

Croydon Eye Clinic Privacy Policy

Last reviewed 26 September 2026

This policy explains how personal and health information is handled when you contact or receive care at Croydon Eye Clinic (CEC), and how you can access your information or raise a concern. We handle information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Health Records Act 2001 (Vic), the Health Privacy Principles (HPPs) and other applicable laws.

The organisation responsible for information held in CEC's practice records is Nazari Medical Pty Ltd, ABN 90 968 334 224. A treating practitioner may also be responsible for records that they hold separately. The Practice Manager can help identify who holds a particular record and direct your request to that person or organisation.

Information we collect

We collect information needed to arrange and provide eye care and manage the clinic. Depending on your circumstances, this may include your name, date of birth, contact and emergency contact details; Medicare, DVA, health fund and payment details; referrals; medical and eye health history; medicines and allergies; examination findings, tests, scans and clinical photographs; treatment, surgery and follow-up records; correspondence with other healthcare providers; and information about a parent, guardian or authorised representative.

Clinical photographs and images of the eyes or face may form part of your medical record. Facial images can identify a person even if names are removed. We take this into account before using any image for a purpose beyond your care.

How we collect information

We usually collect information from you during booking, registration, consultations, forms, telephone calls and messages. We also receive relevant information from referrers, other treating practitioners, hospitals, pathology and imaging services, Medicare, DVA, insurers, and a parent or representative where appropriate. If information arrives without being requested, we assess whether we may lawfully keep it and otherwise securely destroy or de-identify it where lawful and reasonable.

You may ask a general question without identifying yourself where practicable. For treatment, accurate identification is usually needed for patient safety, continuity of care and claims. If you choose not to provide relevant information, we may be unable to provide some services or make a claim on your behalf. We explain any specific collection and consent choices when they arise.

Why we use information

We use information to assess and treat you, make appointments, coordinate referrals, communicate with you and your care team, maintain a clinical record, prescribe and arrange tests, and manage billing and claims. We also use information where reasonably necessary for clinic administration, quality and safety activities, accreditation, staff training, audit, legal obligations and the handling of enquiries or complaints.

We use or disclose health information for another purpose only with consent or where the law allows it, including a directly related purpose you would reasonably expect. Research, clinical trials, publications, teaching or external quality activities may require separate consent or another lawful basis. Where suitable, we use information that has been de-identified, while recognising that some clinical images may remain identifiable. We seek specific permission before publishing an identifiable patient account or image or using it in promotion.

AI assistance during consultations

With your consent before its use, a third-party AI service may assist the treating clinician to transcribe and summarise a consultation for clinical documentation. You may decline the service; your care can continue without it. The clinician remains responsible for reviewing information used in your record and making clinical decisions. We assess the service's privacy and security arrangements and handle information supplied to it under applicable law. Information about the location of service providers and possible cross-border access is addressed below.

Recording and AI enabled devices in consultations

To protect the privacy of patients, staff and others, patients, visitors and accompanying persons must ask the treating clinician for permission before making an audio or video recording, taking a photograph, livestreaming, or using a device or application to transcribe, capture or process a consultation. This includes mobile phones, smart glasses, wearable cameras and AI transcription tools. Please keep these functions switched off unless permission has been given.

We consider requests case by case, including the privacy of anyone whose voice or image may be captured. Please explain the intended use of a recording before it begins. Permission for a personal recording does not extend to livestreaming, publication, sharing or uploading it to an external AI service; please seek separate permission for any such use. If recording has not been agreed, staff may ask that it stop or that the device be switched off or removed from the consulting room.

If a device is needed for vision, accessibility, communication or another health related reason, please tell us. We will consider reasonable adjustments and alternatives that support your care while protecting the privacy of others.

Who may receive information

Information may be shared, as needed and permitted by law, with your general practitioner, referring optometrist or doctor, specialists, anaesthetists, hospitals, pharmacies, diagnostic services and other providers involved in your care. Relevant information may also go to Medicare, DVA, health funds or insurers for claims; to electronic prescription services and SafeScript where applicable; and to My Health Record when we access or upload a record under the applicable rules.

We may give limited access to providers who support our clinical software, AI documentation, communications, data storage, IT security, accreditation or professional services. They should receive only information needed for their role and be subject to appropriate confidentiality and security requirements. We may also disclose information where law requires or permits it, including to a regulator, a court, or to respond to a serious threat to life, health or safety. Access within the clinic is limited to people whose duties require it.

Direct marketing

Appointment reminders, clinical follow-up and information about your care are service communications. We do not use health information for direct marketing without your consent. If you consent to receive marketing, you can withdraw that consent by contacting us or using an unsubscribe method provided in a message.

Storage, security and retention

Records may be held in paper and electronic systems, including clinical images. We take reasonable steps to protect them from loss, misuse, unauthorised access, alteration and disclosure through appropriate access

restrictions, staff obligations, system controls and secure handling. No electronic method of storage or transmission is completely risk free.

We retain health records for at least the minimum periods required by Victorian law and longer where another legal or clinical obligation applies. When information is no longer required, we take reasonable steps to destroy it securely or de-identify it, subject to legal retention requirements.

If an eligible data breach occurs, we assess it and notify affected people and the Office of the Australian Information Commissioner as soon as practicable where the Notifiable Data Breaches scheme requires it.

Information handled outside Victoria or Australia

Some service providers may store information or provide support from another Australian state or from overseas. Transfers of health information outside Victoria, and disclosures to overseas recipients, are assessed against the HPPs and APPs before they occur. We take steps required by law to protect information handled by a recipient outside Victoria or Australia.

Website and online enquiries

If you use our website, its systems or service providers may collect technical information such as your IP address, browser, device, pages visited and cookies or similar data where used. Such information can be personal information. If you use an online contact form, we collect the details you submit to answer your enquiry. We use website information to operate, secure and improve the site. Please avoid sending sensitive clinical information through a general enquiry form unless we have directed you to a suitable channel.

Accessing or correcting your records

You can ask the Practice Manager for access to personal and health information we hold about you, or ask us to correct information that is inaccurate, incomplete, out of date or misleading. Please tell us what you seek and how you would prefer to receive it. We may ask you to put the request in writing and verify your identity. A person acting for you must provide evidence of their authority. We assess requests under the applicable laws, without making access dependent on a doctor's discretionary approval.

We respond without unreasonable delay and within applicable statutory time limits. For Victorian private health records, the maximum is generally 45 days for access and 30 days for correction. You may request a copy, inspection, a summary or an explanation where the law provides these options. There is no charge for making a request; a fee for providing access may apply within the limits set by Victorian law. We will explain any fee before providing access.

Access may be limited or refused only on grounds permitted or required by law. We will give reasons where required and consider an alternative way to provide access where appropriate. If a correction is declined, we will explain the decision and any available option to have your statement associated with the record. We consider requests involving children or another person's records according to capacity, authority and privacy law.

Questions and complaints

Contact the Practice Manager if you want to access or correct information, identify the record holder, ask a question or make a privacy complaint. Please describe the issue and provide a way to contact you. We will acknowledge and investigate a complaint and explain our response. There is no charge to make a complaint.

Practice Manager, Croydon Eye Clinic
77 Hewish Road, Croydon VIC 3136

Telephone: (03) 9723 1055

Email: info@croydoneye.com.au

If you are dissatisfied with our response, you may contact the Office of the Australian Information Commissioner (oaic.gov.au) or, for a complaint about health information handled in Victoria, the Victorian Health Complaints Commissioner (hcc.vic.gov.au).

Changes to this policy

We review this policy when our practices or legal obligations change. The current version will be available from the clinic and, when published, on our website.