COLLEGE OF OPTOMETRISTS OF ONTARIO

Type:	Informatics and Information Technology		
Name:	Information and Data Management Policy		
Status:		**Version:**	1.0
Date Approved:	September 18, 2024	**Date Revised:**	

Purpose

The College of Optometrists of Ontario (COO) prioritizes the privacy and confidentiality of the personal information it collects for its business objectives. This policy underscores the various aspects of information and data management practices that the COO follows to maintain the confidentiality of the information it collects, uses, and discloses.

Background

Personal information refers to any information that can be used to identify an individual, including but not limited to demographic characteristics, information relating to socioeconomic status, personal views held by an individual, and private correspondence between an individual and an organization. Personal health information refers to any identifying information about one's health or healthcare, including information relating to the physical or mental health of an individual, payments made for healthcare services, and more.

The COO collects personal information and personal health information to fulfill its responsibilities as a regulatory college. Information is collected and used primarily for the core regulatory pillars of quality assurance, registration, managing investigations and handling complaints. However, it may also be collected to perform the college's business objectives, support the responsibilities of the Council, and to meet legal requirements.

The COO's information and data management practices/policies are developed and maintained in accordance with key legislation. The Regulated Health Professions Act (RHPA) establishes standards for the professional conduct of regulatory colleges. Concerning the management of data, Section 36 "Confidentiality" outlines that information obtained while carrying out the responsibilities of the college remains confidential and indicates circumstances for when such information can be communicated to others. Section 36 of the RHPA also authorises regulatory colleges to collect information directly from its members for the purposes of health service research and planning.

The Personal Health Information Protection Act (PHIPA) and the Freedom of Information and Protection of Privacy Act (FIPPA) govern the oversight, use, disclosure, and collection of personal health information and personal information by the COO. Additionally, the COO references the 10 fair

information principles from the Personal Information Protection and Electronic Documents Act (PIPEDA) when developing information policies and practices, to ensure that personal information is managed in a way that protects individuals.

Accountability and Governance

The COO's Manager of Informatics and Information Technology is responsible for maintaining and updating the COO's Information and Data Management Policy, reviewing it on an annual basis to ensure alignment with current standards. Additionally, they are responsible for developing information management practices and handling complaints related to information technology and data security. Where appropriate, inquiries and concerns may be escalated to the Deputy Registrar and the Registrar.

The COO collaborates with a Managed IT Services Vendor that assists with technical investigations and provides IT support to accomplish the business objectives of the COO.

COO staff receive regular data privacy and security training to ensure they are aware of the COO's information and data management standards, as well as the best practices for handling personal information.

Collection, Use, and Disclosure of Information

The COO collects information from its registrants and the public, which include:

- Personal information collected from applicants to fulfill the requirements of the registration process;
- Registrant information (i.e. practice location, services offered, etc.) that is collected during annual renewal;
- From patients or members of the public who file complaints to the COO.

Information that the COO collects is used to accomplish its responsibilities as a regulatory college. The purposes for which the COO uses information includes but is not limited to:

- Monitoring registrant compliance with the COO's quality assurance program;
- Evaluating the progress of registrants undergoing a remediation program;
- Processing annual registration renewal forms and associated payments;
- Evaluating the eligibility of applicants;
- Maintaining and establishing standards of practice;
- Making data-driven operational decisions;
- Meeting auditing requirements;
- Supporting the Council in carrying out its responsibilities;
- Carrying out investigations to resolve complaints filed by patients and members of the public.

The COO discloses information where required to do so by law or for the purposes that the information was collected for. The instances where the COO discloses information include:

- Disclosing information on the success of the quality assurance and investigations programs as part of the College Performance Measurement Framework report.
- Disclosing registrant names, practicing status, practice locations, services offered, and restrictions/disciplinary information on its website.

Data Management:

The COO's framework for information and data management consists of 5 key pillars:

- Maximizing Use: The COO collects the minimal amount of information required to carry out its business objectives and prioritizes reusing information where possible and appropriate.
- Digital Management: Information and data that is collected by the college is handled using digital tools whenever possible.
- Open and Transparent: Where appropriate, information and data are made available publicly to support transparent regulation and foster collaboration.
- Security: Security measures are in place to protect data and information based on risk/sensitivity.
- Accessibility: Accurate and complete information is available in accessible formats to authorized entities.

Information that is collected by the COO is retained in accordance with the COO's Internal Record Retention and Destruction Policy, and securely disposed of when no longer required.

The COO takes reasonable steps to ensure that the information it collects, uses, and discloses is up-to-date and accurate. Members who provide information to the COO are required by law to provide the college with accurate and current information.

Security:

The COO takes reasonable measures to ensure that information collected by the college is protected from unauthorized access, theft, and loss. The COO has logical, physical, and technical safeguards in place to protect information based on its sensitivity and risk. Some examples include:

- Role-based access to information;
- Physical access controls (i.e. Key Fob) to access information kept within the COO office;
- Implementing firewalls to block unauthorized access;
- Encrypting data to protect it at rest and in transit;
- Conducting regular staff training on current data privacy and security practices;
- Ensuring information is only used for the purposes it was intended for and safely disposed/destroyed when it is no longer needed.

In the event of a cybersecurity incident that impacts information and data at the COO, the college has an incidence response plan in place to minimize adverse effects and take steps to prevent similar incidents from occurring in the future.

Individual Rights and Access:

Individuals have the right to access and correct their personal information collected by the COO. The COO can provide individuals with information about how their data is being used and who it is disclosed to.

Instances where individuals may be refused access to their personal information include ongoing investigations and other circumstances outlined in the RHPA.

Consent:

Under the RHPA, the COO has legal authority to collect, use, and disclose personal health information and personal information without individual consent in certain situations. For instance, information may be collected without consent for the purposes of carrying out an investigation on a member.

For circumstances where information is voluntarily provided, the COO will ensure that it obtains consent from the individual whose information is being used.

Openness:

The COO is committed to protecting the personal information and personal health information it uses to carry out its regulatory responsibilities, as described in this policy. The Manager of Informatics and Information Technology and the Registrar are responsible for ensuring that all staff members adhere to the procedures outlined in this policy.

Additionally, the COO is dedicated to enhancing the transparency and accessibility of its information management policies and practices. As part of this effort, the COO has made this policy available on its website and will ensure that other relevant information is published to the COO's website.

Challenges:

Inquiries and complaints regarding the COO's Information and Data Management Policy or information and data management in general should be directed to info@collegeoptom.on.ca.

References:

1. Government of Ontario. (2024, July 1). *Regulated Health Professions Act, 1991*. Ontario.ca. https://www.ontario.ca/laws/statute/91r18#BK86

2. Government of Ontario. (2024, June 28). *Personal Health Information Protection Act, 2004*. Ontario.ca. https://www.ontario.ca/laws/statute/04p03#BK5

3. Government of Ontario. (2023, December 4). *Freedom of Information and Protection of Privacy Act*. Ontario.ca. https://www.ontario.ca/laws/statute/90f31

4. Office of the Privacy Commissioner of Canada, O. of the P. C. of C. (2024, May 1). *Pipeda Fair Information principles*. priv.gc.ca. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/