lumenus
Community Services

POLICY

POLICY MANUAL SECTION Organizational	POLICY NAME Privacy of Personal Health Information	POLICY NUMBER ORG 207
POLICY MANUAL SUBSECTION	RESPONSIBILITY Privacy Officer	APPROVED BY CEO
LAST REVIEW DATE November 2025	LAST APPROVAL DATE November 2025	NEXT REVIEW DATE November 2027

SCOPE

This policy establishes requirements and procedures for the protection of the personal health information of Lumenus clients.

POLICY

Lumenus is legally required to protect the confidentiality of the personal health information of all clients that have received services from Lumenus programs.

Lumenus' Privacy Policy is organized around the ten principles of *Ontario's Personal Health Information Protection Act (PHIPA)* which governs the way personal health information may be collected, used and disclosed. If there is a discrepancy between this Policy and *PHIPA*, *PHIPA* takes precedence.

The following definitions will apply to the interpretation and application of this Policy:

"Personal Health Information" (PHI) includes any identifying information verbal, written or electronic about an individual that:

- Relates to the physical or mental health of the individual;
- Relates to any health service provided to the individual;
- Is collected in the course of providing health services to the individual;
- Is collected incidentally to the provision of health services to the individual; or
- Identifies the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual

Information is identifying when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

"**Health Information Custodian**" (HIC) means an individual or organization identified in section 3 (1) of PHIPA who has custody or control of PHI. Lumenus, as an organization, is a HIC.

"**Agent**" in relation to PHIPA, means any individual who is authorized by the organization to do anything with respect to PHI. For Lumenus, this includes employees, volunteers, students or contracted agents who deal with, or have access to, PHI.

"**Privacy Officer**" Every organization that is a health information custodian must appoint one or more employees as Privacy Officers. A privacy officer is responsible for the privacy practices of the organization. At Lumenus, a member of the senior management team is the designated Privacy Officer and contact person on matters related to privacy.

"Privacy Breach" refers to whenever a person has contravened or is about to contravene a provision of the PHIPA or its regulations.

PROCEDURE

Anyone who collects uses or discloses PHI on behalf of Lumenus is required to follow these 10 information practices.

1. Accountability

The Lumenus Chief Executive Officer (CEO) ensures that the organization is compliant with all privacy legislation and designates a Privacy Officer (PO) to have oversight of the organization's privacy practices to meet legislative requirements.

The PO is responsible for:

- Keeping current with legal privacy developments and with best practices within the healthcare industry;
- Addressing privacy questions, concerns and challenges to the organization including privacy breaches;
- Ensuring continuous improvement of health information practices;
- Ensuring that privacy policy review is implemented and ongoing for all those who can access organization personal health information as part of the onboarding of employees and acknowledged through HRIS system.
- Receiving and responding to complaints as they relate to privacy.
- Ensuring proper safeguards are in place to protect health information at Lumenus.

Lumenus will make the name and contact information of its Privacy Officer publicly available on the Lumenus website, through notices distributed to Lumenus clients, and by making the information available upon request.

All Lumenus employees and other parties who access PHI of Lumenus clients are responsible for managing the PHI to which they have access, in compliance with this Policy and with PHIPA.

Lumenus will take the necessary steps (e.g., through contractual or other means) to ensure that a comparable level of privacy practices is employed by external stakeholders (third parties) that it is working with or purchasing related services from.

Lumenus has other policies and procedures that give effect to this Policy including:

- Consent to Release Information Policy
- Confidentiality Policy
- A client complaints process that includes the ability to submit a complaint regarding alleged or actual breaches of this Policy
- Procedures for communicating the Policy to Lumenus Agents, for training them about privacy policies and procedures, and a Confidentiality and Privacy agreement that all Agents are required to sign as a condition of employment or engagement with Lumenus and requires them to read, understand, and comply with the Policy.

Lumenus reviews this Policy and its supporting policies and procedures every two (2) years to ensure its privacy practices adhere to legal requirements and industry best practices. In addition, the Privacy Officer is responsible for ensuring that significant updates to PHIPA or guidance documents from the IPC are communicated to employees as they become available and the Policy modified accordingly if necessary. Any amendments to this Policy and its supporting policies and procedures are approved by senior management. Amendments are communicated to Lumenus employees by the Privacy Officer or their designate.

2. Purposes for Collecting Personal Health Information

Lumenus and its Agents collect personal information for the following purposes:

- Direct client care
- Administration of Lumenus and the health care system
- Authorized health research, teaching and statistics
- Complying with legal and regulatory requirements
- Planning, delivering, evaluating, monitoring and allocating resources to Lumenus Programs and services

In collecting PHI, Lumenus Agents will:

- Identify and explain the purpose(s) for which Lumenus collects, uses, and/or discloses PHI at or before the time the information is originally collected;
- Communicate verbally or in writing the identified purposes to the person(s) from whom the PHI is sought; and,
- Communicate verbally or in writing any new purpose for using or disclosing PHI and obtain the client's consent, as appropriate, prior to making any such uses or disclosures.

