3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

PRIVACY POLICY

POLICY STATEMENT

The Unionville Home Society is committed to individual privacy and to protecting the confidentiality of the health information it holds. It is a health information custodian under the *Personal Health Information Protection Act,* 2004 (“PHIPA”, or the “Act”). The Organization complies with PHIPA and protects “personal health information” as defined under the Act.

SCOPE

In this Privacy Policy (the “Privacy Policy”), we use the language of “Agent” to capture the commitment of the Organization and its agents, defined below: its staff, physicians, volunteers, students and vendors, to abide by this Privacy Policy and to reflect a shared commitment to protecting personal health information.

This Privacy Policy sets out privacy practices and standards to guide the Organization and its Agents. All Agents are obliged to abide by those policies and procedures.

Accountability for Personal Health Information

The Organization is responsible for personal health information in its custody and control, including information collected, used, or disclosed by its Agents.

Agents

“Agents”, including any person or entity that acts on the Organization’s behalf, have a defined role under PHIPA. They may collect, use, disclose, retain, or dispose of personal health information on the Organization’s behalf as permitted or required by law; and only as directed by the Organization. Agents must notify the Organization at the first reasonable opportunity if personal health information they handle on behalf of the Organization is stolen, lost or accessed by unauthorized persons.

We require any Agent 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 pledges annually, privacy training, and contractual means.

Privacy Officer

3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

The Privacy Officer manages the Organization's compliance with this Privacy Policy and PHIPA. The following individual has been designated as the Privacy Officer:

Olga Gluchovsky
4300 Highway 7
Unionville, ON L3R 1L8
ogluchovsky@uhs.on.ca
905-477-2822 ext. 4236

Identifying Purposes for Collecting Personal Health Information

The Organization collects personal health information for purposes related to direct care, administration and management of our programs and services, client billing, administration and management of the health care system, teaching, statistical reporting, fundraising, meeting legal obligations and otherwise, as 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.

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

The Organization requires consent in order to collect, use, or disclose personal health information. In some cases, we may collect, use or disclose personal health information without consent, but only as permitted or required by law.

For consent to be valid, the individual must have capacity to consent and give consent directly. Where required, consent must be obtained from his/her substitute decision-maker, as defined under PHIPA. The consent must be voluntary, knowledgeable, and relate to the information in question.

Implied Consent - For Care

Personal health information may also be released to an individual's other health care providers for health care purposes (within the "circle of care") without the express written or verbal consent of the individual as long as it is reasonable in the circumstances to believe that the individual wants the information shared with the other health care providers. No information will be released to other health care providers if the individual has stated he or she

does not want the information shared (for instance, by way of a “lockbox” on his or her health records, further discussed below).

An individual’s request for treatment constitutes implied consent to use and disclose his or her personal health information for health care purposes, unless he/she expressly instructs otherwise.

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

Within the Organization	**Outside the Organization**
• Registered Nurses • Personal Support Workers • Physicians, Locums • Nursing or other allied health care students • Social Worker • Administrator • Administrative support staff	• Hospitals • Ambulance, EMS • Pharmacists • Laboratories • Regulated health professionals in sole practice or group • A centre, program, or service for community health or mental health • Local health integrated networks (LHINs, re: direct service provision such as former CCAC role)

Express Consent - For Release of Records

Should the individual wish to release a copy of his or her record of personal health information to a lawyer, insurance company, family, employer, landlord or other third-party individuals or agencies (non-health care providers), the individual must sign a release of information form with the Nursing Department.

No Consent - For Limited Activities

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 individuals to (this is not an exhaustive list):

3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

- 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, e.g. Research Ethics Board approval, creation of a research plan)
- Teach, train and educate our Agents
- Compile statistics for internal or mandatory external reporting
- Respond to legal proceedings
- Comply with mandatory reporting obligations

If Agents 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, an individual may choose not to give consent or withhold consent. If consent is given, the individual 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 individuals the opportunity to restrict access to any personal health information or their entire health record by their health care providers within the Organization or by external health care providers. Although the term “lockbox” is not found in PHIPA, lockbox is commonly used to refer to the individual’s ability to withdraw or withhold consent for the use or disclosure of their personal health information for health care purposes. For more information, see the Organization’s relevant lockbox policy.

