Thames Valley Family Health Team	**Policy:** **Safeguards for Personal Health Information Policy**	**Code Number**
		Pages: 12
	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 associated guidelines 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 Safeguarding of Personal Health Information Policy and the importance of complying with this policy and its associated guidelines.

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 utilize best practices to protect the confidentiality and security of Personal Health Information held within the custody or control of the partnering HIC (example: PHI held in the EMR). TVFHT staff members working as agents of HICs partnering with TVFHT will comply with privacy policies and procedures of the applicable Health Information Custodian wherever available, but may refer to procedures and guidelines 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 undertakes to put into place safeguards for the personal health information we hold, which include:

- Physical safeguards such as locked filing cabinets and rooms,
- Organizational safeguards such as permitting access to personal health information by staff on a “need to know” basis only; and
- Technological safeguards such as passwords, encryption and audits.

Thames Valley Family Health Team takes steps to ensure the personal health information we hold is protected against theft, loss and unauthorized access, copying, modification, use or disclosure regardless of the format in which the personal health information is held.

Care is used in the storage, transfer, disposal or destruction of personal health information to prevent unauthorized parties from gaining access to the information.

This policy and its associated guidelines fulfill a portion of Thames Valley Family Health Team’s commitment to protect the privacy, security and confidentiality of patient’s personal health information as indicated in our Privacy Policy. Following this policy and its associated guidelines will minimize the risk of patient information falling into the wrong hands which could cause harm and distress to patients and legal consequences for the Thames Valley Family Health Team and its partners. We require everyone who is affiliated with the Thames Valley Family Health Team to follow the best practices described here. Every team member has a role in keeping our patients’ information secure, and we expect everyone to fulfill that role.

Restricted Access to Patient Information

Access to patient information is provided on a need-to-know basis as appropriate to the staff member’s role and purpose for access. Staff members must not access any health information unless authorized - which means only for reasons that are necessary to their role. Staff members may not access health information of their spouses, children, parents, friends or neighbours, or work colleagues. They may only access their own health information (if applicable) through the normal access channels used by all patients and not directly (refer to the Access and Disclosure of Personal Health Information Policy and Procedure).

Staff members must not:

- Access patient information for "self-education" or out of personal interest
- Edit, cut-and-paste, delete from or otherwise change any health information except for legitimate reasons

Staff should be aware that all access to the electronic medical record (EMRs are owned by the Physician/Family Health Organization/Network or Hospital partnering with TVFHT) is logged and may be audited.

Confidentiality Agreements

All Thames Valley Family Health Team staff members and other individuals working with or on behalf of Thames Valley Family Health Team such as students/learners, researchers, Board of Director members and volunteers will sign a Confidentiality Agreement prior to employment/engagement.

Network/Computer Accounts and Passwords

Our information technology systems are protected by the use of personal accounts and passwords. Individual accounts are given access to information required by the account holder. We require all staff to:

- Use only their own user account and password
- Not permit anyone else to use their account
- Help maintain security by choosing hard-to-guess passwords
- Contact a Privacy Officer if they suspect any kind of computer misuse

On occasion, TVFHT may choose to implement a shared account of some nature for specific operational purposes (e.g., multiple people participating in an OTN conference where only one person logs in, or a shared email account for a specific operational function).

This kind of shared account can only be created with approval from the TVFHT Privacy Officer. TVFHT will create and enforce specific rules about how the account will be used and who will use it. Where this occurs:

- Only those identified as authorized users may access or use that account in the manner and for the purpose which it is has been created.
- Authorized users will not share their passwords or responses to security questions.

An unauthorized person trying to gain access to health information may not be obvious. Data breaches have occurred in other organizations after "confidence tricks" convinced individuals to reveal passwords or other information to intruders, for example claiming to be the "IT helpdesk". Never tell anyone your password no matter who they say they are. If anyone you do not know requests information from you, you must verify their identity and their reason for asking, first. If you are left in any doubt contact a Privacy Officer immediately.

Physical Security On-Site

In carrying out our roles we handle a large amount of patient information in printed format - on paper, in files and binders. Daytimers, schedules and notebooks may also contain patient information and are confidential just as patient files are.

Access to patient information is permitted by individuals who require the information to do their authorized jobs. If patients or visitors are in areas where patient information is kept or in other private areas, politely challenge them as to their business. If there is any doubt as to someone's purpose, they should be asked to leave.

