Thames Valley Family Health Team	**Protocol:** **Privacy Breach Protocol**	**Code Number** **Pages: 6**
	Approval Date: November 7, 2017 **Approval Body:** TVFHT Executive Director	**Last Review Date:** **Last Revision Date:**

About this Protocol:

This protocol provides information and direction to TVFHT staff members, affiliates and supervisors when they identify, or are made aware of a potential or actual privacy breach. These procedures are an adjunct to the TVFHT Privacy Breach Policy. The Personal Health Information Protection Act 2004 (PHIPA) requires TVFHT, as a Health Information Custodian, to take reasonable measures to protect PHI against loss, theft, unauthorized access, use or disclosure. Rapid action in response to an actual, potential or suspected privacy breach is critical and is part of everyone's responsibility for protecting patients' personal health information (PHI).

Annually, the TVFHT's Co-Privacy Officers will submit a privacy report to the Board of the Thames Valley Family Health Team.

What is a Privacy Breach?

A privacy breach occurs when a person contravenes or is about to contravene a rule under the Personal Health Information Protection Act, 2004 (PHIPA) or our privacy policies. The most obvious privacy breaches happen when patient information is lost, stolen or accessed by someone without authorization. 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 **actual**, **potential** or **suspected**. Examples of privacy breaches include:

- A fax is misdirected
- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package is not delivered to the correct address
- A USB key is lost
- A patient reads another patient's health record on a computer while waiting in a clinic room
- A test result is filed on the wrong patient's chart
- Someone talks about a patient of the Family Health Team with a friend
- Health records meant for destruction are recycled and not shredded
- Out of curiosity or concern, a staff member reviews a neighbour's health record
- Health Information is given to the media
- A staff member makes a copy of an ex-spouse's health record without the permission of the patient.

A privacy breach can result in:

- Loss of public trust
- Fines levied against individuals and/or organization[1]
- Legal action against the individual(s) and or the organization by a patient
- Criminal charges
- A patient complaint to the organization and/or to the Ontario Information and Privacy Commissioner (IPC)
- An Order by the IPC requiring remedial action by the organization related to the issue resulting in the breach, which in turn, sets a standard for all Ontario Health Information Custodians and results in media attention, potential fines levied against either or both the individual and the organization by the IPC under PHIPA and its regulations.

Further Examples of Actual, Potential and Suspected Privacy Breaches

Actual Privacy Breaches may also include, but are not limited to:

a. Accessing information on any patient:

- When the information is not required by the employee/affiliate to perform the work duties for which he/she was hired or affiliated. This includes searching for and/or opening the electronic record of family members, friends, co- workers and includes accessing personal information and/or personal health information,
- Directly accessing one's own electronic health record without following the approved process (see the process for "Staff Member Seeking Access to his/her own health record or the health record of a family member or friend" found in the Access to and Disclosure of PHI Policy and Procedure).

b. Disclosing identifiable patient information including photographs and diagnostic images:

- without the patient's informed written consent for any purpose to individuals outside the patient's circle of care,
- without the type of consent relevant to the disclosure e.g., express written consent to disclose to a lawyer or insurance company
- to another employee or affiliate who does not require the information to perform his or her job functions,
- by discussing within hearing range of other people who do not require the information to perform their job functions,
- by faxing or mailing to the wrong recipient e.g., to a private home or business
- by posting to a social networking site, e.g., a blog

[1] More information is found at: https://www.ipc.on.ca/health/breach-reporting-2/potential-consequences-of-a-breach-under-phipa/)

c. Leaving patient information in unattended or unsecured locations where it may be lost, stolen or accessed by unauthorized persons. For example:
   - Leaving patient reports, charts, 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 outside the organization's secure network on unencrypted devices/drives e.g., hard drives, laptops or memory sticks resulting in the information being accessible if the device is lost or stolen,
   - Loss or theft of hard copy records or other patient identifying information.

