Ontario Medical Association

Effective Date: May 8, 2025
Review Date: May 9, 2027

Privacy Policy

1. PURPOSE

The purpose of this policy is to describe the OMA's role as a custodian of personal information (PI) and personal health information (PHI), and to describe the OMA's accountabilities for the protection of privacy and appropriate handling of PI and PHI, as defined in applicable legislation.

2. POLICY

It is the OMA's policy to protect the privacy of individuals whose personal information or personal health information is in the OMA's custody.

The Privacy Officer develops and maintains this policy. It should be reviewed every two years.

3. SCOPE

This policy includes:

- 3.1 The OMA's status under privacy legislation
- 3.2 The OMA privacy program and reporting structure
- 3.3 The measures the OMA takes to meet its legislated privacy principles

4. INDIVIDUALS INVOLVED

This policy applies to:

- 4.1 All OMA officers, employees, contractors, and agents who provide services to or on behalf of the OMA in connection with the OMA's delivery of products, services and information to its members.

5. DEFINITIONS

Employee: The OMA considers an "employee" to be any officer, employee, contractor, or agent of the OMA.

Personal Information (PI): The OMA adopts the *Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA)* definition of "personal information" as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization"[1];

[1] Definition of personal information http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html

- **Personal Health Information (PHI)**: The OMA adopts the *Personal Health Information Protection Act, 2004 (PHIPA)* definition of "personal health information" as amended from time to time."[2]

Data sharing agreement: A "data sharing agreement" is a contract that clarifies the rights and obligations of two or more parties that are sharing PI or PHI to ensure that each party complies with the relevant legislation.

POLICY SPECIFIC INFORMATION AND RESPONSIBILITIES

Status of the OMA

The OMA represents the political, clinical, and economic interests of Ontario's medical profession. The OMA provides its members with a variety of services including practice management, professional and personal support programs and advocacy for doctors and patient care.

The OMA is subject to the requirements of the *Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA)* through the services it provides its members, partners and other individuals and organizations. Specific OMA business units are also subject to the requirements of the *Personal Health Information Protection Act, 2004 (PHIPA)* namely the Physician Health Program in its role as a health information custodian. As such, the OMA is accountable under these *Acts* for protecting the privacy of individuals whose personal information or personal health information is in the OMA's custodianship, and for managing this information in accordance with the requirements of these pieces of legislation. The OMA further commits to best practices and standards in privacy protection regardless of legislation, including in situations where legislation may not apply.

The authority of the OMA to collect, use and disclose personal information is through the consent of its members and other individuals. The OMA also has the authority to collect, use, and disclose personal information as permitted by law.

Privacy standards

The OMA's privacy program will be informed by:

- Relevant legislation and regulations, primarily PIPEDA, and PHIPA where relevant;
- Recognized standards and best practices in privacy protection and management; and
- Orders, guidelines, and best practices produced by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of Ontario.

The OMA's privacy program will meet or exceed generally accepted privacy standards and relevant legislative requirements.

[2] Definition of personal health information http://www.ontario.ca/laws/statute/04p03.

The OMA will promote a culture of privacy protection, which will include training and awareness activities for all OMA employees.

Whenever the OMA adopts a new initiative, it will use a privacy-by-design approach.

OMA privacy program

The OMA's privacy program will be developed and managed by the OMA Privacy Officer.

The Privacy Officer will ensure that the OMA's privacy program includes mechanisms and processes to appropriately safeguard the privacy of individuals from whom PI or PHI has been collected.

The Privacy Officer will:

- Maintain the OMA's privacy policies and procedures;
- Support staff in following and meeting the requirements of the OMA privacy program;
- Ensure that OMA employees receive appropriate privacy and security awareness training;
- Develop and distribute communications materials to interpret the OMA privacy program to the public;
- Ensure that all OMA employees and contractors sign a Confidentiality Agreement with the OMA.

The Privacy Officer and Risk Management staff will complete annual assessments by checklists of the OMA's privacy and security safeguards to address program and system changes or changes in legislation, or as needed after a privacy breach.

Policy authority

The OMA provides a spectrum of services to its members. Unless otherwise noted, this privacy policy and all of the related procedures apply to all OMA business units and to OMA-related activities of all OMA employees, wherever these activities are conducted.

Where there is a discrepancy or gap between this privacy policy and any relevant legislation or regulation, the legislation or regulation will take precedence.

Except where the OMA Privacy Officer has developed privacy policies or procedures for a specific business unit or line of business (e.g., Physician Health Program) these policies and procedures will prevail should a discrepancy or gap exist.

Failure on the part of any OMA employee or third-party service provider to comply with this policy or with provisions or conditions in relevant agreements, contracts or processes may result in disciplinary action up to and including dismissal and/or legal action.