Patient information in paper format should be kept in a locked cabinet, container or room. If a filing cabinet or room where patient information is stored is not in constant use, it should be locked.

Where records are on desks or in in-trays they should be turned over so they cannot be read by someone nearby. Such records should be locked in secure cabinets after hours and on weekends/holidays.

Labels on files should not be visible to visitors.

Patient information that is being stored before secure destruction is carried out, will be kept in a secure location, separate and clearly marked – Confidential Information For Destruction.

Patient Information in Transit

Because of the serious risk of loss or theft, patient information will only ever be removed from the premises by those staff members who have a real need to do so to carry out their duties. This applies to electronic files, paper copies and information on laptops, smart phones, disks and memory sticks (USB keys) and any other formats.

For electronic files, remote access to patient information should be through a secure server, where we can protect it. Every time patient information is saved to a laptop, disk or memory stick there is a chance it may be lost or stolen. Therefore we will do this only when absolutely necessary to carry out our jobs.

Where there is no choice but to take information off-site, patient information will be properly de-identified if possible. Otherwise, if staff members are ever required to copy patient information onto a laptop, memory stick or other portable device strong encryption must be used. If you are not sure how to do this, contact your supervisor. For paper files, keep papers in a locked box for transport.

When in public, steps should be taken to avoid drawing attention to the materials (such as keeping them in an unmarked bag or container).

Endeavour not to leave laptop computers, disks or files on the seat or in the trunk of an unattended car, even for just a few moments.

When transporting patient information, go directly to the destination, making the journey as short as practicable.

Endeavour not to store patient information should not be stored at home or make printouts from remote access at home.

Sending Patient Information

Special care must be taken when sending correspondence about a patient or containing patient information to anyone outside of the Thames Valley Family Health Team - including to another health-care provider, to a third party, or to the patient[2].

In addition to adhering to this policy, physicians and integrated health providers (collectively, “clinicians”) need to follow their own regulatory College’s directives on confidentiality, security of personal health information and communicating with patients to ensure privacy is protected.

External Emails to Health Care Providers and Third Parties

Personal Health Information (with only limited exceptions) is NOT to be included in any email sent by a TVFHT staff member unless using one of the following secure email systems:

[2] If emailing with patients, refer to TVFHT’s Email Communication with Patients Policy.

1. The information is being sent from a ONE MAIL email address and it has been confirmed that the recipient email address is also a ONE MAIL email address, OR
2. The Health Care Professional sending the confidential email has encryption software on his/her system that encrypts outgoing email messages and requires a password to be opened[3];

Mandatory Process -- if a TVFHT employee is sending confidential information via email:

- There must be a disclaimer message at the end of the email message being sent (see Appendix A);
- The clinician must have an automatic response email for all incoming email messages (see Appendix B);
- Before sending, the Health Care Professional must check the email address carefully to confirm it is going to the correct recipient *(NOTE: email programs that "autofill" the recipient field can insert an address you did not intend to send to)*;
- The clinician should avoid using the "reply-all" feature and limit the number of recipients to the minimum necessary;
- The email message must be copied and entered into the health record or the Health Care Professional must write a note in the health record summarizing the clinically relevant information from the email communication; and

The email may only include the minimum amount of personal health information necessary for the purpose.

Emails Sent within Thames Valley Family Health Team
When sending emails within TVFHT, take note if the intended recipient is utilizing an eHealth Ontario's One Mail email address and limit the personal information included to the minimum necessary. Refer to patients by their initials rather than using their full names, if it is possible to do so. Outgoing information is only encrypted if both the sender's and the recipient's email addresses are One Mail addresses.

When using the "reply-to" feature there is a risk of including more information than necessary by including a copy of the original email. Therefore, start a new email rather than responding to an email thread.

Carefully check the recipient address before hitting the send button. Email programs that autofill the recipient field can insert an address you did not intend to send to.

[3] The CPSO policy on Medical Records reads: "E-mails may not be secure. Therefore, physicians who wish to send personal health information by e-mail must obtain express consent to do so from the patient or their representative unless they have reasonable assurances that the information sent and received is secure. Physicians should use a secure e-mail system with strong encryption.

Avoid using the "reply-all" feature and limit the number of recipients to the minimum necessary.

Accessing Email on a Mobile Device
To access TVFHT email on a smartphones, open Outlook Web Access in your browser and enter your username and password.

Avoid using the Outlook app to access TVFHT email on your smartphone – the app stores email information on your device and this could cause a privacy breach if your device is stolen or deactivated.

