Société **Alzheimer** *Society*

Programs and Services Policy

Policy: Client Privacy and Confidentiality	**Number: PS-PRI-01**
Effective Date: July 2021 **Review:** July 2021	**Pages:** 8

POLICY

The Alzheimer Society is committed to client 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 Society is accountable and liable for compliance with PHIPA and protects "**personal health information**" (PHI) as defined under the Act.

In this Privacy Policy (the "**Privacy Policy**"), we use the language of "**Agent**" to capture the commitment of the Society and its agents, defined below: its staff, volunteers and students, 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 Society and its Agents. All Agents are obliged to abide by those policies and procedures. Additionally, regulated health professionals will be guided by the standards of practice governing their profession.

The responsibility of the protection of personal information, including personal health information, outlives the professional relationship and continues indefinitely after the provider has ceased to care for the client.

ACCOUNTABILITY FOR PERSONAL HEALTH INFORMATION

The Society is responsible for PHI 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 Society's behalf, have a defined role under PHIPA. They may collect, use, disclose, retain, or dispose of personal health information on the Society's behalf as permitted or required by law; and only as directed by the Society. Agents must notify the Society at the first reasonable opportunity if personal health information they handle on behalf of the Society is stolen, lost or accessed by unauthorized persons.

We require any Agent who collects, uses, or discloses PHI on our behalf to be aware of the importance of maintaining the confidentiality of PHI. This is done through the signing of confidentiality pledges annually, privacy training, and contractual means.

Our commitment to privacy is demonstrated by adherence to this policy. To that end, we will follow the outlined procedures to protect the PHI we hold, and will educate staff and any others who collect, use, or disclose PHI on our behalf about their privacy responsibilities.

Privacy Officer

Société Alzheimer Society

Programs and Services Policy

The following agent has been designated as the Privacy Officer:

Melanie Bouck
420 East St. N
Sarnia, ON N7T 6Y5
519-332-4444 ext. 224
mbouck@alzheimersarnia.ca

The Privacy Officer manages the Society's compliance with this Privacy Policy and PHIPA.

IDENTIFYING PURPOSES FOR COLLECTING PERSONAL HEALTH INFORMATION

The Society collects PHI for purposes related to:

- Providing health support and services based on client needs
- Delivering programs and service
- Communicating with other healthcare professionals involved in client care
- Seeking client consent (or consent of a substitute decision maker) where needed
- Planning, administering and managing internal operations
- Performing risk management, error management and quality improvement activities
- Gathering statistics
- Completing research
- Carrying out client surveys
- Following legal and regulatory requirements
- Fulfilling other purposes permitted or required by law

When PHI 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 Society requires consent to collect, use, or disclose PHI. In some cases, we may collect, use, or disclose PHI without consent, but only as permitted or required by law.

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

Consent may be implied or expressed.

Implied Consent – (Disclosures to other health care providers for health care purposes for care)
PHI may also be released to client's other health care providers for health care purposes (within the "circle of care") without the express written or verbal consent of the client if it is reasonable in the circumstances to believe that the client wants the information shared with the other health care providers. No information will be released to other health care providers if the client has stated he or she does not want the information shared.

A client's request for care constitutes implied consent to use and disclose PHI for health care purposes unless the client expressly instructs otherwise.

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

- Staff, Volunteers, Students

- Home and Community Care
- Hospitals
- Long-term care homes
- Family health teams
- Ambulance
- Pharmacists
- Laboratories
- Regulated health professionals in sole practice or group
- Social workers and social service workers
- A center, program, or service for community health or mental health.

Express Consent - For Release of Records

The Society relies on implied consent for care. For other purposes, generally those not related to healthcare, the Society requires express consent, and the client must sign a release of information form to have PHI released. Examples where express consent is required for the release of PHI include, but are not limited to: lawyer, police, spiritual leaders/healers, insurance company, family, employer, landlord or other third-party clients or agencies (non-health care providers).

