185 Inkerman Street East
Listowel, ON N4W 2N1
T: (519) 291-3125
F: (519) 291-6028

North Perth Family Health Team
Helping you to health yourself

Subject:	Safeguards for Patient Information Guidelines	Date Approved:	January 26, 2017
Approved by:	Board of Directors	Date Revised:	
Specific to:	All Staff and Board of Directors	Next Review Date:	September 2020

PRINCIPLE:
North Perth Family Health Team takes steps to ensure that the personal health information we hold is protected against theft, loss and unauthorized use or disclosure. The details of these safeguards are set out in this policy.

POLICY:
This policy is part of the Privacy Policy.

We hold personal information about our patients.[1] This information is sensitive and valuable to our patients and we are obliged by law to treat it carefully. As part of our duties we must all take steps to keep patient information safe and make sure that it can be accessed only by those who need to see it for a proper reason.

This applies equally to our electronic medical record, paper copies of health records, reports, test results and emails and any other ways patient information can be recorded. We have to protect this information from loss, theft, unauthorized access including any kind of disclosure to the wrong people.

Following these guidelines will minimize the risk of patient information falling into the wrong hands which could cause harm and distress to patients and legal consequences to the Family Health Team and our affiliated physicians. We require everyone who is affiliated with the Family Health Team to follow the best practices described here, including all physicians, staff, volunteers, students, and vendors (collectively "**Team Members**"). Every Team Member has a role in keeping our patients' information secure, and we expect everyone to fulfill that role.

Privacy Breach
A privacy breach happens whenever a person contravenes or is about to contravene a rule under the *Personal Health Information Protection Act, 2004* ("**PHIPA**"). The most obvious privacy breaches happen when patient information is lost, stolen or accessed by someone without authorization.

For example:

- A fax with patient information is misdirected
- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package of patient records is not delivered to the correct address
- An unencrypted USB key with patient information is lost

[1] It is possible that we hold personal health information about individuals who are not current patients (e.g., former patients), and the safeguards guidelines would apply equally to those individuals.

North Perth Family Health Team
Helping you to health yourself

185 Inkerman Street East
Listowel, ON N4W 2N1
T: (519) 291-3125
F: (519) 291-6028

- A patient reads another patient's health record on a computer while waiting in a clinic room
- A Team Member talks about a patient with a friend
- Health records to be disposed of are recycled and not shredded
- Out of curiosity, a Team Member reviews a neighbour's health record
- A student or any other Team Member looks at health records of patients on a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise
- Health information is given to the media
- A Team Member makes a copy of an ex-spouse's health record without the spouse's permission

All privacy breaches must be reported immediately to the Privacy Officer. If you have any questions, contact the Privacy Officer.

Restricted Access to Patient Information
Access to patient information is provided on a need-to-know basis as appropriate to the Team Member's role and purpose for access.

Team Members must not access any health records unless authorized - which means only for legitimate reasons. Team Members may not access health records of their spouses, children, parents, friends or neighbours, or work colleagues. They may only access their own health record (if applicable) through the normal patient access channels and not directly. Team 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 records except for legitimate reasons

Team Members should know that all access to the electronic medical record is logged and audited.

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 Team Members 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 (i.e. passwords that are lengthy (with an ideal minimum length of 12 characters), contain a random (and not sequential) mix of numbers, upper and lower case letters, and symbols and that do not contain personal information or common words – e.g. your name, the Family Health Team's name, your extension number)
- Contact the Privacy Officer if they suspect any kind of computer misuse followed by a call to the IT HelpDesk at ext. 6111.

An unauthorized person trying to gain access to our health records may not be obvious. Data breaches have occurred in other organizations after "confidence tricks" convinced individuals to reveal passwords

North Perth Family Health Team
Helping you to health yourself

185 Inkerman Street East
Listowel, ON N4W 2N1
T: (519) 291-3125
F: (519) 291-6028

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 the Privacy Officer immediately.

Physical Security On-Site

We hold 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 like patient files.

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 double-locked in a locked cabinet, container and/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. Patient identifiable labels on files should not be visible to visitors. Patient information that is being stored before secure destruction will be kept separate and clearly marked.

