PRIVACY POLICY

Implemented: Jan 2025
Replaced: N/A
Reviewed: Dec 2025
Review cycle: Two years
Policy number: 2020-011
Policy owner: Operations - Quality, Compliance & Risk

1. Policy Statement

The Australian College of Optometry (ACO) Ltd acknowledges the significance of privacy and is dedicated to safeguarding the personal information it gathers.

The ACO adheres to the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs) outlined in the Privacy Act, as well as the *Privacy and Data Protection Act 2014* (Vic) (PDPA) and other applicable laws governing the handling of personal information by health service providers, including patient health information.

This privacy policy explains the ACO's approach to protecting personal information, individual's rights concerning their personal data, and how this information is collected, stored, used, and shared.

This policy forms part of the ACO Data Governance Policy Framework.

2. Scope

The policy applies to workplaces under the management or control of the ACO:

Employees	Board Members	Researchers	Contractors (including employees of contractors)	Volunteers	Students	Suppliers	Consultants
✓	✓	✓	✓	✓	✓	✓	✓

3. Policy Procedure

Practices and procedures for managing personal information undergo regular review, which may result in updates to this policy from time to time. When updates occur, the revised policy will be made available on the website.

3.1 Types of information collected by the ACO

The kinds of personal information that the ACO collects differs depending on the type of interaction.

3.1.1 Patients

When an individual is a patient of the ACO we may collect:

- Contact information, such as name, address, telephone number and email address.
- Gender, pronouns, date of birth, language spoken and residence type.
- Information on cultural identity

- Emergency contact details.
- GP contact details.
- Information about eligibility for Medicare rebates (including Medicare number), health fund details and/or Department of Veterans Affairs details (as applicable).
- Information about eligibility for state government funding (including concession status).
- Medical history, medical investigations, medical images, treatment and advice given, and other information relevant to care and personal health.
- General feedback about the ACO and the services we provide.

Every time a patient attends the ACO; new information is added to their record. Reception staff will confirm that each patients' details are correct and up to date at every visit. Information we collect about our patients is generally considered 'sensitive information' (specifically, 'health information') within the meaning of the Privacy Act and the PDPA.

3.1.2 Other Individuals

The ACO may also collect personal information about individuals who are not patients, for example those enquiring about services.

Information may also be collected about individuals who are not patients themselves, when making a record about a patient (for example, collecting emergency contact details or collecting a family medical history).

3.1.3 Referring doctors and healthcare professionals

The ACO may also collect personal information about individual health practitioners who interact with our service such as, referring optometrists, ophthalmologists, doctors or other health professionals involved in the care of our patients.

This information could include names, contact details, professional details, credentials, and information regarding interactions or transactions with the ACO. This information is collected for the purpose of administration, management and the effective operation of the ACO's clinical services and to facilitate safe and effective healthcare for our patients.

3.1.4 Prospective employees/applicants

The ACO collects personal information when recruiting employees, such as their name, contact details, qualifications and work history. Generally, this information is collected directly from prospective employees via our HRIS platform ELMO.

We may also collect personal information from third parties in line with usual recruitment practices (for example, from nominated referees). Before offering a position, the ACO may collect additional details including vaccination status, physical assessment for the role, or other information necessary to conduct police checks.

This Privacy Policy does not apply to ACO employee records. Please see the R*ecords & Data Management Procedure*.

3.1.5 Website visitors

The way in which we handle the personal information of visitors to our website is discussed in section '4. Website Privacy'.

3.2 How the ACO collects personal information

The ACO will, where reasonable and practicable to do so, collect information directly from an individual. This may include:

- In person, over the phone, via email
- When completing written history forms or other paperwork.

In some instances, it may be necessary to collect information from another person such as:

- The referring doctor (or their practice staff)
- Other health professionals involved in patient care
- The private health insurer
- Authorised representatives, relatives, next-of-kin or carers.

3.3 Why the ACO collects personal information

The ACO collects personal information for the purpose of providing a safe and effective health service, improving service delivery and conducting research and related services. This information is also used to manage our services, as well as to fulfill reporting obligations related to our funding from the Victorian Government.

Details about how the ACO uses and discloses personal information are provided below.