3. Consent for Collection, Use and Disclosure of Personal Health Information

Information which is collected, used, or released will be used only for the purpose for which it is collected.

Lumenus can rely on implied consent with other health care custodians under the law, however when possible and appropriate expressed consent will be obtained. If expressed consent has been obtained, reasonable attempts must be made to obtain it in writing. If only verbal consent has been obtained, this must be documented in the client's health record.

The client or their substitute decision maker may withdraw such consent at any time.

Consent to collect use, and release PHI expires when the client is discharged from Lumenus or when they decide to withdraw consent which is effective from the date of withdrawal and cannot be retroactively applied.

To release **written** information, the service provider must obtain expressed written consent.

To release information **verbally** to anyone in the circle of care, implied consent may be used, however, explicit consent is preferable if possible. Note the circle of care can only include other HICs who are involved in service to the client. Non-HICS are never part of the circle of care.

The client or substitute decision maker has the right to request a copy of the information that is released to another party.

When a third party wants to speak to a Lumenus PHI holder about a client who has been discharged from Lumenus, the Lumenus PHI holder requires the discharged client's signed consent before speaking to the third party.

A client may at any time withdraw or withhold their consent to the use and/or disclosure of their PHI for the purposes of health care by giving reasonable notice, verbally or in writing to Lumenus of their intention to do so. If the request to withdraw consent is verbal, the client requesting the withdrawal will be asked to follow up with a written request. Consent cannot be retroactively withdrawn. Service providers are required to document verbal consent or withdrawal of consent in the client information system.

Upon receiving such a request, Lumenus will discuss the following with the client:

- The potential impact their withdrawal may have on their health care,
- Any legal limitations to which their withdrawal of consent may be subject (e.g. PHI will be disclosed in a life-threatening situation regardless of the client's withdrawal of consent.)
- Service providers/employees are encouraged to speak to their manager and the Privacy Officer if a client does not want to provide consent to service.

There are circumstances where Lumenus is permitted or required by law to collect, use and disclose PHI without the consent of the client, such as for health research, teaching and statistics, public health monitoring and quality assurance. In such circumstances, Lumenus will only use and disclose client PHI without consent as permitted or required by law.

4. Limits on Collection of Personal Health Information

Lumenus will limit the amount and type of PHI it collects to that which is necessary to fulfill the purpose identified. Lumenus will not collect PHI indiscriminately or unnecessarily.

Lumenus will collect PHI using fair and lawful means in order to ensure that clients are not misled or deceived about the purposes for which their information is collected.

5. Use, Disclosure and Retention of Personal Health Information

Lumenus and PHI holders will not collect, use or disclose client's PHI for purposes other than those for which it was collected, except with the consent of the client to whom the PHI relates or is as permitted or required by law.

Where consent is obtained to use or disclose PHI for a new purpose not previously identified, Lumenus will document this new purpose in this Policy.

Lumenus will retain PHI only as long as is necessary to fulfill the purpose for which it was collected or as permitted or required by laws governing retention of PHI and health records.

PHI that Lumenus employees use to make a decision about a client will be retained as part of the client record to allow the client access to the information after the decision has been made. The types of information Lumenus routinely collects are contact information, assessment and service delivery information.

Lumenus has policies and procedures in place to specify retention periods and methods to destroy PHI once retention periods are complete. Such processes prevent unauthorized parties from gaining access to PHI in the course of the destruction process. Lumenus complies with legislation and accreditation standards related to retention of client records. See policy **PS-815 Client Record/File Management Policy**.

6. Accuracy of Personal Health Information

Lumenus ensures that PHI collected is as accurate, complete and as up-to-date as is necessary for the purposes for which it is used and to minimize the possibility that inappropriate or inaccurate information may be used to make a decision about the client's service delivery.

Lumenus provides documentation training and support, and chart review practices.

Where a client successfully demonstrates that PHI in the custody or control of Lumenus is inaccurate or incomplete, Lumenus will amend the information to make it accurate and complete unless it involves making a correction to an opinion made by a service provider in good faith. Where appropriate, the amendment of such PHI will be provided to third parties having access to the information in question. Any statement of disagreement will be attached to the client's record of PHI.

Lumenus does not amend the documentation of other organizations.