Identification of purposes

The OMA will document its purposes for all collections of PI or PHI.

The OMA will collect PI or PHI for the purposes of fulfilling OMA programs and activities only. These purposes include but are not limited to:

The collection, use and disclosure of member personal information for the following purposes:

- To register as an OMA member;
- To communicate with for OMA membership products, services, and information;
- To assess needs as an OMA member to determine which OMA products and services are useful and relevant;
- To manage our continuing relationship with the member;
- To conduct and carry out OMA business, including negotiations with government;
- To conduct surveys and polls of OMA members;
- To permit affiliated and other reputable third-party organizations, subsidiaries, and preferred suppliers to provide products, services, and information to members;
- To facilitate communication and otherwise assist individuals or institutions during a public health or other emergency;
- To meet any legal or regulatory requirements such as disclosures under the Ontario *Not-for-Profit Corporations Act*; and
- For other purposes consistent with the above.

From time to time, the OMA receives requests from members, under the Ontario *Not-for-Profit Corporations Act* section 96, for member contact information. This information is restricted to names and business addresses kept in a register specific to the purposes of the Ontario *Not for Profit Corporations Act*.

As applicable, OMA employees will communicate and explain the purposes for collecting PI or PHI to individuals either verbally or in writing through OMA documentation and communication materials before the collection takes place.

If the OMA wishes to use PI or PHI for a new purpose that was not communicated to the member at the time of collection or permitted by law, then the OMA will obtain consent from members before using PI or PHI for a new purpose.

Communication

The Privacy Officer will make available to members and the public a privacy notice that includes:

- Her or his name and contact information;
- How to access PI or PHI held by the OMA;
- A description of what PI and PHI the OMA collects and how it uses this information;
- What information is made available to OMA subsidiaries and other third parties.

The Privacy Officer will ensure that the privacy notice:

- Uses plain and simple language;

- Is consistent in tone, format and appearance across OMA business units, subsidiaries and partners;
- Is consistent in tone, format and appearance across mediums;
- Is available on OMA websites at points where the OMA uses its website to collect PI or PHI;
- Is in all languages required by law;
- Is clearly dated; and
- Is the most current notice available.

The Privacy Officer will ensure that all OMA business units are aware of any change to OMA privacy notices as soon as possible.

The Privacy notice shall be posted on the OMA website.

Consent

OMA employees will rely on an individual's implied consent for the collection, use and disclosure of her or his PI or PHI, unless it is authorized under legislation.

Under PIPEDA, the OMA is authorized to collect, use and/or disclose PI without the individual's knowledge or consent if it is:

- Clearly in the interests of the individual and consent cannot be obtained in a timely way, e.g., an emergency situation;
- For collecting a debt owed by a member or individual to the OMA;
- For specific research purposes as explained under PIPEDA;
- To comply with a subpoena or warrant issued or an order made by a court; or
- For purposes related to investigating a breach of an agreement or a violation of the laws of Canada or a province.

OMA employees will never obtain consent through deception or coercion.

OMA employees will respect a member's right to withdraw consent for secondary or additional uses and disclosures of his or her personal information and employees will take required measures to not use the PI or PHI.

Members will not be able to withdraw consent for the use and disclosure of their PI or PHI in cases where the OMA has legislative authority to collect, use and/or disclose the information without the consent of the member (e.g. the information relates to a government investigation, the member owes a debt to the OMA).

Limiting collection

OMA employees will limit the collection of PI or PHI to only the information that is required to fulfill the purposes for which the information was collected.

OMA employees will not indiscriminately collect member PI or PHI or collect PI or PHI in the expectation that the information may be of use in the future unless the OMA has identified this purpose and the member has given her or his consent for collection for this purpose.

Accuracy

OMA employees will ensure that PI or PHI held by the OMA is correct, complete and current for the purposes for which it was collected and to minimize the possibility that inaccurate information is being used to make a decision about the member.

OMA business units will identify PI or PHI data elements (e.g. address, phone number) they collect and use that require updating at specific times and for specific purposes.

OMA business units will ensure the accuracy and completeness of the PI or PHI that requires updating.

Limiting use, disclosure, and retention

OMA employees will limit the use and disclosure of PI or PHI to only those activities that support the purposes for which the information was collected, and either

- For which the individuals from whom the information was collected have provided consent, or
- What is authorized or required by applicable legislation (e.g. an emergency situations relating to the member, a government investigation).

The OMA will maintain documentation on all external organizations and individuals to which OMA business units disclose PI or PHI and the purposes for these disclosures.

The OMA business unit manager will notify the Privacy Officer if PI or PHI will be linked or cross-referenced to other information in other information systems, technologies, or programs internal and external to the OMA.

