

Management System\Tillsonburg District Memorial Hospital\Administrative Services\General Policies & Forms\

| | |
|--|--|
| Subject: Confidentiality Policy Statement | |
| Distribution: | Document # 14361 Version: Current 2.0 |
| | Last Modified Date: 8/30/2017 12:24:43 PM |
| | Authorized by: Crystal Houze |

This is a CONTROLLED document. Only the original electronic document is to be considered current. Paper copies may be outdated.

Purpose:

To outline the hospital's expectations and standards of behaviour related to confidentiality.
To safeguard and protect the privacy of patients, team members and hospital affiliates, according to legislative requirements and build upon the existing Position Statements/standards of confidentiality established by regulatory and professional bodies.

Policy:

Tillsonburg District Memorial Hospital (TDMH) has a legal and ethical responsibility to protect the privacy of patients/(residents)/clients, their families, and team members/affiliates, and ensure confidentiality is maintained.

TDMH considers the following types of information to be confidential:

- Personal information and personal health information regarding patients/(residents)/clients (hereafter referred to as "patients") and their families;
- Personal information, personal health information, employment information, and compensation information regarding team members and affiliates; and,
- Information regarding the confidential business information of the hospital, which is not publicly disclosed by the hospital

This policy applies whether this information is verbal, written, electronic, or in any other format. Audits are performed to determine compliance.

In addition to standards of confidentiality, which govern Regulated Health Professionals, team members and affiliates are bound by the hospital's responsibility to maintain confidentiality. The hospital expects team members/affiliates to keep information, which they may learn or have access to because of their employment/affiliation, in the strictest confidence. It is the responsibility of every team member/affiliate:

- To become familiar with and follow the hospital's policies and procedures regarding the collection, use, disclosure, storage, and destruction of confidential information.
- To collect, access, and use confidential information only as authorized and required to provide care or perform their assigned duties.
- To divulge, copy, transmit, or release confidential information only as authorized and needed to provide care or perform their duties. (See [Release of Information Patient Information Access and/or Disclosure of Personal Health Information Policy](#))
- To safeguard passwords and/or any other user codes that access computer systems and programs.
- To identify confidential information as such when sending E-mails or fax transmissions and to provide direction to the recipient if they receive a transmission in error.
- To discuss confidential information only with those who require this information to provide care or perform their duties and make every effort to discuss confidential information out of range of others who should not have access to this information.
- To continue to respect and maintain the terms of the [Confidentiality Agreement](#) after an individual's employment/affiliation with the hospital ends.
- To participate in the hospital's Privacy and Confidentiality education program, review this policy, and sign a Confidentiality Agreement before commencing work or the provision of service at TDMH as a condition of employment/appointment/ contract/association for team members/affiliates at TDMH.
- To report to their Leader suspected breaches of confidentiality, or practices within the hospital that compromise confidential information. If the Leader is the individual suspected of the breach, team members/affiliates may contact the Privacy Officer or Human Resources/Chief of Service.

Management System\Tillsonburg District Memorial Hospital\Administrative Services\General Policies & Forms\

| | |
|--|--|
| Subject: Confidentiality Policy Statement | |
| Distribution: | Document # 14361 Version: Current 2.0 |
| | Last Modified Date: 8/30/2017 12:24:43 PM |
| | Authorized by: Crystal Houze |

This is a CONTROLLED document. Only the original electronic document is to be considered current. Paper copies may be outdated.

Misuse, failure to safeguard, or the disclosure of confidential information without appropriate approvals may be cause for disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation with the hospital.

Procedure:

A. General

- Leaders must review any department specific information or procedures related to confidentiality with new team members and affiliates.
- Team members/affiliates may consult their Leader, Professional Practice Leader, Privacy Officer, or Human Resources regarding confidentiality issues or inquiries

B. Confidentiality Agreement

1. Confirmation of the successful completion of the educational program and the signed [Confidentiality Agreement](#) will be kept on the individual's file in:
 - Human Resources for team members, non-medical students, and contract staff.
 - Administration Office for physicians, residents, medical students, dentists, and secretaries who are privately employed by physicians, Medical Department Administrative Officers
 - Volunteer Services for volunteers
 - Service Area under whose supervision, contract staff, vendors, or consultants are working (i.e., any individual employed by third-party organizations who are performing work in the organization on a temporary basis), It is the responsibility of Education Services/Professional Practice Leaders to stipulate in Education Affiliation Agreements with education institutions, the obligation to ensure that students and faculty abide by the hospital's standards of confidentiality.

C. Investigating Alleged Breaches of Confidentiality

It is the responsibility of Leaders, in conjunction with Human Resources, and the Privacy Officer, to investigate alleged breaches of confidentiality.