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 Team Members who have a real need to do so to carry out their duties, e.g. who provide care to patients in the community. 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 our 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 de-identified if possible. Otherwise, if Team Members are ever required to copy patient information onto a laptop, memory stick or other portable device strong encryption must be used. Strong encryption is more than just password protected. If you are not sure how to do this, the Privacy Officer (or your IT department) will show you how. For paper files, keep papers in a locked box or briefcase 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).

Laptop computers, disks or files must not be left 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. Patient information should not be stored at home, except in very limited circumstances and if this occurs, the information must be held securely. Team Members should not make printouts from remote access at home.

Sending Patient Information

North Perth Family Health Team
Helping you to health yourself

185 Inkerman Street East
Listowel, ON N4W 2N1
T: (519) 291-3125
F: (519) 291-6028

Special care must be taken when sending correspondence about a patient or containing patient information to anyone outside of the Family Health Team - including to another health-care provider, to a third party, or to the patient.
In addition to this policy, interdisciplinary 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 and Text Messages
Until appropriate secure safeguards have been implemented in compliance with PHIPA, emailing and texting patients are prohibited. Emailing and texting other health care providers about a patient are permitted as long as there are no patient identifiers in the message.

Emails Sent within Family Health Team
When sending emails within the Family Health Team, you must 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.

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 before hitting the send button. Email programs that auto-fill the recipient field can insert an address you did not intend to send to.

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

Accessing Email on a Mobile Device
If a Family Health Team email address is to be accessible on a mobile device (such as a smart phone), the device must be an approved Family Health Team device that has been set up through the LWHA IT Department, and the following steps must be undertaken:

- Team Members must have permission from the Privacy Officer to load a Family Health Team email address account on a mobile device;
- The device must be password protected and subject to a strong level of encryption;
- The device contents must be able to be erased remotely (that means, all content from the device can be remotely deleted by the Family Health Team);
- Any loss of the device must be reported immediately to the Privacy Officers to assess exposure and remotely delete the contents of the device if necessary

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

North Perth Family Health Team
Helping you to health yourself

185 Inkerman Street East
Listowel, ON N4W 2N1
T: (519) 291-3125
F: (519) 291-6028

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. The cover sheet should not include any patient information. Where appropriate, call the recipient prior to sending a fax so they can be waiting to retrieve it.

In the event that you are notified by an unintended recipient that they received the fax in error, ensure that you obtain the recipient's name and contact information in case he/she needs to be contacted at a later date. After sending a fax, collect and keep a confirmation receipt. 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.

Social Media

Team Members must never post information about patient-specific cases and are advised against 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.

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.

If we have the patient's consent to leave a message and you are answered by a 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.

If a patient calls us for patient care information, the call must be forwarded to the primary care nurse or telephone triage nurse and steps should be taken to confirm the caller's identity before providing the information. Our patients expect it. We can do this 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?

185 Inkerman Street East
Listowel, ON N4W 2N1
T: (519) 291-3125
F: (519) 291-6028

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 and mark it “Personal and Confidential” 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.

Destroying Patient Information

When patient information is no longer needed we must make sure it is 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.)	Shredding
CDs, DVDs, disks, USB keys	Shredding or breaking into pieces
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 – to be performed by LWHA IT Dept.

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. Please refer to the policy *Patient Records Management*.

Third Party Vendors

When the 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. Any vendor agreement with respect to IT network and telecommunications issues needs to be in compliance with LWHA’s existing procurement /contract policies.

We only select contractors who commit to enter a legal agreement with the Family Health Team to:

- Agree to be a PHIPA agent of the Family Health Network
- Hold and follow written privacy policies and procedures saying how material is to be kept secure in transit, storage and destruction as applicable
- Have insurance coverage for their liabilities under contract
- Require their own personnel to sign confidentiality agreements

185 Inkerman Street East
Listowel, ON N4W 2N1
T: (519) 291-3125
F: (519) 291-6028

- Have appropriate training for their personnel on privacy policies and the procedures to implement them

Breach of Privacy Safeguards

Failure by Team 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.