Providing accurate and complete information is essential to ensure the safety, quality, and effectiveness of the care we deliver. If information is withheld, inaccurate or incomplete, the safety and quality of the services we offer may be compromised. In some cases, if we do not receive accurate and complete information, we may be unable to provide healthcare services. If an individual has any concerns about the personal information we request, they should contact the ACO Privacy Officer, Kylie Harris at aco@aco.org.au.

Individuals are not required to provide identifying information when contacting this service and may opt to use a nickname or alias to maintain privacy. However, anonymity is typically not feasible for patients who are receiving healthcare services.

3.4 How personal information is used and disclosed

Personal information is typically disclosed to third parties only for purposes related to healthcare provision and in ways that would be reasonably expected. Disclosure for other purpose occurs with the individual's consent or when required or authorised by law. Any such disclosure must adhere to existing data security and storage requirements.

Personal information may be shared with health professionals and health service providers involved in the individual's care, such as:

- A referring practitioner
- A general practitioner (GP).

Personal information may also be disclosed during discussions about care with authorised representatives, relatives, next-of-kin or carers where the individual has provided consent. Consent will be noted on the patient record and can be revoked by the individual at any

time. If the individual is unable to give or communicate consent physically or legally, the disclosure is limited to the extent reasonable and necessary for the provision of care or treatment.

Disclosures of health and personal information (as authorised by the *Health Services Act 1988*) may be made for quality and safety purposes. This is restricted to entities responsible for investigating failures in quality and safety or those overseeing health system quality and safety including the relevant state health department, state regulatory bodies, and/or other health service entities. In such circumstances, personal information is used to address any quality and safety issues that may have affected the individual, ensuring continuous service improvement.

Personal information may be used and disclosed to third parties for administration, management, and operation of the ACO, including:

- Administering billing (such as Medicare benefits, health fund benefits, and other third-party payment arrangements) and debt recovery.
- Managing, monitoring, planning, and evaluating services.
- Conducting safety and quality assurance and improvement activities.
- Providing training for staff and healthcare workers.
- Providing clinical placements to optometry students with patient consent.
- Testing and maintaining information technology systems.
- Undertaking risk management.
- Responding to complaints or inquiries regarding health services provided.
- Obtaining advice from consultants and professional advisers.
- Responding to subpoenas and other legal orders and obligations.

3.5 Direct marketing

If you are a patient, the ACO will not use or disclose your personal information for direct marketing without your consent.

If you are a healthcare professional, the ACO may collect and use your personal information to send you information about our services and activities (such as newsletters).

If you do not wish to receive direct marketing communications, please email us at marketing@aco.org.au.

The ACO will never sell, distribute or lease personal information to third parties unless we have an individual's permission.

3.6 Security of personal information

Steps are taken to ensure that personal information is protected from misuse, interference, loss, as well as any unauthorised access, modification, or disclosure. Personal information may be stored electronically or physically.

Storage of electronic information occurs on secured servers or in controlled, access-restricted environments such as password-protected computer systems. Strict policies govern who is authorised to access personal information, and employees are required to maintain the confidentiality of any personal information.

In certain circumstances, personal information may also be held on behalf of the ACO in paper-based or electronic formats by service providers (for example, offsite document storage providers or electronic back-up data storage providers). Agreements with these service providers impose confidentiality and privacy obligations on them consistent with the Privacy Act.

When personal information is no longer required, it is destroyed or de-identified, unless retention is otherwise required or authorised by law. For more information see *Records & Data Management Procedure*.

3.7 Sending personal information overseas

The ACO does not typically or routinely disclose personal information to overseas recipients. Information will only be disclosed overseas if:

1. Written consent has been provided by patient or carer; and
2. The recipient complies with the APPs or an exception under the APPs applies.

Overseas secure cloud-based servers are not used in general by the ACO to hold personal information. Where servers are hosted overseas, this would only be done in compliance with APPs

3.8 Correcting, accessing or updating personal information

Reasonable steps are taken to ensure that collected personal information remains accurate, up to date, and complete. If personal information for a patient (such as a name or address) changes, these can be updated in writing or in person

Individuals have the right to request:

- Access to the personal information held about them.
- Correction of personal information that is incorrect, inaccurate, out of date, incomplete, irrelevant, or misleading.