Facsimile (Faxes)
If possible, remove personal identifiers such as names and addresses from information that is to be faxed.

Misdirected faxes are easy to send and difficult to correct. They make up a significant proportion of privacy breaches. Therefore when sending patient information by fax, carefully check the fax number - multiple times - to ensure it is correct.

Include a cover sheet stating for whom the fax is intended. The cover sheet must ask a recipient to call if information is received in error.

Where appropriate, call the recipient prior to sending a fax so they can be waiting to retrieve it.

If you are using a fax machine that is separate from the EMR, you may decide to collect and keep a confirmation receipt depending on the nature of the fax you're sending. If there is any question about a wrong number being used, the receipt will make it much easier to check and to retrieve information sent to the wrong place. The confirmation receipt should be scanned into the EMR for safekeeping and the paper version should be disposed of securely.

Social Media
Staff are advised to avoid posting information about patient-specific cases or providing medical or other clinical **advice** online. Regulatory colleges and professional liability indemnity providers recommend that clinicians avoid posting comments in internet discussion forums or other online groups to avoid the perception of providing medical or health care **advice**. While it may be acceptable to provide general health-related information for public or professional educational purposes, those purposes should be clearly identified and clearly marked as not providing **advice**. (Refer to TVFHT's Guidelines for Safe Social Media Activity).

Telephone
Patients may ask us to relay their own health information to them by telephone. Calling a patient at home or at work or leaving messages carries a real risk to our patients' privacy. It may be difficult to verify the identity of the person who answers or control who hears a message.

To minimize these risks, ask patients every time they register for an appointment to check that their contact information is up to date so we have their most recent telephone

numbers (and home address – see mail below). Ask if we can leave a message with someone or on an answering service and confirm the number.

If we have the patient's consent to leave a message and your call is answered by a message machine, listen for clues that you may have misdialed before leaving a message. For example, if the message repeats a name or number other than the one you expected to hear. If you are in any doubt leave a message only to say to call the office.

At all times when leaving messages, leave only the minimum information required on the message. Do not provide information about test results or the reason for an appointment unless the patient has expressly asked you to do so in that specific instance.

If a patient calls us we must take steps to confirm the caller's identity before providing information. Our patients expect it. If we are in doubt as to the identity of the caller, we can confirm the caller’s identity by asking questions such as:

- When was your last appointment with us?
- What medications are you currently taking?
- What allergies do you have?
- What is your health card number?

Mail
Sometimes it is necessary to send patient information by mail or courier. When sending information in the mail, check the address to make sure it is correct. Also, mark the envelope or package "Attention <name>" on the outside to make sure it is opened only by the intended recipient.

Make sure that no health information can be read through the envelope or window.

Obtain a tracking number when sending mail by any method other than general mail and follow up with the patient to make sure it was received.

Text and other Direct Messaging

Texting and direct messaging do not have many of the necessary safeguards in place to protect employees or patients, or to meet legislative or documenting requirements.

As a result, texting and direct messaging with patients is not permitted. However, if you believe you have an exceptional situation that would make texting or direct messaging with a patient necessary, you must notify a TVFHT Privacy Officer to discuss the circumstances.

Destroying Patient Information

When patient information is no longer needed it must be destroyed securely. Different methods of destruction are appropriate depending on how the data is stored:

Material	Appropriate Method of Destruction
Paper (e.g., printouts, faxes, letters, labels, etc.)	Cross Cut Shredding – Use secure confidential waste containers available in all TVFHT office areas
CDs, DVDs, disks, USB keys	Shredding or magnetically erasing or overwriting the information in such a way that the information cannot be recovered
Audio or video tapes	Shredding
Pictures, slides	Shredding
Medication containers (bottles and bags) with ID labels	Shredding of label (or container) or return to supplier along with unused medications
IV bags	Label goes in shredding
Electronic devices with memory storage (e.g., laptops, PCs, printers, photocopiers, dictaphones)	Data wiping prior to redeployment or return to vendor.

If computers are to be sold, all personal health information must first be erased in such a way that it cannot be recovered. If office machines such as photocopiers, fax machines, scanners and printers contain storage devices (such as a hard drive) that have not been disabled, these should be overwritten, or removed and destroyed, when the machines are replaced. *(Need to work with service/equipment providers to ensure agreed upon strategy is included in the service agreement and a process exists to support compliance).* [Company/Vendor/Supplier] shall provide TVFHT [Client] with a Certificate of Destruction documenting the date, time, location and method of destruction and bearing the signature of the operator, either at the conclusion of the destruction process or, if destruction is performed as part of a regularly scheduled event, at specified regular intervals as agreed to by [Company] and TVFHT [Client].