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 clients to (this is not an exhaustive list):

- Plan, administer and manage our internal operations, programs and services
- Receive payment for services
- 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 staff, volunteers and students
- Compile statistics for internal or mandatory external reporting
- Respond to legal proceedings
- Comply with mandatory reporting obligations, including a duty to report a threat of harm to self or others, which may include children in your care.

If Agents have questions about using and disclosing PHI without consent, they can ask the Privacy Officer.

Withholding or Withdrawal of Consent

A client may choose not to give consent or may withhold consent. If consent is given, the client 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.

PHIPA gives clients the ability to restrict access to their PHI, either in part or in full, from any internal or external health care providers.

Clients may initiate the process for restricting access by contacting the Privacy Officer. Clients must submit their request for a restricted access in writing. Clients will be asked to complete a request form that must be submitted to the Privacy Officer or designate.

Restricting access does not prevent the Society from using or disclosing PHI where there is a legal obligation to do so (for example, to fulfill mandatory reports to the Children's Aid Society or to the Ontario

Ministry of Transportation). The Society may also use or disclose PHI if there are reasonable grounds to believe that using or disclosing the information is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. There may be other circumstances where the use or disclosure of PHI is required or permitted by law, and agents should consult with a Privacy Officer when in doubt.

The Society provides programs and services based on a "shared care" model. This involves the use of a single client chart that, in appropriate circumstances as determined by the client's provider, may be shared with designated member(s) of our team. Should a client withhold or withdraw consent; the Society may only be able to provide limited programs and services.

LIMITING COLLECTION OF PERSONAL HEALTH INFORMATION

The Society limits the amount and type of PHI we collect to what is necessary to fulfill the purposes identified. We will not collect PHI if other information, such as de-identified information, will serve the purpose for the collection. Information is collected directly from the client 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 Society or the Privacy Officer.

LIMITING USE & DISCLOSURE OF PERSONAL HEALTH INFORMATION

Use

PHI is not used for purposes other than those for which it was collected, except with the consent of the client or as permitted or required by law. The Society will not use PHI if other information, such as de-identified information, will serve the purpose.

PHI may only be used within the limits of each Agent's role. Agents may not read, look at, receive, or otherwise use PHI unless they have a legitimate "need to know" as part of their position. If an Agent is in doubt whether an activity to use PHI is part of their position, consult with the Society's 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

PHI is not disclosed for purposes other than those for which it was collected, except with the consent of the client or as permitted or required by law. We will not disclose PHI if other information, such as de-identified information, will serve the purpose for the disclosure.

PHI may only be disclosed within the limits of each Agent's role. Agents may not share, talk about, send to, or otherwise disclose PHI to anyone else unless that activity is an authorized part of their position. If an Agent is in doubt whether an activity to disclose PHI is part of their position, consult with the Society's Privacy Officer.

RETENTION, STORAGE, & DISPOSAL OF PERSONAL HEALTH INFORMATION

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

PHI that is no longer required to fulfill the identified purposes is securely destroyed, erased, or made anonymous safely and securely. Please see Policy and Appendices related to Records Management: ORG-CUL-06.

The Alzheimer Society prohibits the use of parallel files (parallel files are copies of health records kept as hard copies outside of the main electronic client record) except for client requested "lockbox" (see policy PS-PRI-02). Health records will be kept in the electronic records management system (client database). Hard copies of health records will be scanned in a read only format to the electronic file. Once the record is scanned to the electronic file, Alzheimer Staff should double check the reliability of the digital copy and properly dispose (shred or delete) any hard copy.

Any paper documents will be stored in designated storage areas and shredding will occur according to retention schedule and approved by management.

ACCURACY OF PERSONAL HEALTH INFORMATION

The Society takes 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 client.

SAFEGUARDS FOR PERSONAL HEALTH INFORMATION

The Society has put in place safeguards for the PHI we hold, which include:

- Physical safeguards (such as locked filing cabinets and rooms);
- Organizational safeguards (such as permitting access to PHI 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 PHI we hold is protected against theft, loss and unauthorized use or disclosure.