If PI or PHI is linked, the OMA business unit managers will provide the Privacy Officer with details on:

- How PI or PHI is linked or cross-referenced;
- Who will have custody of the other information system, technology or program;
- Why the link is required; and
- What the effect(s) would be if the link was not possible.

The Privacy Officer will ensure that employees retain PI or PHI:

- Only for the time period required to fulfill the purposes for which the information was collected;
- As authorized or required by legislation; and

For the period of time specified for the PI or PHI by law or as required for the purpose for which the information was collected. All retention periods will align with and meet applicable legislative requirements.

PI or PHI that is no longer required by the OMA for its identified purposes will be securely destroyed, rendered irretrievable or anonymized to prevent unauthorized access to the information. OMA employees will be required to transfer or delete PI or PHI from portable devices (e.g., laptops, tablets) and portable media (e.g., USB drives) once it is no longer needed for the purposes it was approved for and while being stored on the device.

Destruction and Disposal of Records

Under PIPEDA, the retention period is set at two years unless the collection information continues to be required for the purpose for which it is collected.

Individual OMA business units will document all uses for personal information or personal health information in their custody. In other words, units will create and keep an inventory of types of personal information and accompanying uses. This list of information and uses shall be reviewed by the relevant department staff annually to ensure the information collected is still being used for the purposes set out. Changes to this list will then be reviewed by the Privacy Officer to determine next steps.

OMA business units will securely dispose of PI or PHI that has served its purpose.

OMA employees will place paper documents that contain PI or PHI in a secure shredding bin.

Third party service providers will provide the OMA with certificates of destruction for all PI or PHI that they dispose of.

Education and Training

All OMA staff will be required to complete privacy training at onboarding. Thereafter, all staff will be required to complete an annual privacy refresher online.

At least once per year, the Privacy Officer shall address privacy at an all-staff meeting.

Privacy incident management

The Privacy Officer will ensure that the Board of Directors, the Senior Management Group, privacy leads and all OMA employees have the capacity and knowledge to implement measures for the containment, resolution and investigation of privacy and security incidents within the OMA.

For every confirmed privacy and security incident, the Privacy Officer will manage the execution of procedures to:

- Contain the incident;
- Determine the nature and scope of the incident;
- Work with any relevant stakeholders to investigate and resolve the incident;
- Provide notifications through a documented communications and escalation process;

- Evaluate the cause(s) of the incident and conduct remediation activities as required; and
- Document the incident in a breach log.

All OMA employees who believe they may have been involved in a breach incident shall (1) fill out the Privacy Breach Management Checklist and (2) report the incident as soon as it is discovered to their manager and the OMA Privacy Officer. OMA employees shall not delete any information or documentation relevant to the breach.

Safeguards

The Privacy Officer, business unit managers and other OMA staff will ensure that the OMA uses appropriate safeguards to protect personal information, including:

- **Administrative safeguards** such as training and awareness activities;
- **Technical safeguards** such as firewalls and encryption; and
- **Physical safeguards** such as locked cabinets for paper records of PI or PHI.

De-identification of PI or PHI

Information will be deemed to be **de-identified** if all direct identifiers (e.g. name, OHIP number, address) are removed and only a limited number of indirect identifiers (e.g. date of birth, a common medical condition, gender) remain, so that when the information is used in combination with other information it is not reasonably foreseeable to the OMA that the information could be used to re-identify an individual.

OMA employees will be required to use or disclose de-identified or aggregate data instead of PI or PHI where such data will support OMA programs, services or agreements with third parties.

OMA employees will not attempt to identify individuals from or by using de-identified information.

The OMA or its third-party service providers will be responsible for de-identifying information and will follow approved procedures for de-identifying PI or PHI.

Data sharing agreements

The OMA will enter into data sharing agreements with any organization from which it indirectly collects PI or PHI or to which it discloses PI or PHI.

Agreements prior to access to personal information or personal health information

The OMA will execute agreements with all third party service providers for services before providing the third party service provider with access to PI or PHI, or to environments where employees of the service provider may have access to PI or PHI.

The OMA will ensure due diligence for privacy issues when selecting a vendor for third party services.

Third party service providers with access to PI or PHI will be subject to the same conditions, where applicable, as OMA employees regarding the handling of this information.

OMA managers or employees responsible for procurement of services will ensure that an agreement with a third-party service provider:

- Describes the purposes for any access (including incidental access) of service provider employees to PI or PHI;
- Obligates the service provider to meet all obligations in the OMA Privacy Policy that apply to the activities of the service provider employees or substantively similar terms;
- Specifies privacy and security terms for the transfer of PI or PHI between the OMA and the service provider where such transfers occur; and
- Includes the right of designated OMA employees to audit the practices of the service provider to ensure that specified privacy and security controls and service delivery terms have been implemented as required in the agreement with the service provider.

