Thames Valley Family Health Team	**Policy:** **Privacy Breach Involving Personal Health Information**	**Code Number** **Pages: 4**
	Approval Date: November 7, 2017 **Approval Body:** TVFHT Executive Director	**Last Review Date:** **Last Revision Date:**

This policy applies to: Thames Valley Family Health Team[1] and our staff members and to personal health information (PHI) held in the custody or control of Thames Valley Family Health Team (examples: PHI collected in relation to health wellness programs delivered by the TVFHT and PHI collected in the process of completing mandatory reporting to the LHIN and MOHLTC and stored on TVFHT network or devices). This policy does not directly apply to personal health information stored in electronic medical records (EMR) held in the custody of Physicians/Family Health Organizations/Networks or Hospitals partnering with the Thames Valley Family Health Team, who are also, each, Health Information Custodians (PHIPA, 2004) governed by Ontario's privacy legislation. This policy and its related procedures are intended to ensure TVFHT's compliance with Ontario's privacy legislation and to complement and support policies and procedures established by the partner Physicians/Family Health Organizations/Networks and Hospitals.

Thames Valley Family Health Team requires anyone who collects, uses or discloses personal health information on our behalf to be aware of our policies and procedures related to Access to and Disclosure of Personal Health Information and the importance of complying with this policy and its related procedures.

Thames Valley Family Health Team (TVFHT) staff members working as agents of Health Information Custodians (HICs) partnering with TVFHT are expected, in compliance with Ontario's privacy legislation and within the scope of their individual role responsibilities, to act on behalf of the applicable HIC to any actual, suspected or potential breach of privacy related to patients' personal health information held within the custody or control of the partnering HIC (example: PHI held in the EMR). In response to an actual, potential or suspected breach of privacy involving PHI, TVFHT staff members will comply with privacy policies and procedures of the applicable Health Information Custodian wherever available, but may refer to procedures associated with this TVFHT policy wherever it is useful to do so, to assist in ensuring compliance with Ontario's privacy legislation.

[1] Throughout this policy we use "Thames Valley Family Health Team" (TVFHT) to refer to everyone employed at Thames Valley Family Health Team as well as other individuals working with or on behalf of TVFHT such as students/learners, researchers, Board of Director members, and volunteers. This excludes physicians, Family Health Organizations/Networks and Hospitals who partner with TVFHT.

Thames Valley Family Health Team (TVFHT) as a Health Information Custodian under the Personal Health Information Protection Act (PHIPA) 2004, is responsible and accountable for the privacy and security of the personal health information (PHI) held in its custody or under its control. TVFHT staff members working as agents for other Health Information Custodians partnering with TVFHT are also responsible, within the scope of their individual professional standards and their individual role responsibilities to:

- handle PHI held in the custody or control of the partnering HICs in a manner that protects its privacy and security regardless of the storage of the record or the medium of the information, and
- comply with the partnering HIC's policies and procedures regarding management of personal health information and privacy breaches.

A privacy breach occurs whenever PHI is:

- lost or stolen, or
- accessed, disclosed, copied or modified without authority, or
- disposed of in an insecure manner, or
- managed in any manner that contravenes, or there is a risk of contravention of the Personal Health Information Protection Act (PHIPA) 2004

A privacy breach can occur via verbal or written communication, by phone, e-mail, fax, electronic means or any other medium. A privacy breach can be potential**,** suspected, or actual (see definitions for examples).

By law (PHIPA 2004), TVFHT must notify a patient, if capable, or the patient's Substitute Decision Maker (hereafter referred to as patient/SDM), if the patient is not capable, if there has been a breach of their privacy related to their PHI.

TVFHT is also obligated to provide the Privacy Commissioner with a yearly high level summary report on privacy breaches occurring with information under TVFHT's custody and control, specifically on the number of times personal health information is stolen, lost, or used without authority or disclosed without authority.

TVFHT staff members are responsible to:

- Comply with their professional obligations as well as TVFHT policies, and when acting as an agent of a partnering HIC, also comply with the partnering HIC's policies related to confidentiality and privacy;
- Protect and secure PHI to prevent a breach of a patient's privacy ;
- Immediately notify their supervisor or the TVFHT or FHO/N Privacy Officer (as applicable), if made aware of a potential, suspected or actual privacy breach or if made aware of a complaint by a patient about an alleged breach;
- Participate in the investigation and management of a privacy breach, as applicable.

Supervisors are responsible to:

- Ensure that the applicable Privacy Officer(s) are aware of a potential, suspected or actual privacy breach;
- Promptly investigate suspected breaches and respond to the Privacy Officer following the Breach Procedures;

- Collaborate with the Privacy Officer to promptly contain and investigate a breach to reduce risk of further breach;
- If a breach is confirmed, in collaboration with the Privacy Officer:
  - notify the affected patient(s). If the patient is deceased, consult with the Privacy Officer related to the organization's obligations,
  - review the details of the breach and information obtained as part of the investigation and put measures in place to reduce the risk of reoccurrence.

