District manages patient information and safeguards privacy.

PHIPA Is the Law

Starting November 1, 2004, any health information custodian (“**HIC**”) in the Ontario health care system that collects, uses or discloses PHI must comply with the *Personal Health Information Protection Act, 2004*.

The Hospital is a HIC and is responsible for the PHI we collect, use, maintain and disclose, as set out in this Policy.

What Information Does the Hospital Collect From Patients?

Generally, the hospital will ask patients to give whatever information about their health and their family's health that is needed to provide appropriate care.

Timmins and District will collect information from patients for the following purposes, which are our “**main activities**”: caring, administration of the Hospital and the health care system, teaching, limited research, statistics and complying with legal and regulatory requirements.

Timmins and District Hospital will either directly tell the patient why we are collecting this information or will post a notice or give out information that describes why we are collecting patient information.

The hospital will only collect information from patients indirectly (e.g., from other health care providers or from the patient's family and friends) if necessary to provide care, when a patient cannot provide the information or cannot consent to providing the information.

How Does the Hospital Use Patient Information?

Patient information is given to caregivers in Timmins and District Hospital to be used to care for patients. The hospital's directors, employees, professional staff (doctors, dentists, midwives, and nurse practitioners), volunteers and students are trained and understand that patient information is private and can only be used or accessed to provide care or carry out the hospital's main activities.

People who have a contract to provide services to the Hospital (such as fixing equipment, maintaining computers) may have access to patient information, and the hospital takes steps through contracts to make sure this information is kept private.

Unless the hospital has a patient's consent to use their information for research purposes, patient information will only be used for research if the strict process (ensuring both privacy and ethical conduct) in PHIPA is followed by both Timmins and District Hospital and the researcher.

If the hospital uses patient information for any purpose other than its main activities, the hospital will ask the patient's permission.

When Will The Hospital Disclose Patient Information?

Unless a patient tells the hospital not to, the hospital will disclose patient information to other health care providers in the “Circle of Care” who need to know this information to provide care or help to provide care. The “Circle of Care” includes health care professionals, pharmacies, laboratories, ambulance, nursing homes, CCACs, other hospitals in partnership with Timmins and District Hospital (NEON, NORrad, CRLP, eCHN) and home service providers who provide a patient with health care services.

Unless a patient tells the hospital not to, the hospital will tell anyone who calls or visits Timmins and District Hospital that:

- The patient is in the Hospital (Room #)

Unless a patient tells the hospital not to, if the patient gives the hospital information about their religious affiliation, the hospital may give the patient's name and room number to a Timmins and District Hospital representative of the patient's religious affiliation.

Unless a patient tells the hospital not to, the hospital may give a patient's name and address to the Foundation, which may contact a patient for fundraising purposes. The patient can ask not to be contacted for fundraising at any time.

Sometimes the law requires the hospital to disclose information about a patient, such as to OHIP for payment purposes. The hospital will only disclose patient information when the law requires or permits the hospital to do so.

Getting a Patient's Consent

A patient's consent to the hospital's collection, use or disclosure of their information may be implied or express. In certain circumstances the hospital will always ask for express consent:

- Where the hospital is disclosing patient information to someone who is not a HIC (e.g., to a patient's insurer or employer); and
- Where the hospital is disclosing patient information to someone who is a HIC but for purposes other than providing health care.

Where the hospital obtains implied consent, a patient will have been provided with a notice (either posted in a place where they are likely to see it or given to them directly) and a chance to withhold their consent.

A patient may withdraw or limit their consent at any time, unless doing so prevents T&DH from recording the information the hospital requires at law or under professional standards. A patient can give an express instruction that specific information not be used or disclosed.

The hospital may sometimes collect, use or disclose patient information without consent in limited instances that are expressly permitted by PHIPA. For example, some statutes require disclosure of patient information, such as the *Coroners Act* and the *Vital Statistics Act*.

Ontario Wait Times Information System (WTIS) and Enterprise Master Patient Index (EMPI)

PHIPA provides for and governs the collection, use and disclosure of personal health information.

The EMPI contains personal health information relating to patients registered at T&DH and is collected through the Ontario WTIS. EMPI data may include patient identifying information such as patient name, patient demographics eg postal code, date of birth, address, and patient identifiers such as health card number and medical record number. This information is considered personal health information and is protected under PHIPA

The Wait Times Information System (WTIS) is governed by the rules of PHIPA. Hospitals have legal authority to disclose personal health information from the WTIS to Cancer Care Ontario (a prescribed entity under the Act) without patient consent.

Video Monitoring

The hospital recognizes that through the implementation of video surveillance we can provide increased safety to our patients, visitors and staff. Video monitoring is used in public places throughout T&DH. It is not used in areas where there is a reasonable expectation of privacy eg. washrooms and patient rooms. Any recording which includes images of patients becomes personal health information under the Personal Health Information Protection Act 2004. All collection, use and disclosure of such video material will be done within the parameters of the legislation.