7. Safeguards for Personal Health Information

All PHI in the custody, or under the control, of Lumenus will be protected by the following administrative, technical, and physical safeguards:

- Lumenus uses administrative safeguards such as this policy and its supporting policies and procedures, contractual means (e.g. confidentiality agreements and contracts) and training to inform its employees and third parties of the safeguards they must employ to protect the PHI to which they have access.
- Lumenus applies technical safeguards such as computer access codes, login passwords, and encryption software on all electronic data stores where PHI is retained or accessed.
- Lumenus uses physical safeguards (such as locked cabinets, offices, and secure work environments) to protect PHI in electronic and hard copy form from inappropriate or unauthorized use and disclosure.
- Lumenus ensures that the transmission of PHI is limited to secure and/or encrypted methods including when PHI is shared between service providers
- Service providers are allowed to use text messages for scheduling appointments based on client preferences and with client consent. Any communication with clients over text message must take into account the limitations of security of texting and ensure that sensitive information is not included in the texts. Service providers are prohibited from using text messages as a means to exchange PHI with clients, internal Lumenus employees or external service providers. **PS-807 Email and Communication Policy**

Any person or Agent who suspects or becomes aware of a Privacy Breach will follow the Privacy Breach Management Protocol found in Appendix A to this Policy.

8. Openness about Lumenus' Privacy Policy

Lumenus will make available on its website information about Lumenus' privacy policy and practices including:

- The process of requesting access to PHI held by Lumenus.
- A description of the types of PHI held by Lumenus, including a general account of its use.
- Brochures or other documents that explain Lumenus' policies, standards or codes; and,
- Contact information for the Lumenus Privacy Officer.

9. Individual Access to Personal Health Information

Upon request in writing to the Privacy Officer, a client will be informed of:

- The existence of any PHI related to them in the custody or under the control of Lumenus:
- The uses to which that information has been put; and,
- Disclosure by Lumenus of such information to any third parties unless Lumenus is required or permitted by law to withhold such information.

A client seeking access to information about the PHI that Lumenus has in its custody or under its control, has the responsibility to provide satisfactory proof of identification to Lumenus before it is able to provide an account of the existence, use and disclosure of PHI.

In providing information about third parties to whom PHI has been provided, Lumenus will be as specific as possible.

Lumenus may request that the client, seeking access to their PHI, meet with an appropriate healthcare practitioner about the requested PHI before such information is provided; however, Lumenus does not have the authority to require such as meeting.

If, for any reason, Lumenus has PHI about a client that it cannot release to them for legal or other reasons, the reasons for such refusal will be provided to that client upon request. A client is entitled to challenge the refusal by submitting a request in writing to the Privacy Officer.

Lumenus will provide clients with access to their PHI at minimal or no cost within 30 days, subject to extension upon appropriate notice. Should the client require photocopies of such information, Lumenus reserves the right to charge the client an amount that reasonably covers the cost of photocopying.

10. Challenging Compliance with the Lumenus Privacy Policy

An individual is entitled to challenge Lumenus's compliance with this Policy. Any such challenge must be made in writing and directed to the Privacy Officer by email at: privacy@lumenus.ca

Lumenus has procedures to receive and respond to complaints, challenges or inquiries about its practices relating to the handling of PHI.

Anyone who submits a written complaint, challenge or inquiry will be provided with a written copy of Lumenus' policy and procedures governing such complaints, challenges and inquiries.

Lumenus investigates all complaints received in accordance with the established procedure. If a complaint is found to have merit, Lumenus will take appropriate measures to address the complaint, including if necessary, amending its policies and practices in respect of the handling of PHI.

lumenus
Community Services

APPENDIX A - PRIVACY BREACH MANAGEMENT PROTOCOL*

STEP 1	**RESPOND and REPORT: Take action and report when a breach is suspected or known.** ● Anyone aware of a privacy breach or suspected privacy breach should report it to their supervisor/manager immediately and to the Privacy Officer within 1 business day. ● Depending on the risk to the organization, the Privacy Officer may inform the CEO and/or other Senior Leadership. ● The reporting Employee/Manager will complete a Privacy Breach Report.
STEP 2	**CONTAIN** **Identify the scope of the breach/potential breach and take steps to contain it.** The Privacy Officer is responsible for: ● Ensuring the collection of any hard copies of Personal Health Information (PHI) that has been disclosed. ● Ensuring that no copies of PHI have been inappropriately made or retained. ● Determining whether the breach would allow unauthorized access to any other PHI and taking whatever steps are needed (e.g. changing passwords, ID numbers etc.) to protect that information. ● Take any other steps necessary to contain the breach
STEP 3	**NOTIFY: Identify and notify those individuals whose privacy was breached.** The Privacy Officer is responsible for ensuring that the client or applicant is notified at the first reasonable opportunity (by phone, in writing, or in person) of the breach and the steps to contain the breach.
STEP 4	**INVESTIGATE and REMEDIATE** The Privacy Officer will: ● Conduct an internal investigation to: ensure that immediate requirements of containment and notification have been addressed; review circumstances surrounding breach; and review internal policies. ● If appropriate, report the breach to the Information and Privacy Commissioner. ● Ensure that employees have adequate training. ● Document the breach in preparation for the annual privacy breach report that must be submitted to the IPC at year end (December 31st).

*For detailed information about protocols, please refer to www.ipc.on.ca
What to do When Faced with a Privacy Breach: Guidelines for the Health Sector