Privacy and Protection of Personal Information Policies and Procedures	Lakelands Family Health Team
	Updated: January 2020

Intent:

Protecting the privacy and confidentiality of personal information is an important aspect of the way Lakelands Family Health Team (LFHT) conducts its operations. As part of our mission to provide compassionate and respectful care by following best practice guidelines, we are committed to promoting patient privacy and protecting the confidentiality of health information that we hold. Collecting, using, and disclosing personal information in an appropriate, responsible, and ethical manner is fundamental to LFHT's daily operations. Each staff member of LFHT must be aware of and abide by our organization's practices and procedures when handling personal information.

Purpose:

The purpose of this policy is to outline LFHT requirements and principles for managing the collection, use, and disclosure of personal information and personal health information by employees and team members of LFHT; as well as outline protocols for managing patient requests, complaints and privacy breaches.

Definitions & Principles:

Health Information Custodian and Agents

Our employees belong to a Family Health Team (LFHT) and are collectively health information custodians (HICs) under the Personal Health Information Protection Act, 2004 (PHIPA). Lakelands FHT is accountable and liable for compliance with PHIPA and the protection of health records. For the purposes of privacy obligations, the Lakelands Family Health Team and our staff ("team members") are agents of the FHT.

Personal Information (PI)

Personal information is defined as any identifying information about an individual or group of individuals, including name, date of birth, address, phone number, email address, nationality, gender, health history, opinions, personal views, etc.

Personal Health Information/Protected Health Information (PHI)

Personal health information is defined as any information about health status, provision of health care, or health care information that can be linked to a specific individual.

Privacy Officer

The designated Privacy Officer for Lakelands FHT is our lead administrator, the Executive Director. The Privacy Officer is accountable for compliance with our privacy policies and compliance with PHIPA.

Informing Patients about their Privacy Rights
We post privacy posters and our policies in patient areas and on our website. We welcome any and all questions and concerns regarding privacy as necessary.

Why We Collect Personal Health Information
We collect personal health information for purposes related to:

- Providing direct patient care
- Communicating with other health care providers who also provide services to our patients
- Administration and management of our programs and services
- Patient billing
- Administration and management of the health care system
- Research (with research ethics board approval)
- Teaching
- Statistical reporting
- Meeting legal obligations 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.

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.

Implied consent – The Circle of Care

When a patient comes for health services, it is implied we have consent to use and disclose his/her personal health information for health care purposes, unless there is an express instruction otherwise.

Patient information may be released to a patient's other health care providers for health care purposes (within the "circle of care") without express written or verbal consent 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, if there is a "lock" on his/her health records or if the patient has specifically asked that it not be shared).

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

<u>Within the physician's office and Family Health Team:</u>

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

<u>Outside of the Family Health Team:</u>

- Hospitals

- Community Care Access Centres
- Community Health Centres
- Long-term care homes
- Ambulance
- Pharmacists
- Laboratories
- Regulated health professionals in solo practice or group
- Social workers and social service workers in solo practice or group
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care
- And others

For clarity – the following groups are NOT in the circle of care and we do not share personal health information about our patients with them relying on implied consent. That does not mean we never disclose to these groups – but we may only do so if we have express consent or if we are otherwise permitted or required by law to disclose:

- Ministry of Health and Long-Term Care staff
- Insurance companies
- Workplace Safety and Insurance Board
- Children's Aid Society
- Police
- Landlords (other than some supportive housing and residential tenancies who may be in the circle)
- Employers
- Teachers and schools (however, psychologists, social workers, nurses, psychiatrists, speech-language pathologists, occupational therapists, physiotherapists, or audiologists affiliated with schools may be in the circle of care if they are providing health care)
- External unregulated care providers
- Spiritual leaders/healers

Express Consent

A general rule is if we are disclosing personal health information to someone other than a health care provider for health care purposes, we need express consent. For example, if an employer, landlord, school, insurance company, or family member (who is not a substitute decision maker) would like health information about our patient, we need express consent. There are some exceptions to the general rule (see "no consent" below).

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
- Receive payment
- 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
- Anonymize health information

If Team Members have questions about using and disclosing personal health information without consent, they can ask our Privacy Officer and are welcomed in doing so.

