

Subject: Privacy Policy	Date Effective: April 18, 2019
Approved By: The Summerville Board of Directors	Date Revised:
Specific to: Employees (FHT and FHO), affiliated physicians, residents, volunteers, students, vendors and contractors	Next Review Date: As required

Privacy Policy

We are committed to patient¹ privacy and to protecting the confidentiality of the health information we hold.

Summerville Family Health Team is a health information custodian (HIC) under the *Personal Health Information Protection Act, 2004* (PHIPA). We are accountable and liable for compliance with PHIPA and the protection of health records. For the purposes of privacy obligations, physicians affiliated with family health organizations are agents of the Family Team as are their staff (if any). This relationship has been established through the annual services agreement signed by the physicians and the Summerville Family Health Team.

In this Privacy Policy, we use the language of “Team Members” to capture the commitment that Summerville Family Health Team and all our staff, affiliated physicians (and their staff), residents, volunteers, students and vendors and any other agents will 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. 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

Summerville Family Health Team is responsible for any personal health information we hold.

The Executive Director of the Family Health Team and a Physician representative selected by the Summerville Family Health Organization act as joint Privacy Officers.

The Privacy Officers are accountable for compliance with this Privacy Policy and compliance with PHIPA.

Our commitment to privacy is demonstrated by adherence to our 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.

¹ We have used the term “patient” throughout the policy. It is possible that we hold personal health information about individuals who are not rostered to an affiliated Family Health Organization physician or registered to the Family Health Team or who are former patients, and this policy would apply equally to those individuals.

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, quality improvement, 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.

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

In general, 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 (Disclosures to other health care providers for health care purposes) – Circle of Care

Patient information may be released to a patient’s other health care providers for health care purposes (within the “circle of care”) relying on implied consent and without requiring 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 they do not want the information shared (for instance, by way of the placement of a “lockbox” or “consent directive” on their health records).

A patient's request for treatment constitutes implied consent to use and disclose their 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 Summerville Family Health Team, our affiliated physicians’ offices and Family Health Organization:

- Other physicians in this practice and our Family Health Organization and locums
- Interprofessional health providers (Nurse Practitioner, Registered Nurse, Registered Practical Nurse, Dietician, Psychologist, Social Worker, Pharmacist, Physiotherapist, Health Promotion Specialist)
- Medical students and residents or nursing or other allied health care students

Outside of Summerville Family Health Team, our affiliated physicians’ offices and Family Health Organization: (among others)

- Regulated health professionals in solo practice or group
- Social workers and social service workers in solo practice or group
- Hospitals

- Community Health Centres
- Long-term care homes
- Ambulance
- Pharmacists
- Laboratories
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care

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 individuals and groups - but we only do so if we have express consent or if we are otherwise permitted or required by law to disclose:

- 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)
- Children’s Aid Society
- Police
- Landlords
- Employers
- External unregulated care providers
- Spiritual leaders/healers
- Insurance companies
- Lawyers

Express consent

Patients may also provide a verbal or written consent if they wish for Summerville Family Health Team to release their information to their external health care providers. See our *“Access and Correction Policy – Release of Patient Information”*.

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

No Consent

There are certain activities for which consent is not required to collect, 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 some research projects (subject to certain rules, such as obtaining research ethics board

- approval and having research contracts)
- 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 our *“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 a 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 – Consent Directive

PHIPA gives patients the opportunity to restrict access to any personal health information or their entire health record by their health care providers within Summerville Family Health Team, our affiliated physicians’ offices and Family Health Organizations or by external health care providers. Although the term “lockbox” is not found in the privacy legislation, 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 *“Lockbox Policy”* for details of how the lockbox works.

If a physician leaves a Family Health Organization, their patients will be notified and will have a choice to transfer a copy of their health records in accordance with the rules set forth by the College of Physicians and Surgeons of Ontario and our policies.

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 and others.

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.

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 their position – they should ask a Privacy Officer. For example, looking at health records out of personal curiosity or a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise is not permitted.

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 their position – they should ask a 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.

We follow the Canadian Medical Protective Association (CMPA) and College of Physicians and Surgeons of Ontario (CPSO) recommendations 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). In some cases, we 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 our "*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 confidential shredding bins, locked filing cabinets and rooms,

- clean desks);
- 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, audits, back-up, secure disposal).

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 *"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. We take care if we transfer files to a medical storage company.

Principle 8 – Openness about Personal Health Information

Information about our policies and practices relating to the management of personal health information is 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 our Privacy Officer 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 *"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 have a right to ask for their records to be corrected if they can demonstrate that the records we hold are inaccurate or incomplete in some way for the purposes for which we hold that information. In some cases, instead of making a correction, we may offer a patient an opportunity 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 Our Privacy Policies and Practices

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

Privacy Officer
Executive Director
Summerville Family Health Team
101 The Queensway West, 5th Floor
Mississauga, Ontario
L5B 2P7

We will receive and respond to complaints or inquiries about our policies and practices relating to the handling of personal health information.

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 Summerville Family Health Team and all physicians, staff, residents, students, volunteers, and vendors:

	Last Updated
Public-Friendly Privacy Notice	April 2019
Access and Correction Policy – Release of Patient Information	April 2019
Lockbox Policy	April 2019
Safeguards for Patient Information Guidelines	April 2019
Privacy Breach Protocol	April 2019