Subject:	Privacy Policy	Date Approved:	April 1, 2021
Approved by:	Board of Directors	Date Revised:	
Specific to:	All Staff and Board of Directors	Next Review Date:	September 2024

PRINCIPLE:
The Family Health Team is committed to patient[1] privacy and to protecting the confidentiality of the health information we hold.

POLICY:
Our doctors belong to a Family Health Network (FHN) and are collectively health information custodians (HICs) under the *Personal Health Information Protection Act, 2004* (PHIPA). The FHN is accountable and liable for compliance with PHIPA and the protection of health records. For the purposes of privacy obligations, the Family Health Team and our staff are agents of the FHN. This relationship has been established through a "PHIPA Agency Agreement" signed by each physician and the Family Health Team.

In this Privacy Policy, we use the language of "**Team Members**" to capture the commitment that all physicians, and all Family Health Team and FHN staff, volunteers, students and vendors abide by this Privacy Policy and to reflect our shared commitment to protecting personal health information.

This Privacy Policy acts as the articulation of the privacy practices and standards to guide all Team Members and any other agents. There are additional privacy policies that are included by reference to this Privacy Policy and are listed at **Appendix A**. All Team Members agree to abide by those policies as well.

Principle 1 – Accountability for Personal Health Information
Our physicians are responsible for any personal health information held. The following position has been designated as the Privacy Officer: Executive Director. The Privacy Officer is accountable for compliance with this Privacy Policy and compliance with PHIPA.

Our commitment to privacy is demonstrated by adherence to privacy policies and procedures to protect the personal health information we hold and by educating our staff and any others, who collect, use or disclose personal health information on our behalf about their privacy responsibilities.

Principle 2 – Identifying Purposes for Collecting Personal Health Information
We collect personal health information for purposes related to direct patient care, administration and management of our programs and services, patient billing, administration and management of the health care system, research, teaching, statistical reporting, meeting legal obligations, fundraising, marketing and as otherwise permitted or required by law.
When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is permitted or required by law, consent will be required before the information can be used for that purpose.

[1] We have used the term "patient" throughout the policy. It is possible that we hold personal health information about individuals who are not the Family Health Team's patients or who are former patients and the privacy policy would apply equally to those individuals.

Principle 3 – Consent for the Collection, Use and Disclosure of Personal Health Information

We require consent in order to collect, use, or disclose personal health information. However, there are some cases where we may collect, use or disclose person health information without consent as permitted or required by law.

Express consent

Should a patient wish his/her other health care providers (outside of their health care providers at the Family Health Team) to have access to the patient health record, the patient can provide a verbal or written consent to this effect, which will be communicated to the patient's physician. See the Family Health Team's "*Access and Correction Policy – Release of Patient Information*".

Should a patient wish his/her lawyer, insurance company, family, employer, landlord or other third party individuals or agencies (non-health care providers) to have access to his/her health record, the patient must provide verbal or written consent to this effect, which will be communicated in accordance with the Family Health Team's policy: "*Access and Correction Policy – Release of Patient Information*".

Implied consent (Disclosures to other health care providers for health care purposes) – Circle of Care

Patient information may also be released to a patient's other health care providers for health care purposes (within the "circle of care") without the express written or verbal consent of the patient as long as it is reasonable in the circumstances to believe that the patient wants the information shared with the other health care providers. No patient information will be released to other health care providers if a patient has stated he/she does not want the information shared (for instance, by way of the placement of a "lockbox" on his/her health records).

A patient's request for treatment constitutes implied consent to use and disclose his/her personal health information for health care purposes, unless the patient expressly instructs otherwise.

Who can be in the "circle of care" includes (among others providing direct patient care if authorized by PHIPA):

Within the physician's office and Family Health Team:

- All physicians in this practice
- Interprofessional health providers
- Medical students, residents and locums
- Nursing or other allied health care students

Outside of the Family Health Team:

- Hospitals
- Community Care Access Centres
- Community Health Centres
- Long-term care homes
- Ambulance
- Pharmacists
- Laboratories
- Regulated health professionals in sole practice or group

- Social workers and social service workers in sole practice or group
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care

No Consent

There are certain activities for which consent is not required to use or disclose personal health information. These activities are permitted or required by law. For example, we do not need consent from patients to (this is not an exhaustive list):

- Plan, administer and manage our internal operations, programs and services
- Get paid
- Engage in quality improvement, error management, and risk management activities
- Participate in the analysis, administration and management of the health care system
- Engage in research (subject to certain rules)
- Teach, train and educate our Team Members and others
- Compile statistics for internal or mandatory external reporting
- Respond to legal proceedings
- Comply with mandatory reporting obligations

A list of mandatory reporting obligations is found in the Family Health Team's "*Access and Correction – Release of Patient Information Policy*".

If Team Members have questions about using and disclosing personal health information without consent, they can ask the Privacy Officer.

Withholding or Withdrawal of Consent

If consent is sought, a patient may choose not to give consent ("withholding consent"). If consent is given, a patient may withdraw consent at any time, but the withdrawal cannot be retrospective. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

Lockbox

PHIPA gives patients the opportunity to restrict access to any personal health information or their entire health record by their health care providers within the Family Health Team or by external health care providers. Although the term "lockbox" is not found in PHIPA, lockbox is commonly used to refer to a patient's ability to withdraw or withhold consent for the use or disclosure of their personal health information for health care purposes. See the Family Health Team's "*Lockbox Policy*" for details of how the lockbox works.