Consent by Authorized Persons: Who May Consent on Behalf of a Client
When consent is required under this policy or another privacy policy, the following people may give consent as "authorized persons"):

- The patient, if the patient is capable.
- There is no specific age of consent to make information decisions. The test is whether the individual is capable. A clinician determines capacity and it is usually connected with whether the patient is capable to make decisions about the specific treatment or counseling. Patients are presumed to be capable unless it is unreasonable in the circumstances to presume. Patients may be capable of some decisions and not all information decisions.
- Please note for capable patients under the age of 16: If a patient is capable and also under the age of 16, the patient may consent AND the patient's parent or person who has lawful custody may also consent. BUT the parent or person with lawful custody may not consent if the information to be disclosed relates to "treatment" (as defined under the Health Care Consent Act, 1996) about which the patient has made his/her own decision or "counseling" (as defined under the Child and Family Services Act) about which the patient who is over the age of 12 participated on his or her own. (That means if a patient consented to the treatment or counseling on his/her own – a parent or legal guardian cannot consent to the release of that information on behalf of the patient). And if there is a disagreement between a capable patient under the age of 16 and the parent or legal guardian about the release of information, the capable patient's wishes prevail.
- A substitute decision-maker, if the patient is incapable.

Please refer to section 26 of PHIPA which lists the hierarchy of individuals/agencies that can act as substitute decision-makers:

- The individual's guardian of the person or guardian of property, if the consent relates to the guardian's authority to make a decision on behalf of the individual.
- The individual's attorney for personal care or attorney for property, if the consent relates to the attorney's authority to make a decision on behalf of the individual.
- The individual's representative appointed by the Consent and Capacity Board, if the representative has authority to give the consent.
- The individual's spouse or partner.
- A child or parent of the individual, or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent [Note: This paragraph does not include a parent who has only a right of access to the individual. If a children's aid society or other person is lawfully entitled to consent in the place of the parent, this paragraph does not include the parent.]
- A parent of the individual with only a right of access to the individual.
- A brother or sister of the individual.
- Any other relative of the individual.

- The estate trustee or person who has assumed responsibility for the deceased person's estate if documented in writing, in the case of a deceased client.

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.

Locked Records
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.

If a patient leaves the Family Health Team, they 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.

Limiting Collection, Use and Disclosure 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, used by or disclosed within the limits of each team member's role. Team members shall not initiate their own projects to collect new personal health information from any source, or use it or disclose it without being authorized by a physician or the Family Health Team or 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. LFHT maintains all patient medical records as per CMPA/CPSO guidelines.

Personal health information that is no longer required to fulfill the identified purposes is destroyed, erased, or made anonymous safely and securely. The Privacy Officer at LFHT maintains records of safe and secure records disposal. All inactive files are stored in a double-locked storage area and only authorized personnel can access them with express purpose identified by the Privacy Officer and in the course of their position.

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.

Safeguards for Personal Health Information
We have put in place safeguards for the personal health information we hold, which include:

- Physical safeguards (such as restricted office access, using alarm systems, locked filing cabinets and rooms where health information is stored, keeping portable devices in a secure location such as a locked drawer or cabinet when unattended);
- Organizational safeguards (such as permitting access to personal health information by staff on a "need-to-know" basis only, and confirming patient contact information on a regular basis); and
- Technological safeguards (such as the use of passwords, encryption, firewalls, anti-malware scanners and audits). Routers and servers connected to the Internet are protected by a firewall, and are further protected by virus attacks or "snooping" by sufficient software solutions.

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 our "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.

Patients Have a Right to Access Their Personal Health Information
Patients may make written requests to have access to their records of personal health 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.

Roles & Responsibilities

Role	Responsibility
Administration/ Privacy Officer	1. Ensure the Privacy and Protection of Personal Information policy remains current relative to all legislative changes. 2. Educate all employees/team members on the content and intent of the Privacy and Protection of Personal Information policy and pertinent procedures. 3. Notify individuals when their personal information is stolen, lost, or accessed by unauthorized persons.

	4. Listen and follow up on any patient or employee privacy complaints or concerns.
Employees/ Team Members	1. Maintain the privacy, confidentiality, and security of a patients' personal health information as indicated by this policy and PHIPA. 2. Bring any privacy concerns or questions to Administration, including any and all breaches of privacy. 3. Complete any and all privacy training as is deemed necessary by Administration upon hiring. 4. Complete any additional privacy training as is deemed necessary by Administration throughout the course of employment.

PROCEDURES

Patient Request for Personal Information/Patient Amendment Requests

In most instances, LFHT will grant individuals access to their personal information.

1. Patients must provide a written request for personal information, and the provision of satisfactory identification.
2. Should LFHT deny an individual's request for access to their personal information, LFHT will advise in writing of the reason for such a refusal. The individual may challenge the decision.
3. Should a patient request a change to their personal information, an amendment will be added to their electronic chart as is deemed necessary by the Privacy Officer and shall be made in writing.

Concerns, Complaints, Public Information and Questions about our Privacy Practices

Any person may ask questions or challenge our compliance with this policy or with PHIPA by contacting our Privacy Officer.

