PROTECTION OF PATIENT INFORMATION - PHIPA

[Organization Name] is committed to adhering to all applicable legislation regarding the collection, use, storage, and disclosure of patient information in accordance with the *Personal Health Information Protection Act* (PHIPA). Personal health information is sensitive and private information and [Organization Name] will ensure that this information is protected and only used for its stated and intended purpose.

DEFINITIONS

Personal Health Information means identifying information about an individual in oral or recorded form, if the information:

1. Relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family,
2. Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
3. Is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019,
4. Relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
5. Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
6. Is the individual’s health number, or
7. Identifies an individual’s substitute decision-maker.

POLICY

Following the guidelines outlined by PHIPA, [Organization Name] will only collect, use, or disclose the personal health information of patients who have provided their consent. [Organization Name] will not collect, use, or disclose any personal health information if there is another way that would serve the same purpose. [Organization Name] will also not collect any more personal health information than what is absolutely required. This includes limiting the collection of additional personal health information, including health care numbers.

[Organization Name] will ensure that:

1. It retains up-to-date health records;
	1. This includes making corrections to personal health information upon request from a patient within a reasonable timeframe of 30 days;
2. All records are secure;
	1. Records must be stored in locked file cabinets, or in areas where access is only granted with a key or pin pad access. [Organization Name] will also not store personal health information on unsecured computers or hard drives;
3. Records are stored for appropriate lengths of time;
	1. This includes retaining them for the duration of an investigation into any breaches of personal health information access;
4. Breach procedures are in place;
	1. This includes informing a patient if their information is accessed without their consent;
5. It appoints a contact person for ensuring the privacy of personal health information;
	1. This contact person is responsible for compliance with PHIPA, as well as training other employees regarding PHIPA, and responding to requests for access of personal health information records;
6. It establishes and publishes its privacy practices;
7. Consent is obtained;
8. Access to personal health information is provided under the appropriate circumstances (e.g., within 30 days of a request being made either orally or in writing).

Patient Rights under PHIPA

PHIPA has established the following rights for patients providing their personal health information. [Organization Name] will ensure that these rights are always considered when there is a challenge brought forward concerning patient information. They include a patient’s right to:

* Be informed of the reason why [Organization Name] is collecting, using, or disclosing their information;
* Be notified in the event that any of their personal health information is lost, stolen, accessed without their consent;
* Refuse to provide consent for the collection, use, or disclosure of their health information;
* Provide notice about a change in their consent;
* Instruct [Organization Name] that their personal health information may not be used or disclosed without their consent for any other purposes;
* Access their own personal health information records, possibly in an electronic format (if that format meets requirements set out in the regulations);
* Correct their health records (this must be requested by the person); and
* Pursue a complaint if they are refused access, refused a correction, if their privacy is breached, or start a court proceeding for damages relating to harm suffered under PHIPA.

Health Information Custodian Duties

Under PHIPA, [Organization Name] is considered to be a “health information custodian” because it has custody or control of patients’ personal health information. As a health information custodian, [Organization Name] is required to:

* Establish information practices that comply with PHIPA and follow those information practices;
* Designate a contact person who will:
	+ Ensure that [Organization Name] is complying with its obligations under PHIPA;
		- The contact person is (Insert position);
	+ Ensure that all employees are informed of their duties under PHIPA;
	+ Reply to any questions concerning their information practices from the public, or from any patients;
	+ Reply to any requests for access or correction under PHIPA; and
	+ Receive and investigate any complaints about breaches involving personal health information.
* [Organization Name] will also develop a written public statement that outlines:
	+ The information practices of [Organization Name];
	+ How to contact (Insert position of the custodian);
	+ How an individual may obtain access to or request any corrections to their personal health information; and
	+ The process for a person to make a complaint to the (Insert position) and to the Health Commissioner under PHIPA.
* [Organization Name] will ensure that consent is obtained when collecting, using, and/or disclosing a patient’s personal health information, except in any circumstances outlined by PHIPA;
* It will also ensure that the only the personal health information that is necessary under PHIPA is collected, used, or disclosed;
* [Organization Name] will ensure that all reasonable precautions are taken in order to safeguard against any theft, loss, or any unauthorized collection, use, disclosure, copying, modification, and/or disposal of patients’ personal health information
* [Organization Name] will inform the patient as soon as possible in the event that their personal health information is used in any way without their consent or outside of the company’s information practices;
* The Commissioner will be notified of any privacy breaches under PHIPA;
* [Organization Name] will ensure that all health records are accurate, up-to-date, and as complete as necessary for their purposes;
* All personal health records will be retained, transferred, or disposed of in a secure manner; and
* [Organization Name] will ensure that all employees are knowledgeable about the contents of this policy and their obligations under PHIPA.

Non-Compliance

The Information and Privacy Commissioner of Ontario (IPC) has been provided with the authority to impose administrative monetary penalties on contraveners of PHIPA. [Organization Name] will therefore be penalized if it is not compliant with PHIPA. The regulator can issue penalties up to a maximum of CAD500,000 for organizations as of January 1st, 2024.