Privacy Officers are responsible to:

- Implement the Privacy Breach Protocol.
- Notify the supervisor if made aware of a potential, suspected or actual privacy breach,
- Depending on the severity of the breach, bring together the appropriate parties from impacted organizations to facilitate the investigation and management of the breach,
- Where applicable, submit a report outlining the breach, the investigation, patient notification and outcome to the Office of the Information Privacy Commissioner of Ontario and work with the Commissioner's Office to ensure the organization has met its legal obligations under PHIPA.
- Ensure that privacy breach statistics are tracked and provide the Privacy Commissioner with a yearly report on privacy breaches within the last calendar year.

Breach of privacy may be cause for disciplinary action up to and including termination of employment or contract or loss of appointment with the organization.

DEFINITIONS

Affiliates – Other individuals working with or on behalf of TVFHT such as students/learners, researchers, Board of Director members, and volunteers.

Personal health information is any identifying information with respect to an individual, whether living or deceased, and includes:

- Information concerning the physical or mental health of the individual;
- Information concerning any health service provided to the individual, including the identification of the person that provided health care to the individual;
- Information concerning the donation by the individual of any body part or any bodily substance of the individual;
- Information derived from the testing or examination of a body part or bodily substance of the individual;
- Information that is collected in the course of providing health services to the individual; or
- Information that is collected incidentally to the provision of health services to the individual.

Privacy Breach – Actual - includes, but is not limited to:

1. Accessing patient personal health information when it is not required to provide or maintain care to a patient or in the performance of duties, for example:
   - Accessing one's own electronic health record directly, rather than by adhering to the approved procedure for accessing one's own PHI,
   - Accessing the health record of another staff member, a family member, friend, or any other person for whom you do not have a requirement to view the information in order to provide health care or perform work related responsibilities,

- Accessing any patient information (e.g., address, date of birth, next of kin, etc.) of a staff member, family member, friend, or any other person for whom you do not have a requirement to view the information in order to provide health care or perform work duties.

2. Disclosing patient information:
   - Without the appropriate consent, e.g. to a lawyer or insurance company
   - To another staff or affiliate who does not require access to the information to perform his or her role responsibilities,
   - By discussing within hearing range of other people who do not require access to the information to perform their role responsibilities,
   - By faxing or mailing PHI to the wrong recipient at a private home or business
   - By posting PHI to a social networking site e.g., a blog.

3. Leaving patient information in unattended or unsecured locations where it may be accessed by unauthorized persons. For example:
   - Leaving patient reports, files, or worksheets that contain patient-identifying information in a public area,
   - Leaving access to electronic patient information unattended on an open log in,
   - Storing electronic patient-identifying information on portable information devices or unsecured drives, e.g., hard drives, memory sticks that have not been encrypted
   - Theft of electronic devices that contain patient-identifying information
   - Loss of hard copy records or other patient-identifying information.

Privacy Breach – Potential – occurs when an individual's personal health information is at high risk of being accessed, used or disclosed inappropriately. A potential privacy breach includes, but is not limited to situations in which a patient:

- Alerts the supervisor or the Privacy Officer that a staff or affiliate may access information about him/her inappropriately,
- Requests additional security measures for his or her personal health information.

Privacy Breach – Suspected – occurs when there has been an allegation of a privacy breach, but the allegations have not yet been substantiated or refuted by investigation e.g., a supervisor may receive a complaint or report from a person stating that he/she has witnessed a breach of privacy; or a patient may contact a Privacy Officer alleging that a family member has personal health information about the patient that they have no legitimate reason to have.

Supervisor – for the purpose of this policy a supervisor is the person that the TVFHT staff member directly reports to within the TVFHT structure, but may also be a:

- Coordinator,
- Director or his/her delegate,
- The TVFHT Executive Director

REFERENCES

Personal Health Information Protection Act, 2004 Public Hospitals Act 1990 (as amended)
Regulated Health Professions Act 1991 (as amended)
Professional Standards: College of Medical Laboratory Technologists of Ontario
College of Nurses of Ontario, Standards of Practice – Confidentiality and Privacy - Personal Health Information College of Occupational Therapists (select practice

standards/Guidelines/Position Statements, Practice Guideline: Client Records)
College of Pharmacists of Ontario
College of Physicians and Surgeons of Ontario – Confidentiality and Access to Patient Information
College of Physiotherapists of Ontario - Privacy Code
College of Psychologists of Ontario
College of Social Workers and Social Service Workers – Privacy Toolkit