When destroying health records, a log will be maintained including the name of patients whose records have been destroyed, the date of destruction and the manner in which records were destroyed.

Never recycle any paper or media which contains patient information. Never treat any paper which has been printed with patient information as reusable for scrap. When patient information is no longer needed, it should be securely destroyed.

IT Security

Reasonable steps will be taken to ensure technological security of personal health information.

- Up to date anti-virus, Firewall and Spyware software will be used
- Staff will not install any unauthorized software or connect any unauthorized devices to their computer or use the computer for unauthorized purposes
- Staff cannot copy or transmit externally any personal health information from their computers unless authorized (including email or instant messaging) and if authorized (e.g., transmitting OHIP billing) will use encryption and/or a secure site e.g., Smart Systems for Health Agencies – VPN)
- Staff will be advised to be aware of the 'reader over the shoulder' and neighbours overhearing loud conversations

Third Party Vendors

When Thames Valley Family Health Team hires outside contractors to do data entry or provide information systems or to store, transport or destroy patient information we only use those that are bonded and insured and maintain a verifiable commitment to confidentiality. We make sure that the contractor uses the methods documented in the contract we have with them. TVFHT retains the right to request proof of a third party vendor's compliance with these requirements.

We only select contractors who commit under contract to:

- Agree to be a PHIPA agent of the TVFHT
- Hold and follow written privacy policies and procedures saying how material is to be kept safe in transit, storage and destruction as applicable
- Have insurance coverage for their liabilities under contract
- Require their own personnel to sign confidentiality agreements
- Have appropriate training for their personnel on privacy policies and the procedures to implement them

Breach of Privacy Safeguards

Should any person working for or with the Thames Valley Family Health Team become aware of a privacy breach or suspect that a privacy breach has or is about to take place, that person shall contact his or her immediate supervisor and/or a TVFHT Privacy Officer immediately or if not possible immediately, that person (or their supervisor) shall contact a TVFHT Privacy Officer at the very earliest moment possible.

If patient information is lost, stolen or accessed by unauthorized persons, the patient or their personal representative will be notified at the very first opportunity by Thames Valley Family Health Team.

All confirmed privacy breaches will be reported promptly to the Office of the Information and Privacy Commissioner of Ontario by one of the Co-Privacy Officers at Thames Valley Family Health Team.

Failure by staff members to adhere to the privacy safeguards and guidelines set out above may result in disciplinary measures, up to and including termination of employment or contract.

Other Resources

Information and Privacy Commissioner of Ontario website (https://www.ipc.on.ca) has a number of fact sheets available to assist in safeguarding the privacy and security of personal health information including:

Safeguarding Personal Information https://www.ipc.on.ca/images/Resources/fact-01-e.pdf

Encrypting Personal Health Information on Mobile Devices
https://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=613

Healthcare Requirement for Strong Encryption
https://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=969

The Secure Transfer of Personal Health Information
https://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=1200

Secure Destruction of Personal Information
https://www.ipc.on.ca/images/Resources/fact-10-e.pdf

Guidelines on Facsimile Transmission Security
https://www.ipc.on.ca/images/Resources/fax-gd-e.pdf

Appendix A – Email Disclaimer Message

This e-mail message is confidential and is intended only for the person(s) named above. If you have received this message in error, please notify the sender immediately and delete/remove it from your computer system. Any reading, distribution, printing or disclosure of this message if you are not the intended recipient is strictly prohibited. Thank you.

Appendix B – Automatic Response Email

Thank you for your message.

- If you are experiencing a medical emergency, please contact 9-1-1 or go to an emergency department or local hospital.
- All appointments with our office must be made by phone to * (insert #) and we are unable to accept email requests for new appointments.
- I do not monitor this email address 24 hours a day/7 days per week. There may be a delay in my ability to respond to your message.
- We make every effort to ensure the security of information within our email system but we cannot guarantee the security and confidentiality of any email you send or receive from us. As the message leaves the Thames Valley Family Health Team it is sent across the internet and it could be intercepted and read.

(Note: In Microsoft Outlook, you can customize a different automatic response for internal and external contacts. If you need assistance with this, please ask your team assistant or supervisor.)