Fax Transmissions

When sending confidential information (both inside and outside the hospital), emails and fax cover sheets must contain the following confidentiality statements:

CONFIDENTIALITY NOTICE

If you do not receive all of the pages, please telephone our office immediately. The contents of this telecommunication are highly confidential and intended only for the person(s) named above. Any other distribution, copying or disclosure is strictly prohibited. If you have received this telecommunication in error, please notify us immediately by telephone and return the original transmission to us by mail without making a copy. If you do not receive all of the pages please telephone our office immediately.

E-MAIL

Email is not a secure, privacy or confidential mode of information transmission. Confidential or sensitive business, or identifiable patient or team member/affiliate information must not be transmitted by email external to the Hospital secure e-mail system.

Emails containing confidential information sent within the TDMH system must be flagged as "Confidential". Users must also identify the communication as "Confidential" in the subject line. The confidentiality notice below is automatically attached to all e-mails sent **externally**.

Management System\Tillsonburg District Memorial Hospital\Administrative Services\General Policies & Forms\

| | |
|--|--|
| Subject: Confidentiality Policy Statement | |
| Distribution: | Document # 14361 Version: Current 2.0 |
| | Last Modified Date: 8/30/2017 12:24:43 PM |
| | Authorized by: Crystal Houze |

This is a CONTROLLED document. Only the original electronic document is to be considered current. Paper copies may be outdated.

CONFIDENTIALITY NOTICE

This e-mail and any files sent with it contain confidential information and are intended only for the named recipient(s). If you are not the named recipient(s) please telephone or e-mail the sender immediately. You should not disclose the content or take, retain or distribute any copies

Definition of Terms:

Affiliates

Individuals who are not employed by the hospital but perform specific tasks at or for the hospital, including appointed professionals (example, physicians/midwives/dentists), students, volunteers, researchers, contractors, or contractor employees who may be members of a third-party contract or under direct contract to the organization, and individuals working at the organization, but funded through an external source.

Confidential Business Information of the Organization: Information regarding the Organization's business, which is not subject to public disclosure under the Freedom of Information and Privacy Protection Act (FIPPA) and which individuals may come across during the performance of their roles at the Organization, including, but not limited to:

- Information exchanged in confidence with the Government of Ontario or another government or agency.
- Third party information as described in FIPPA 1990, c. F. 31 s. 17(1).
- Information provided in confidence to, or records prepared with the expectation of confidentiality by, a hospital committee to assess or evaluate the quality of health care and directly related programs and services provided by a hospital, if the assessment or evaluation is for the purpose of improving that care and the programs and services.
- Information exchanged with or provided to legal counsel in the process of seeking advice or legal opinion.
- Negotiations related to labour relation matters and settlements.
- Negotiations that give rise to employment or employment contracts.
- Legal matters that involve the hospital that are not public knowledge.
- Plans relating to the management of personnel or the administration of an institution that have not yet been put into operation or made public .
- Information related to intellectual property held by the organization (e.g. information directly included in patients or other intellectual property applications, prior to publication of those patents or applications in public format).
- Information related to the Organization's information technology security and systems access (e.g. remote access credentials; hardware/software vendor names for products which may be vulnerable to external access attacks).

Personal Health Information – As defined by the Personal Health Information Protection Act (PHIPA), identifying information about an individual in oral or recorded form, if the information:

- Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- Is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual,
- Relates to payments or eligibility for health care in respect of the individual,
- Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- Is the individual's health number, or
- Identifies an individual's substitute decision-maker.

Personal Information – As defined by the Freedom of Information and Privacy Protection Act

Management System\Tillsonburg District Memorial Hospital\Administrative Services\General Policies & Forms\

| | |
|--|--|
| Subject: Confidentiality Policy Statement | |
| Distribution: | Document # 14361 Version: Current 2.0 |
| | Last Modified Date: 8/30/2017 12:24:43 PM |
| | Authorized by: Crystal Houze |

This is a CONTROLLED document. Only the original electronic document is to be considered current. Paper copies may be outdated.

(FIPPA), recorded information about an identifiable individual, including:

- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- Any identifying number, symbol or other particular assigned to the individual,
- The address, telephone number, fingerprints or blood type of the individual,
- The personal opinions or views of the individual except where they relate to another individual,
- Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- The views or opinions of another individual about the individual, and
- The individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;
Personal information does not include:
 - Information about an individual who has been dead for more than thirty years
 - The name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.

REFERENCES

Related Policies:

Privacy Policy

Privacy Breach Policy

Release of Patient Information Access and/or Disclosure of Personal Health Information Policy

Release of Patient Information to Law Enforcement Agencies Policy

Security of Confidential Information Policy

Waste Collection and Disposal Policy

Legislation:

Personal Information Protection and Electronic Documents Act, (PIPEDA) (2004)

Personal Health Information Protection Act (PHIPA) (2004)

Public Hospitals Act, 1990 (as amended)

Regulated Health Professional Act, 1991 (as amended)

Freedom of Information and Protection of Privacy Act (FIPPA)