Retaining Patient Information and Disposing of Patient Information

We retain patient information in the Hospital or in premises controlled by the Hospital in a secure manner and keep it for as long as necessary to fulfil the purposes for which it was collected, or as required by law.

Timmins and District Hospital has a policy in place to address the retention and destruction of records in the Hospital. This policy sets out minimum and maximum retention periods and complies with applicable laws governing retention of information.

Where a patient has requested access to a record with their information, the hospital will retain that record until the access request is exhausted.

Accuracy of Patient Information

The hospital takes reasonable steps to ensure patient information is as accurate, complete and up-to-date as necessary on collection. The hospital will not routinely update information in its control unless routine updates are necessary to fulfil the purposes for which the information was collected. The hospital takes reasonable steps to ensure that any information that is used by Timmins and District Hospital on an ongoing basis, including any information that is routinely disclosed to others under this Policy, is accurate, complete and up-to-date. Where the hospital knows that information is not accurate, complete or up-to-date, this fact will be indicated at the time of use or disclosure.

Security of Patient Information

Security safeguards protect patient information in the custody or control of Timmins and District Hospital. These security safeguards are in keeping with industry standards and are designed to protect patient information against loss or theft as well as unauthorized access, disclosure, copying, use or modification.

Among the steps the hospital takes to protect patient information are:

- premises security, including locked filing cabinets where cabinets are located in publicly accessible areas;
- restricted access to information stored electronically;

- using technological safeguards like security software and firewalls to prevent hacking or unauthorized computer access; and
- internal password and security policies.

Hospital agents are aware of the importance of keeping patient information confidential. As a condition of employment or obtaining/maintaining privileges, all Hospital agents are required to sign a Confidentiality Agreement, which is reviewed and renewed annually during the agent's performance review.

The hospital will notify the patient at the first reasonable opportunity if their information is lost, stolen, or subject to unauthorized access, disclosure, copying, use or modification.

How to Access Patient Information

A patient can request access to any records in the Hospital's custody or control that contain their information by writing to the hospital's Privacy Officer. The guidelines for processing these requests are available on request. The patient will receive at least a preliminary response from the Privacy Officer within 30 days, and a full response within 60 days.

The patient's right to access their information is not absolute. The hospital may deny access when:

- denial of access is required or authorized by law (e.g., there is a court order prohibiting access); or
- where the request is frivolous or vexatious or in bad faith.

If the Privacy Officer refuses access to a patient's records, there will be a reason given, and the patient will also be notified of their right to complain to the IPC.

A patient is also entitled to challenge the accuracy or completeness of any of their information in the hospital's custody or control. Requests to challenge and/or change a patient's information should be directed to the Privacy Officer. The patient will receive at least a preliminary response from the Privacy Officer within 30 days, and a full response within 60 days.

The hospital will charge a reasonable fee (based on cost recovery) for copies of patient information. We will advise the patient of any fee before copies are made.

Challenging The Hospital

The patient is entitled to challenge the hospital's compliance with the principles set out in this Policy. Please direct any challenge in writing to the hospital's Privacy Officer.

Anyone who submits a written complaint, challenge or inquiry will be given a written copy of the hospital's procedures governing such complaints, challenges and inquiries.

The hospital will investigate all complaints received. If a complaint is found to have merit, the hospital will take appropriate measures to address the complaint, including, if necessary, taking disciplinary action against Hospital agents and/or amending our policies and practices relating to management of patient information.

Compliance with this Policy

All Hospital agents (employees, directors, volunteers, students, and professional staff members) are required to know and comply with this Policy. Confirmation of compliance is required. Any breach of this Policy may result in significant disciplinary action, including:

- for employees and volunteers, suspension, demotion, and termination; and
- for professional staff members, restriction or revocation of privileges, in whole or in part.

Agents may only use patient information as permitted by the Hospital and within the same legal limitations imposed on the Hospital. All agents must notify the Hospital at the first reasonable opportunity if patient information is lost, stolen or accessed without authorization.

The Hospital's Privacy Officer

The Chief Executive Officer ("CEO") of the Hospital is ultimately responsible for ensuring accountability and compliance with this Policy. The CEO appoints a member of our staff to act as the Hospital's Privacy Officer; the Privacy Officer reports directly to the CEO. The Privacy Officer may delegate to others the day-to-day supervision of the collection, use and disclosure of information.

The Privacy Officer for Timmins and District Hospital can be reached at:

(705) 360 - 6055 - phone
(705) 267 - 6311 - FAX

Privacy Voicemail – 705-267-2131 ext 6005
Privacy e-mail privacy@tadh.com

References

Cassels Brock Law Firm