Anyone who collects, uses or discloses PHI on behalf of the Society is made aware of the importance of maintaining the confidentiality of PHI. This is done through the signing of confidentiality agreements, privacy training, and contractual means.

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

OPENNESS ABOUT PERSONAL HEALTH INFORMATION

We make available the following information about the Society'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 client may make a complaint to the Society or to the Information and Privacy Commissioner of Ontario (the "**IPC**").

The Society posts its privacy statement in high traffic areas, in brochures and on its website.

PRIVACY BREACHES & 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 Society, including in cases where a client's information is lost, stolen, or accessed by an unauthorized person.

The Society 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 Society, 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 who will follow the Society's Privacy Breach Protocol, PS-PRI-04 APPENDIX 04.

CLIENT ACCESS TO AND CORRECTION OF PERSONAL HEALTH INFORMATION

Clients may make written requests to have access to or correction of their records of personal health information by contacting the Privacy Officer who will act in accordance with the Society's relevant Access and Correction Policy, PS-PRI-04.

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

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

The Society may not be able to provide access to all the PHI we hold about the client. 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.

ASSESMENTS OF AND CHALLENGES TO COMPLIANCE WITH THE SOCIETY'S PRIVACY POLICIES AND PRACTICES

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

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

The IPC oversees the Society'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

Société Alzheimer Society

Programs and Services Policy

Phone: 1 (800) 387-0073 (or 416-326-3333 in Toronto)
Fax: 416-325-9195
www.ipc.on.ca

The Society will receive and respond to complaints or inquiries about its policies and practices related to the handling of PHI. Clients who make inquiries or lodge complaints will be informed of the available complaint procedures – see ORG-CUL-05 Comments, Compliments and Complaints.

SCOPE:
This policy applies to board of directors, staff, volunteers, students, and vendors, are to abide by this Privacy Policy and to reflect a shared commitment to protecting personal health information.

DEFINITION(S):

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

Blocking: blocking a health record is a common term for a client who withholds or withdraws consent to collect, use or disclose their health record for healthcare purposes. This is also referred to internally a as lock box or consent directive.

Confidentiality - is the protection of acquired information about a client.

Stakeholder: Board members, staff, students, volunteers, vendors, and any other agents of the Alzheimer Society of Sarnia-Lambton

Personal Health Information: Personal Health Information (PHI) as defined by the provincial Personal Health Information Protection Act (PHIPA) refers to identifying information about an individual in oral or recorded form relating to their physical or mental health (including personal and family medical history), the provision of health care to the individual including a plan of service, payments or eligibility for health care, substitute decision-makers, organ and tissue donation information and health number. In addition, any other information about an individual that is included in a record containing PHI is also part of this definition.

Identifying Information: information is considered "identifying" if it is foreseeable that it could be used alone or in combination with other information that is reasonably available to identify a client.

Health Record: a health record is any written (including, but not limited to, electronic) information that contains personal health information about a client.

Implied Consent: implied consent is obtained when, given the circumstances of the client, it is reasonable to conclude that the client has by their conduct consented to the collection, use or disclosure of the client's personal health information.

Express Consent: express consent is obtained when a client explicitly agrees orally or in writing to the collection, use and disclosure of the client's personal health information.

Privacy Breach: A privacy breach occurs with respect to personal information, when there is unauthorized access or disclosure of information and/or loss of information that could result in information being accessed or disclosed without authority. Breaches can be intentional or unintentional and may be the

result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

Privacy Incident: A privacy incident is typically less severe than a privacy breach. An incident occurs when personal information is mishandled or incorrectly collected, used or disclosed. However, unlike a privacy breach, the situation can be corrected easily and quickly without any prejudice to the individual.

POLICY REVIEW:

The Executives will review this Policy every 2 years and will present recommended and required revisions to staff Society. If there are legislated changes required, these changes will be made as close as possible to the effective date of the legislative change.