Potential Privacy Breaches occur when an individual's personal health information is at high risk of being accessed, used or disclosed inappropriately. For example:

- A patient alerts a staff member, affiliate, supervisor or the Privacy Office that a an employee or affiliate may access information about him or her inappropriately,
- A patient requests restriction to the use and/or disclosure of his or her personal health information. (See the Patient Requests to Restrict the Use and Disclosure of Personal Health Information Policy).
- A well-known TVFHT staff member or member of a Physician/FHO/Network or Hospital partnering with TVFHT is experiencing health problems and may be away from work for an extended period related to health issues,
- A high profile member of the community is being treated by a TVFHT staff member or a Physician/FHO/Network or Hospital partnering with TVFHT,
- An individual or patient of one of the Physicians/FHO/Networks or Hospitals has recently been profiled in the media, or
- A person has been profiled in the media following a local tragedy or alleged criminal act.

Suspected Privacy Breaches occur when there has been an allegation of a privacy breach, but the allegations have not yet been substantiated or refuted by investigation, including (but not limited to):

- An individual witnesses another staff member or colleague accessing a patient's record when they are not part of that patient's care team, nor do they require that person's personal information to support that patient's care team in the delivery of health care to that patient,
- A patient reports that they believe a staff member has inappropriately accessed his or her personal health information, or
- An individual overhears two staff members discussing another patient's personal health information and reports it to his or her physician (or any staff member),

Privacy Breach Protocol

The following steps must be taken when an actual potential, or suspected breach of privacy is identified.

Note: Depending on the type of breach, these steps…

- May not all occur;
- May not be sequential; or
- Could occur concurrently

Step 1: Implementing the privacy breach protocol	
Most responsible person:	**Action**
Person becoming aware of the breach (either by witnessing it personally or receiving information from patient or other party)	Respond **immediately** by implementing this Privacy Breach Protocol • Ensure appropriate staff members within the Thames Valley Family Health Team are immediately notified of the breach. This includes your immediate supervisor and/or one of the two TVFHT Co-Privacy Officers. • If applicable, supervisor and/or TVFHT Co-Privacy Officers would notify appropriate individuals at the FHO/N or Hospitals partnering with TVFHT.

Step 2: Containment - Identify the scope of the potential breach and take steps to contain it	
Most responsible person:	**Action**
TVFHT Privacy Officer(s) (May delegate this responsibility to supervisor as appropriate)	• Retrieve the hard copies of any personal health information that has been disclosed. • Ensure that no copies of personal health information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required. • Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g., change passwords, temporarily suspend access and/or temporarily shut down a system).Consider notifying the Information and Privacy Commissioner/Ontario (IPC/O) and/or legal counsel if appropriate.

Step 3: Notification - Identify those individuals whose privacy was breached and notify them of the breach	
Most responsible person:	**Action**
TVFHT Privacy Officer(s) (May delegate this responsibility to supervisor as appropriate)	• At the first reasonable opportunity, any affected patients (or others whose personal health information has been affected) will be notified. • The type of notification will be determined based on the circumstances (such as the sensitivity of the personal health information, the number of people affected, and the potential effect the notification will have on the patient(s)). For example, notification may be by telephone or in writing, or depending on the circumstances, a notation made in the patient's file to be discussed at his/her next appointment. • Provide details of the extent of the breach and the specifics of the personal health information at issue. • Advise affected patients of the steps that have been or will be taken to address the breach, both immediate and long-term. • Consider notifying the IPC/O and/or legal counsel if appropriate.

Step 4: Investigation and Remediation	
Most responsible person:	**Action**
TVFHT Privacy Officer(s) TVFHT Executive Director (if this individual is not a Privacy Officer (may delegate to Senior Director and/or Supervisors as appropriate)	• Conduct an internal investigation into the matter. The objectives of the investigation will be to: a) Ensure the immediate requirements of containment and notification have been addressed. b) Review the circumstances surrounding the breach. c) Review the adequacy of existing policies and procedures in protecting personal health information. d) Address the situation on a systemic basis. e) Identify opportunities to prevent a similar breach from happening in the future. • Change practices as necessary. • Ensure staff are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future. • Continue notification obligations to affected individuals as appropriate.

Step 4: Investigation and Remediation	
Most responsible person:	**Action**
	• Consider notifying the IPC/O and/or legal counsel as appropriate. • Consider any disciplinary consequences with staff or contract issues with independent contractors or vendors that follow from the privacy breach. • Ensure privacy breach statistics are kept in order to comply with obligation to report yearly to the Privacy Commissioner.