Limiting Collection of Personal Health Information

The Organization limits the amount and type of personal health information we collect to what is necessary to fulfill the purposes identified. We will not

3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

collect personal health information if other information, such as de-identified information, will serve the purpose for the collection. Information is collected directly from the individual, unless the law permits or requires collection from third parties.

Agents may only initiate their own projects to collect new personal health information from any source with permission of the Organization or the Privacy Officer.

3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

Limiting Use and Disclosure 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 individual or as permitted or required by law. The Organization will not use personal health information if other information, such as de-identified information, will serve the purpose.

Personal health information may only be used within the limits of each Agent's role. Agents 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 an Agent is in doubt whether an activity to use personal health information is part of his or her position, he or 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 individual or as permitted or required by law. We will not disclose personal health information if other information, such as de-identified information, will serve the purpose for the disclosure.

Personal health information may only be disclosed within the limits of each Agent's role. Agents 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 an Agent is in doubt whether an activity to disclose personal health information is part of his or her position, he or she is trained to ask the Privacy Officer.

Retention, Storage and Disposal of Personal Health Information

Health records are retained as required by law and professional regulations and to fulfill the Organization's purposes for collecting personal health information. For example, standards of health regulatory Colleges and associations apply. There may be reasons to keep records for longer than standard minimum periods.

3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

Personal health information that is no longer required to fulfill the identified purposes is securely destroyed, erased, or made anonymous safely and securely. Please see the Organization’s retention, storage, and disposal policy.

3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

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 an individual.

Safeguards for Personal Health Information

The Organization has 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 Agents 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 Organization's information security policy.

Openness About Personal Health Information

We make available the following information about the Organization's policies and practices relating to the management of personal health information:

- 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;
- Notice of information practices; and
- A description of how the individual may make a complaint to the Organization or to the Information and Privacy Commissioner of Ontario (the "**IPC**").

Privacy Breaches and Audits

A privacy breach occurs whenever a person contravenes or is about to contravene a rule under PHIPA or this Privacy Policy or related policies and

procedures of the Organization, including in cases where an individual's information is lost, stolen or accessed by an unauthorized person.

The Organization will conduct random audits routinely, and as deemed necessary in a given circumstance. Failure to comply with PHIPA, this Privacy Policy, related policies and procedures of the Organization, whether intentionally or inadvertently, may result in disciplinary action of the Agent, up to and including termination of employment, privilege, or services.

All privacy breaches must be reported immediately to the Privacy Officer. If you have any questions, contact the Privacy Officer. For more information, see the Organization's relevant privacy breach protocol.

Individual Access to and Correction of Personal Health Information

Individuals may make written requests to have access to or correction of their records of personal health information, in accordance with the Organization's relevant access and correction policy.

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

Individuals 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, individuals may ask to append a statement of disagreement to their file.

The Organization may not be able to provide access to all the personal health information we hold about the individual. 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. See the Organization's Access & Correction policy for more detail.

Assessments of and Challenges to Compliance with the Organization's Privacy Policies and Practices

Any person may ask questions or challenge our compliance with this policy or with PHIPA by contacting the Organization's Privacy Officer, who will**:**

3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

- Receive and respond to complaints or inquiries about the Organization policies and practices relating to the handling of personal health information.
- Inform individuals who make inquiries or lodge complaints of other available complaint procedures.
- Investigate all complaints. If a complaint is found to be justifiable, the Organization will take appropriate measures to respond.

3005 Privacy Policy

Manual: 1000 Corporate	Section
Reviewer: Julie Horne	Original Date September 7, 2022
Approver: Julie Horne	Next Review Date September 2, 2026

The IPC oversees the Organization's compliance with privacy rules and PHIPA. Anyone can make an inquiry or complaint directly to the IPC 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
> www.ipc.on.ca

The Organization conducts routine assessments of new and modified work processes or systems, as well as operational compliance with this policy and with PHIPA routinely. For more information, see the Organization's relevant compliance policy.

References: *Personal Health Information Protection Act,* 2004.