The Ottawa Hospital | L'Hôpital d'Ottawa

ADMINISTRATIVE POLICIES AND PROCEDURES

Privacy
NO.: 00175
(Formerly ADMII260)

ISSUED BY: Chief Privacy Officer

DATE OF APPROVAL: 2004/10/20

APPROVED BY: Senior Management Committee

LAST REVIEW/REVISION DATE: 2012/12/19

CATEGORY: Administration

IMPLEMENTATION DATE: 2004/10/20

POLICY STATEMENT:

At TOH we are committed to protecting the privacy of our patients and the confidentiality and security of all personal health information with which we are entrusted by our patients

DEFINITION(S):

1. **Staff**: For the purposes of this policy, all permanent or temporary, full-time, part-time, casual or contract employees including physicians, residents, interns, volunteers, students and members of affiliated organizations.

2. **Personal Health Information (PHI)**: All identifying information about an individual in oral or recorded form, if the information relates to:
   - **i.** the individual's physical or mental health, including family health history;
   - **ii.** the provision of health care to the individual, including identification of the health-care provider;
   - **iii.** payments or eligibility for health care, or eligibility for coverage for health care;
   - **iv.** donation of body part or bodily substance;
   - **v.** the individual's health number; or
   - **vi.** identification of an individual's substitute decision maker.

3. **Privacy breach:** The unauthorized access, collection, use or disclosure of any personal information or personal health information. Breaches can be intentional (e.g. purposely accessing information on your ex-partner when you do not require such information for your job) or inadvertent (e.g. accidentally sending a report to the wrong fax number). Breaches also include a failure to protect personal information or personal health information with which an employee or agent is entrusted (e.g. leaving health records unattended, sharing passwords or discussing personal health information via social media).

4. **Collect**: To gather, receive or obtain personal health information from any source and may be collected in any manner, e.g. written, verbal, electronic or photographic, etc.

5. **Use**: To handle or deal with personal health information, including the sharing of such information between TOH and any of its agents, but does not mean to disclose personal health information.

6. **Disclose**: To release or make personal health information available to another person, organization or health information custodian; it does not mean to use.

7. **Implied consent**: When one may conclude from surrounding circumstances that a patient would reasonably agree to the collection, use or disclosure of the patient's personal health information.

8. **Express consent**: When a patient explicitly agrees to the collection, use or disclosure of their personal health information, which can be given in writing, orally, by telephone or electronically.

9. **Privacy**: The right of individuals to determine for themselves when, how and to what extent personal information about them is communicated, and the right to be secure from unauthorized use or disclosure of their personal health information.

10. **Agent**: Person authorized by TOH to act for or on behalf of TOH to deal with patients' personal health information, whether or not the agent has authority to bind the custodian, is employed by TOH, or is being paid (e.g., employees, physicians, volunteers, contractors, students, suppliers).

ALERTS: N/A

PROCEDURE:

The following section sets out the fundamental privacy principles and TOH's responsibilities for *Personal Health Information Protection Act* (PHIPA) compliance.

1. Accountability

TOH staff members demonstrate their accountability for individual privacy rights and compliance by respecting the fundamental principles and rules for the collection, use,

disclosure, retention and disposal of personal health information (PHI) found in the *Personal Health Information Protection Act* (PHIPA), and by adhering to all TOH privacy and security policies, procedures and guidelines.

Violation of this policy is grounds for disciplinary action up to and including dismissal or termination of hospital privileges. In addition, privacy breaches involving regulated health professionals will be reported to their respective colleges.

TOH staff members are responsible for reporting any known breach of privacy to their manager and the Privacy Officer. TOH will inform patients of the loss, theft or inappropriate access of their personal health information as soon as reasonably possible.

TOH has appointed a privacy contact person – the Privacy Officer – who is responsible for facilitating TOH's compliance with the PHIPA; ensuring that all staff members are appropriately informed of their duties under the PHIPA; responding to inquiries from the public about TOH's information practices; ensuring that requests for access to or correction of a record of personal health information are processed; and receiving complaints from the public about any alleged contraventions of the PHIPA.

TOH is responsible for personal health information transferred to a third party for processing and will use contractual agreements or other means to ensure a comparable level of protection whenever information is transferred.