Privacy review shall be part of the legal review process for external agreements.

Privacy Impact Assessments

All OMA employees/business units considering a new project or agreement shall assess whether the project requires a privacy impact assessment (PIA). The following factors shall be considered in determining whether a PIA is required:

1. The project involves new collection, use or disclosure of *personal information* (e.g., collecting information on member's spending habits)
2. The project involves expanding the scope of personal information being collected, used, or disclosed within an existing information system, service, or program (e.g. collecting additional types of personal information to approve OMA membership or membership renewal)
3. The project involves collecting *personal information* about individuals or groups outside of the OMA membership (e.g., the public, physicians outside of Ontario)
4. The project involves shifting from direct to indirect collection of *personal information* (e.g., OMA website begins collecting member online behavior in addition to what members directly input into the online OMA member portal)
5. The project involves linking *personal information* from two or more OMA systems (e.g., linking membership database with OMA Insurance or Physician Health Program database)
6. The project involves developing a new system or enhancing an existing system that contains *personal information* (e.g., using member information within a database for data analytics; significant upgrades to or the adoption of a new web portal for members or a system for an OMA business unit)
7. The project involves significant changes to how employees or contractors can access *personal information* in OMA systems (e.g., enabling remote access to OMA systems; creating a new user role in a database or application)

8. The project involves contracting or outsourcing an OMA activity, program or service that involves *personal information* to another organization (e.g., involving any third party in the collection, use, disclosure, storage or destruction of personal information held by the OMA, hosting a database in the cloud)
9. The project involves transferring an OMA program or service that involves *personal information* to another organization (e.g., transferring all OMA insurance services to third parties)
10. The project involves acquiring a new program that involves *personal information* and therefore, assuming accountability for the new personal information.

If there is a need for a PIA, the business unit/employee shall inform the Privacy Officer, who will conduct the assessment and determine next steps. A PIA checklist shall be made available to employees.

Access and correction

The Privacy Officer will provide an individual with access to his or her PI or PHI that is held by the OMA where lawful and appropriate.

The Privacy Officer will provide an individual with documentation on how the OMA has used or currently uses her or his PI or PHI, and any third parties that the OMA has or continues to disclose this information to. The OMA will be as specific as possible when providing this information.

The Privacy Officer will respond to an individual's request for access to or correction of their PI or PHI within a reasonable time and at minimal or no cost to the individual.

The Privacy Officer will make PI or PHI available to the individual in a form that is understandable to them, e.g., by explaining acronyms, etc.

The OMA will enable members to correct their PI or PHI directly through such means as their member account on the OMA website.

Access and correction requests will be addressed by the Privacy Officer.

Privacy inquiries and complaints

The OMA will accept complaints and inquiries, or any other feedback, regarding the OMA's privacy program and OMA privacy management from any individual or organization.

The Privacy Officer will notify individuals of the existence of relevant complaint procedures once an inquiry or complaint is made.

The Privacy Officer will transfer the management of the privacy complaint to another OMA employee if the complaint pertains to the performance of the Privacy Officer.

The Privacy Officer will address and investigate all privacy inquiries and complaints.

Whistleblowing

An OMA employee will notify the Privacy Officer if she or he believes or has reason to believe that another OMA employee, third party service provider or any other individual has or intends to violate the OMA Privacy Policies or breach OMA security safeguards for PI or PHI.

Meetings with Information Management Staff

Privacy staff shall meet quarterly with Information Management (IM) staff to coordinate on data inventory and retention and disposal matters. Third party risk management shall also be reviewed.

Reporting to Executive and CEO

A privacy report on compliance and breach reporting shall be brought biannually to the Executive Team and included annually in a CEO report to the Board of Directors.

SUPPORTING/REFERENCED DOCUMENTS

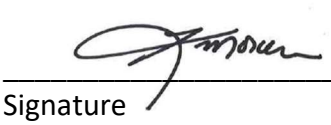
Use Type	Document Title
Referenced	Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA) Personal Health Information Protection Act, 2004 (PHIPA)

RESPONSIBILITIES

Position	Actions
CEO	Approve operating policies and/or procedures.
Process Owner/Author	Include the responsibility information required for the Process/Service Owner of the Policy/Procedure being written.
Knowledge & Records	Review and provide additional metadata as required. Notify Authoring Department when each policy reaches its review date. Maintain original documentation for archiving.
Department Directors	Monitor compliance with this policy by employees. Obtain training for employees, if required.
Employees	Acknowledge as required and comply with policies/procedures.

Author: Jennifer Gold
Process/Service Owner: Privacy Officer

Approved by: Chief Executive Officer



Signature

May 8, 2025
Date