In writing to: Lakelands Family Health Team
12357 Highway 41
Northbrook, Ontario
K0H 2G0
Attention: Janice Powell, Executive Director

Via email to: info@lakelandsfht.ca

By telephone to: Janice Powell, Executive Director, 1-613-336-8888

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 ask that any incident of a breach or complaint be made in writing.**

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:

Information and Privacy Commissioner of Ontario
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

Consequences for Breach of Privacy

Failure by Team Members to adhere to this policy or other privacy policies may result in disciplinary measures up to and including termination of employment or contract. All issues with breaches of privacy will be discussed by the Privacy Officer (Executive Director) and then subsequently with the individual involved.

We are obligated to notify any affected patient(s) of a privacy breach and their rights and will do so in accordance with the requirements of PHIPA and our "Privacy Breach Protocol".

Privacy Breach Protocol

A privacy breach occurs when PHI is collected, used or disclosed without authorization. This can include theft, loss, or unauthorized copying, modification, or disposal. The following steps are to be taken immediately, and some steps may need to be returned to or repeated, depending on the type of breach that has occurred.

1. Notify pertinent staff and other custodians.
    a. Notify staff of the breach, with paramount importance of informing the Privacy Officers (Executive Director). All employees and team members are mandated to report any and all privacy breaches to the Privacy Officer.
    b. Staff members are asked to fill out the LFHT "Breach Report Form" available in the Executive Director's office.
    c. Notify all affected custodians, if the breach involves PHI on an electronic system.

2. Identify the scope of the breach and take steps to contain it.
    a. Identify the scope of the breach, including individuals or organizations who may have been involved with or are responsible for the breach, and the nature and quantity of the PHI that is affected.
    b. Retrieve any copies of PHI that have been disclosed.
    c. Ensure that no copies of PHI have been made or retained by anyone who was not authorized to receive the information. Record the person's contact information in case follow-up is required.
    d. Take any additional steps that may be appropriate in the case, such as changing passwords and identification numbers and/or temporarily shutting down your computer system. Consider suspending access rights.

3. Notify the individuals affected by the breach and potentially the IPC.
    a. PHIPA requires custodians to notify individuals of a breach at the first reasonable opportunity. Notification can be via telephone or in writing. Depending on the circumstances, a notation can be added to a patient's chart to discuss at their next appointment.
    b. If unsure of all factors, contact the IPC to discuss the case.
    c. When notifying individuals affected by the privacy breach, you should provide the following information:
        i. The date of the breach
        ii. A description of the nature and scope of the breach
        iii. A description of the PHI that was subject to the breach
        iv. The measures implemented to contain the breach, and
        v. The name and contact information of the person to direct inquiries to (Executive Director).
    d. Notice to affected individuals must include a statement letting them know they are entitled to make a complaint to the IPC.

4. Notify Regulatory Colleges.
    a. A health care practitioner's regulatory college must be notified within 30 days if any of the following applies:
        i. If a termination, suspension, or disciplinary action was taken as a result of the breach;
        ii. If the practitioner's privileges or affiliation is revoked, suspended, or restricted as a result of the breach;
        iii. The practitioner resigns as a result of the breach;
        iv. The practitioner relinquishes or restricts their privileges as a result of the breach.

5. Investigate and Remediate.
    a. An internal investigation shall occur that ensures the requirements of containment and notification have occurred; the circumstances surrounding the breach have been reviewed; and whether existing policies and procedures around protecting PHI need to be updated.
    b. Work with the IPC to provide details as necessary.
    c. Keep a log with details and information about any breach, as is required by PHIPA.
    d. Continue to review and educate staff as necessary.
    e. Review all safeguards and update/upgrade as necessary.
    f. When in doubt, seek advice from another Privacy Officer or legal representation.

References & Acknowledgements

The following websites can provide more information in supporting our Privacy Policies. These are available to all of our Team Members inside our Human Resources Policies and Procedures binder as Appendices.

Personal Health Information Protection Act 2004
https://www.ipc.on.ca/wp-content/uploads/Resources/hguide-e.pdf

Quality of Care Information Protection Act 2016
http://www.health.gov.on.ca/en/common/legislation/qcipa/

Responding to a Health Privacy Breach: Guidelines for the Health Sector 2018, Information and Privacy Commissioner of Ontario
https://www.ipc.on.ca/wp-content/uploads/2018/10/health-privacy-breach-guidelines.pdf

Special thanks to the Central East LHIN, London Family Health Team, and Central Hastings Family Health Team for modelling outstanding Privacy Policies and Procedures, from which we have created ours in accordance with the above legislations and materials.