2. Identifying purposes and limiting collection, use and disclosure

The Ottawa Hospital (TOH) collects, uses, discloses and retains personal health information (PHI):

- **i.** to provide patient care;
- **ii.** to monitor and evaluate the quality of care we provide;
- **iii.** to administer and manage the operations of the hospital;
- **iv.** to do research, educate and collect statistics;
- **v.** to comply with legal and regulatory requirements; and
- **vi.** to raise funds through The Ottawa Hospital Foundation.

TOH shall collect no more information than is necessary to fulfill these purposes.

When staff members provided with appropriate access log into the TOH network, a notice automatically appears reminding them that they may access PHI only on a need-to-know basis, that their access to PHI in the database will be tracked and audited to ensure compliance, and that failure to comply will result in disciplinary measures up to and including termination. These individuals must affirmatively select "Accept" or "Cancel" before proceeding.

3. Consent

TOH may collect, use and disclose PHI if a patient consents or where PHIPA permits or requires the collection, use and disclosure of PHI.

If TOH receives personal health information from a patient or another custodian for the purpose of providing health care to that patient, TOH is entitled to assume the patient's implied consent to collect, use and disclose to another custodian unless TOH becomes aware that the patient has withdrawn his or her consent.

If collection, use or disclosure is for purposes other than health-care-related, express consent must be obtained (e.g. when TOH discloses to a non-custodian).

There are circumstances that allow the collection, use or disclosure without consent, such as the following:

- **i.** Where there is no time to collect the information directly with consent;
- **ii.** Where use is to manage risk and errors, or improve quality of care or services; or,
- **iii.** Where disclosure is necessary to prevent serious bodily harm or reduce a significant risk of harm to any person.

Individuals may withdraw their consent at any time (see Policy # 00205 - Locking Patient Health Information Records).

4. Accuracy

Staff should record PHI when it is collected or as soon as possible afterward. Whenever possible, the person collecting should be the one recording PHI and that person's name should be documented and any errors corrected immediately.

5. Safeguards

TOH employs various security safeguards to protect PHI against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. These include:

i. Physical: Locking file cabinets; restricting office access; not leaving PHI in unsecured areas where unauthorized personnel or members of the public could access it.

ii. Administrative: Confirmation of identity before providing access to PHI outside TOH; sign-out procedures for health records; policies and procedures; requirements to sign confidentiality agreement; awareness and training sessions.

iii. Technical/Electronic: Strong password requirements; expectation to not share; use of encryption; auditing to trace and rectify any privacy breaches; electronic reminders.

6. Transparency and openness

TOH has various materials to increase transparency to patients. These include Notice to Patients, Patient Brochure, Frequently Asked Questions and the current Privacy Policy that informs the public and staff about TOH's privacy practices. These materials are located on TOH's website.

7. Access

TOH will respond to an individual's access request within the response time detailed in PHIPA and processed through the Health Records department. Verification of identity is required and a reasonable fee may apply.

When an individual successfully demonstrates the inaccuracy or incompleteness of personal health information, TOH will amend the information as required by law. Amendments may involve 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.

8. Challenging Compliance with TOH's Privacy Practices

An individual may bring forward his or her complaint about TOH's privacy practices to the Privacy Officer. Instructions for making complaints are posted on TOH's website. All complaints will be investigated and TOH will take the necessary steps to address them in a timely manner.

RELATED POLICIES / LEGISLATION:

1. Personal Health Information Protection Act

2. Corporate - Administration Policy # 00270 – Information Systems - Desktop Request Policy

3. Corporate - Administration Policy # 00268 – Information Systems - E-mail Access and Usage Policy

4. Corporate - Administration Policy # 00253 – Occupational Health and Safety - Employee Health Records and Disclosure of Information

5. Corporate – Administration Policy # 00184 - Communications - Intra-Hospital Release of Information

6. Corporate – Administration Policy # 00195 - Communications - Ownership and Security of the Health Records

7. Corporate - Administration Policy # 00182 - Communications - Faxing Confidential Information

8. Guidelines for Investigating Privacy Breaches and/or Complaints

9. Corporate - Administration Policy # 00205 - Communications - Locking Patient Health Information Records

10. Correction of Health Records Policy

11. Lydia Wakulowsky, Personal Health Information Protection Act: Implementing Best Privacy Practices, 2nd edition, Lexis Nexis, 2011

REFERENCES: N/A

COMMENTS / SIGNIFICANT REVISIONS: N/A