Privacy Policy

Effective Date: June 26, 2018
Review Date: June 26, 2023

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. SCOPE

This policy includes:

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

3. INDIVIDUALS INVOLVED

This policy applies to:

> 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.

4. 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];

Personal Health Information (PHI): The OMA adopts the *Personal Health Information Protection Act, 2004 (PHIPA)* definition of "personal health information" as "identifying information about an individual in oral or recorded form, if the information,

- Relates to the physical or mental health of the individual, including the health history of the individual's family,
- 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,

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

- Is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual,
- Relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
- 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,
- Is the individual's health number, or
- Identifies an individual's substitute decision-maker."[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.

5. POLICY SPECIFIC INFORMATION AND RESPONSIBILITIES

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 and shall, in consultation with relevant staff as required, update it every two years.

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. However, specific OMA business units are subject to the requirements of the *Personal Health Information Protection Act, 2004 (PHIPA)* namely OntarioMD in its role as a service provider and 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 authority of the OMA to collect, use and disclose personal information is through the consent of its members and other individuals from whom the OMA collects, uses and discloses personal information or personal health information.

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

Privacy standards

The OMA's privacy program will be informed by the following standards and best practices:

- Relevant legislation and regulations, primarily *PIPEDA*, and also *PHIPA* where relevant;
- The GDPR, insofar as OMA collects web-based data analytics;
- 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.

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

The OMA will develop and implement programs and information management processes using a privacy-by-design approach intended to prevent, rather than manage and resolve, the occurrence of privacy breaches and unauthorized collections, uses, and disclosures of PI or PHI, or the unauthorized retention or destruction of PI or PHI.

The OMA will have a privacy governance and accountability framework in place, which will include roles and responsibilities for ensuring the protection of privacy within the OMA.

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 OMA business units maintain documented procedures for privacy operations, including consent management, incident handling, access and correction requests, complaints and inquiries, and training and awareness activities;
- Monitor the implementation and operation of the OMA privacy program through reports from privacy leads and business unit managers and maintain a breach log;
- Maintain an OMA privacy risk management framework to ensure that a preventative approach to privacy protection is being followed; and
- Ensure that all OMA employees sign a Confidentiality Agreement with the OMA

The Privacy Officer and Technology staff will complete annual or as-needed assessments 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 through its business units and subsidiaries including the Ontario Medical Foundation and OMA Insurance. Unless otherwise noted, this privacy policy and all of the related privacy policies and procedures (e.g. Privacy Governance and Accountability Policy, Privacy and Security Breach Management Policy and 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.

Where there is a discrepancy or gap between this policy and any other OMA standard or process for the protection or management of PI or PHI, this policy shall 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 or OntarioMD for the Hospital Report Manager), 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 the OMA Privacy and Security Code of Conduct 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 through its policies on managing PI or PHI, privacy notices and access policies and procedures.

The OMA will collect PI or PHI for the purposes of fulfilling OMA programs and activities only. These purposes include:

- Communicating with OMA members;
- Assessing the needs of OMA members;
- Providing products, services and information to members;
- Conducting surveys and polls of members;
- Permitting affiliated and other reputable third-party organizations, subsidiaries and preferred suppliers to provide products, services and information to members;
- Managing OMA relationships with members;
- Meeting any legal or regulatory requirement; and
- Other purposes consistent with the above.

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.

OMA business unit managers will maintain and communicate to members, on behalf of the Privacy Officer, statements of purpose for all holdings of PI or PHI in the custodianship of the OMA.

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, 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;
- How to access the OMA privacy policies, standards and codes of conduct; and
- 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 Officer will maintain copies of previously posted privacy notices.

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;
- 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 obtain consent from individuals for any *new* purposes for the use or disclosure of their PI or PHI.

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 in OMA's *Policy on Retention, Transfer and Disposal of Personal Information and Personal Health Information.*

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.

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. These measures are documented in the OMA's *Privacy and Security Breach Management Policy*, and associated breach management procedures.

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; and
- Evaluate the cause(s) of the incident and conduct remediation activities as required.

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.

The Privacy Officer and the OMA internal auditor will conduct regular reviews of information security safeguards to ensure they are effective and appropriate.

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 less 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.

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 or a privacy lead according to the OMA's *Access* and *Corrections Procedures*.

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 according to the OMA's *Privacy Inquiries and Complaints Procedure*.

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.

6. SUPPORTING/REFERENCED DOCUMENTS AND TEMPLATES

Use Type	*Document Title*
Mandatory	*Procedures for Responding to an Access or Correction Request for Records of PI or PHI*
Mandatory	*Procedures for Responding to Privacy Inquiries and Complaints*
Mandatory	*Privacy Governance and Accountability Policy*
Mandatory	*Procedures for Conducting a Privacy Impact Assessment*
Mandatory	*Privacy and Security Breach Management Policy*
Mandatory	*Procedures for Privacy and Security Breach Management*
Mandatory	*Privacy and Security Training and Awareness Policy*
Mandatory	*Information Safeguards Policy*
Mandatory	*Retention, Transfer and Disposal of PI and PHI Policy*
Mandatory	*Execution of Agreements with Third Party Service Providers Policy*
Mandatory	*Procedures for executing Agreements with Third Party Service Providers*
Optional	*Form A – Access or Correction Procedures Checklist*
Mandatory	*Form B – Access or Correction Intake and Review Form*
Mandatory	*Form C – Access Response Letter*
Mandatory	*Form D – Correction Response Letter*
Optional	*Form E – Privacy and Security Breach Management Procedures Checklist*
Mandatory	*Form F – Privacy Breach Intake, Containment and Notification Form*
Mandatory	*Form G – Privacy Breach Investigation Form*
Mandatory	*Form H – Privacy Breach Notification Letter*
Mandatory	*Form J – Privacy Inquiry or Complaint Intake and Investigation Form*
Mandatory	*Form K – Privacy Inquiry or Complaint Response Letter*
Mandatory	*Form L – Determining Need for a PIA*

Author: Jennifer Gold

Process/Service Owner: Privacy Officer

June 26, 2018

_____ _____

Approved By *Approval Date*