Access to any personal information can be requested at any time. If an individual is entitled to access the information, suitable arrangements will be made to provide it. There is no charge for making the request itself; however, if a copy of the information is sought, a charge may be applied to cover administrative costs. In limited circumstances, a request for access may be declined in accordance with privacy laws. Requests should be made online via the FOI page on the ACO website.

When it is believed that information held by the ACO should be corrected, a request for correction may be made. Changes to clinical information in a medical record are generally not possible, but a request can be made to include a statement in the record. Requests should be made in writing or in person.

From time to time, verification may be requested to ensure personal information is accurate and up to date. To protect privacy, identity verification is required before granting access or making corrections to personal information.

3.9 Privacy Complaints

If you have questions or concerns about privacy, please contact us using the contact information below.

Email: aco@aco.org.au; Attn: Privacy Officer, Kylie Harris

Post: Attn: Privacy Officer, Kylie Harris
The Australian College of Optometry
374 Cardigan Street, Carlton VIC 3053

If a matter remains unresolved after contacting the ACO, a complaint may be lodged. The complaint will be reviewed to determine whether simple or immediate steps can be taken to resolve it.

If a more detailed assessment is required, acknowledgment of the complaint will be provided within two weeks, and every effort will be made to respond as promptly as possible. In most cases, a response will be issued within 30 days; if complex issues are involved, additional time may be needed.

If the outcome of the complaint is not satisfactory, the matter may be referred to the Office of the Australian Information Commissioner at www.oaic.gov.au or by calling 1300 336 002.

4. ACO Research

4.1 Types and uses of information

The ACO conducts research approved by Human Research Ethics Committees for public interest purposes, through its research arm the National Vision Research Institute. This is done in compliance with the Guidelines of the National Health and Medical Research Council made under section 95A of the Privacy Act and the ACO Research Policy.

The information collected for these research projects is de-identified whenever possible; that is data with any and all potentially identifying information is removed (e.g. a dataset could include vision measurements, age to the closest year, and suburb, but would not include name or Medicare number). Consent is not required under the Privacy Act to collect this de-identified data, and use by ACO Research adheres to the ACO Research Policy as well as guided by ethics approval from a Human Research Ethics Committee operating to NHMRC guidelines. Participant-level, de-identified data is held, and/or destroyed after specified time periods, in accordance with the requirements stipulated by the Ethics approval for that project. Summary statistics (e.g. an average vision measurement across a community) are similarly held.

Some research requires participants to be identified in datasets, requiring a higher level of security. In these cases, participant-level data is securely held and accessible on a limited basis only by those with a need to know within the ACO or collaborators and is destroyed in accordance with the timelines stipulated by the Ethics approval for that project.

Individuals are always able to opt-out of research or choose not to participate where they are invited to do so.

If you have any questions about ACO research, please contact the Privacy Officer using contact information set out at paragraph 3.9 above.

5. Website Privacy

5.1 Types of information collected by the ACO

5.1.1 Contact details

Information is collected as supplied from time to time. The ACO is committed to ensuring the security of payment information. All payment transactions conducted through the ACO website comply with the Payment Card Industry Data Security Standard (PCI DSS) to safeguard financial data. Payment transactions are processed using PCI DSS-compliant payment gateways, and credit card details are not stored. Data is encrypted in transit using industry-standard encryption protocols. Strict access controls are in place to limit access to payment information to authorized personnel only. Systems undergo regular security assessments and updates to maintain PCI DSS compliance.

5.1.3 Click trails and cookies

Paths taken by visitors through the website are recorded, typically linked to their IP address, and may be correlated by computer. In most cases click trail data is not directly individually identifiable. As requests reach the website, servers record click trails, which include, but are not limited to:

- The type of browser you are using
- The date and time of your visit
- Your IP address
- The address of the website that referred you to ours
- The addresses of pages accessed, and any documents downloaded.

Click trails can be correlated over time by use of cookies. A cookie is a small file which is placed on your computer or device when you visit our website. Cookies only identify your device and do not identify you personally.