If a physician leaves the Family Health Network, his/her patients will be notified and will have a choice whether to transfer their health records in accordance with the rules/guidelines set forth by the College of Physicians and Surgeons of Ontario. http://www.cpso.on.ca/

Principle 4 – Limiting Collection of Personal Health Information

We limit the amount and type of personal health information we collect to that which is necessary to fulfill the purposes identified. Information is collected directly from the patient, unless the law permits or requires collection from third parties. For example, from time to time we may need to collect information from patients' family members or other health care providers.

Personal health information may only be collected within the limits of each Team Member's role. Team Members should not initiate their own projects to collect new personal health information from any source without being authorized by the Family Health Team or the Privacy Officer**.**

Principle 5 – Limiting Use, Disclosure and Retention of Personal Health Information
Use

Personal health information is not used for purposes other than those for which it was collected, except with the consent of the patient or as permitted or required by law.

Personal health information may only be used within the limits of each Team Member's role. Team Members may not read, look at, receive or otherwise use personal health information unless they have a legitimate "need to know" as part of their position. If a Team Member is in doubt whether an activity to use personal health information is part of his/her position – he/she should ask the Privacy Officer**.** For example, self-directed learning is not allowed (randomly or intentionally looking at health records for self-initiated educational purposes) without specific authorization.

Disclosure
Personal health information is not disclosed for purposes other than those for which it was collected, except with the consent of the patient or as permitted or required by law.

Personal health information may only be disclosed within the limits of each Team Member's role. Team Members may not share, talk about, send to or otherwise disclose personal health information to anyone else unless that activity is an authorized part of their position. If a Team Member is in doubt whether an activity to disclose personal health information is part of his/her position – he/she should ask the Privacy Officer.

Retention
Health records are retained as required by law and professional regulations and to fulfill our own purposes for collecting personal health information.

The Canadian Medical Protective Association (CMPA) and College of Physicians and Surgeons of Ontario (CPSO) advise their members to retain health records for at least 10 years from the date of last entry or, in the case of minors, 10 years from the time the patient would have reached the age of majority (age 18). There may be reasons to keep records for longer than this minimum period.

Personal health information that is no longer required to fulfill the identified purposes is destroyed, erased, or made anonymous safely and securely. Please see the Family Health Team's "*Safeguards for Patient Information Guidelines*".

Principle 6 – Accuracy of Personal Health Information

We will take reasonable steps to ensure that information we hold is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate information may be used to make a decision about a patient.

Principle 7 – Safeguards for Personal Health Information
We have put in 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 the use of passwords, encryption, and audits).

We take 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 the Family Health Team's "*Safeguards for Patient Information Guidelines*".

We require anyone who collects, uses or discloses personal health information on our behalf to be aware of the importance of maintaining the confidentiality of personal health information. This is done through the signing of confidentiality agreements, privacy training, and contractual means.

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

Principle 8 – Openness about Personal Health Information
Information about our policies and practices relating to the management of personal health information are available to the public, including:

- Contact information for our Privacy Officer, to whom complaints or inquiries can be made;
- The process for obtaining access to personal health information we hold, and making requests for its correction;
- A description of the type of personal health information we hold, including a general account of our uses and disclosures; and
- A description of how a patient may make a complaint to the Family Health Team or to the Information and Privacy Commissioner of Ontario.

Principle 9 – Patient Access to Personal Health Information
Patients may make written requests to have access to their records of personal health information, in accordance with the Family Health Team's "*Access and Correction Policy – Release of Patient Information*".

We will respond to a patient's request for access within reasonable timelines and costs to the patient, as governed by law. We will take reasonable steps to ensure that the requested information is made available in a format that is understandable.

Patients who successfully demonstrate the inaccuracy or incompleteness of their personal health information may request that we amend their information. In some cases instead of making a correction, patients may ask to append a statement of disagreement to their file.

Please Note: In certain situations, we may not be able to provide access to all the personal health information we hold about a patient. Exceptions to the right of access requirement will be in accordance with law. Examples may include information that could reasonably be expected to result in a risk of serious harm or the information is subject to legal privilege.

Principle 10 – Challenging Compliance with the Family Health Team's Privacy Policies and Practices
Any person may ask questions or challenge our compliance with this policy or with PHIPA by contacting our Privacy Officer:

Executive Director
Listowel-Wingham and Area Family Health Team
185 Inkerman Street East
Listowel, ON N4W 2N1
(519) 291-3125 ext.6273

We will receive and respond to complaints or inquiries about our policies and practices relating to the handling of personal health information. We will inform patients who make inquiries or lodge complaints of other available complaint procedures.

We will investigate all complaints. If a complaint is found to be justified, we will take appropriate measures to respond.

The Information and Privacy Commissioner of Ontario oversees our compliance with privacy rules and PHIPA. Any individual can make an inquiry or complaint directly to the Information and Privacy Commissioner of Ontario by writing to or calling:

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 Canada
Phone: 1 (800) 387-0073 (or 416-326-3333 in Toronto)
Fax: 416-325-9195
www.ipc.on.ca

Appendix A –Supporting Privacy Policies

The following policies and documents are incorporated into the Privacy Policy and must be followed by all physicians, the Family Health Network, the Family Health Team and all staff, students, volunteers, and vendors:

Access and Correction Policy – Release of Patient Information
Lockbox Policy
Lockbox Information Sheet for Patients
Patient Lockbox Request Form
Privacy Breach Protocol
Public-Friendly Privacy Notice
Safeguards for Patient Information Guidelines