5.1.4 Activity history

Orders, enquiries, and votes submitted via the website, along with any offline contact (such as phone calls), make up the activity history. This history is recorded whenever an enquiry is submitted, a comment is posted, or a vote is cast, and may also be recorded during offline interactions.

5.1.2 Publishable content

Comments or other content intended for publication on the website are collected when provided by individuals through the website or by other means.

Submitting content for publication (including but not limited to comments, testimonials, votes, or forum posts) grants a transferrable, perpetual right to publish and/or commercially use that content without limitation. By providing such content, it is warranted that the content is owned or created by the submitting party, or that permission has otherwise been obtained to assign publication rights. Publication rights do not extend to fields explicitly marked as private (such as an email address), unless a clear breach of the terms of use has occurred.

Content submitted for publication may be disclosed to all website visitors and/or republished on other websites at the ACO's discretion. If personal information belonging to the submitting party or a third party is included as part of the content, it is warranted that appropriate permission has been secured to publish that information, and the ACO is indemnified against any consequences arising from its publication.

If personal information is discovered on the website without consent, the ACO should be contacted immediately.

5.2 Disclosing information

Personal information may be disclosed to third parties under the following circumstances, and by providing personal information, individuals consent to such disclosures:

- When explicit authorisation is given at the time the information is provided.
- As required or authorised by any applicable law.
- When necessary for credit card payment processing by internet payment gateways or merchant facilities.
- As part of an investigation into an individual's activity on the website (including disclosure to the individual's internet service provider or network administrator).
- If there is reason to believe a breach of the terms of use or other unlawful activity has occurred, and disclosure is reasonably considered necessary (including disclosure to the police, another enforcement body, or the individual's internet service provider or network administrator).
- To lessen or prevent a serious threat to a person's health or safety.
- As part of a sale of all or part of the business.

5.3 Opting in and out

The correlation of passive activity data may be opted out of by disabling cookies in the browser. While most web browsers automatically accept cookies, these settings can generally be modified to decline them if desired. Doing so may affect the functionality of the website, as well as other websites.

When an email address is provided, the option may be offered to receive marketing information by email or other means. An opportunity to opt out of further communications is given each time such information is sent, typically via an "unsubscribe" link located in the footer or header of the email.

If any communication purporting to be associated with this site or its products or services appears to have been sent in a manner inconsistent with this policy, or in breach of any law, the ACO should be contacted immediately on 9349 7400.

5.2 Links to other websites

The ACO website may contain links to other sites. The ACO is not responsible for the privacy practices or content of other sites. Individuals should be aware when they leave the site and read the privacy statements of each website linked on the ACO website.

5.3 Privacy and our website

A copy of this privacy policy is available on the ACO website – www.aco.org.au

The ACO will take all reasonable steps to ensure that any personal information held is not lost, misused, or inadvertently provided to unauthorised third parties, including by means of firewalls, password locking, truncation of credit card data, encryption of data in transit, and secured servers.

It is acknowledged that the security of electronic communications cannot be guaranteed, and information is provided via the internet at one's own risk. Responsibility cannot be accepted for the misuse, loss, or unauthorised access to personal information when security is not fully under the ACO's control. The security and confidentiality of any username or password used to access this website must be maintained by the user, who will be held accountable for all activities occurring under their login credentials (including, but not limited to, publishing illegal or defamatory material, engaging in other unlawful activities, or initiating unauthorised credit card charges).

No responsibility is assumed for the privacy or security practices of third parties, and the collection or use of information by those parties may be subject to separate privacy and security policies. If there is a suspicion of misuse, loss, or unauthorised access to personal information, the ACO should be contacted immediately.

6. Other relevant ACO Policies

Staff, especially managers and supervisors, are encouraged to read this policy in conjunction with other relevant ACO policies, including:

- Code of Conduct and Disciplinary Procedure
- Records and Data Management Procedures
- Research Policy
- Mission, vision, and values statements

7. Legislation and Related Resources

7.1. Legislation

- The Australian Privacy Principles and the *Privacy Act 1988* (Cth)
- *Health Records Act 2001* (Vic)
- *Privacy and Data Protection Act 2014* (Vic)
- *Health Services Act 1988* (Vic)

8. Feedback

Individuals may provide feedback about this document by emailing the ACO Privacy Officer at privacy@aco.org.au