



DR. ANTHONY BARKER

EXPERTISE. EXPERIENCE. EXCEPTIONAL CARE.

PRIVACY POLICY

Dr. Anthony Barker

Specialist Plastic & Reconstructive Surgery

1. Introduction and Purpose

Dr. Anthony Barker (referred to in this policy as 'we', 'us', or 'our') is a specialist plastic and reconstructive surgery practice. We are committed to protecting the privacy and dignity of every patient and to handling all personal and health information in a responsible, lawful, and compassionate manner.

This Privacy Policy explains how we collect, use, disclose, store, and protect your personal and health information, including sensitive clinical images taken as part of your surgical care. It also explains your rights regarding that information and how you may make a complaint if you have a privacy concern.

We comply with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the My Health Records Act 2012 (Cth), relevant state and territory health privacy legislation, and the advertising and professional standards set by the Australian Health Practitioner Regulation Agency (AHPRA). From 10 December 2026, we will also comply with the updated Privacy Act provisions on automated decision-making.

This Policy will be updated from time to time to reflect changes in our practice, technology, or the law. The current version will always be available at reception and on our website.

2. About Our Practice

We are a specialist plastic and reconstructive surgery practice operating in [City/State]. Our services include, but are not limited to:

- Reconstructive surgery following trauma, cancer, or congenital conditions
- Cosmetic surgical and non-surgical procedures
- Skin cancer excision and reconstruction
- NEED TO CONFIRM WITH ELESIA

All services are provided in-house by our surgical team, clinical staff, and administrative personnel. We do not use external third-party reception or administration providers.

3. Collection of Personal and Health Information

3.1 What We Collect

We collect personal and health information that is necessary for providing you with safe, high-quality surgical care. This may include:

- Personal identifiers: full name, date of birth, address, phone number, and email address
- Medicare number, private health insurance details, and pension or concession card information
- Emergency contact and next-of-kin details
- Comprehensive medical history, current medications, allergies, and anaesthetic history
- Referral letters and correspondence from your general practitioner and other treating specialists
- Surgical consent documentation
- Pre-operative, intra-operative, and post-operative clinical notes and records
- Pathology results, imaging reports, and diagnostic investigations
- Clinical photographs and video recordings taken for medical documentation purposes (see Section 5)
- Billing, payment, and health fund claim information
- Correspondence relating to complaints, feedback, or legal matters

3.2 How We Collect Information

We collect your information:

- Directly from you at the time of enquiry, during your consultation, and throughout your care
 - From your referring general practitioner or other treating healthcare providers
 - From hospitals, day surgery facilities, or anaesthetists involved in your care
 - From diagnostic and pathology services
 - Via our website, patient intake forms, and pre-operative questionnaires
-

3.3 Consent to Collection

When you first attend our practice, we will ask you to provide information and confirm your consent to its collection and use. By attending and receiving care from us, you consent to the collection of the information described in this Policy for the purpose of your healthcare.

For certain purposes — including clinical photography, research participation, or use in educational materials — we will seek your express written consent separately, as described in the relevant sections of this Policy.

4. Use and Disclosure of Personal and Health Information

4.1 Permitted Uses

We use your personal and health information for the following purposes:

- Providing surgical assessment, treatment, and post-operative care
- Communicating with you about your appointments, care, and results
- Corresponding with your referring practitioner, GP, and other members of your treating team
- Processing health fund claims and billing
- Meeting legal, regulatory, and professional obligations
- Practice accreditation, quality improvement, and internal auditing activities

4.2 Disclosure to Third Parties

We will not disclose your information to persons outside your care team without your consent, except as required or permitted by law. We may disclose your information to:

- Your referring general practitioner and other treating specialists, as part of coordinated care
- Hospitals, day surgery facilities, and anaesthetists involved in your procedures
- Pathology laboratories, radiology providers, and other diagnostic services
- Health funds and Medicare Australia for billing and rebate purposes
- Our medical indemnity insurer, where necessary
- Regulatory bodies (such as AHPRA) or law enforcement, where required by law
- Courts or tribunals, in response to a lawful order

We will not sell, rent, or trade your personal or health information to any third party. We will not disclose your information to family members or friends without your prior written authority.

4.3 Overseas Disclosure

We do not routinely disclose patient information to overseas recipients. If overseas disclosure is ever required (for example, to facilitate care while you are travelling), we will seek your prior consent and ensure appropriate safeguards are in place in accordance with APP 8.

5. Clinical Photographs and Visual Records

In specialist plastic surgery, clinical photographs are a critical part of surgical planning, documentation, and post-operative assessment. We treat all clinical images with the same care and confidentiality as any other health record.

5.1 Why We Take Clinical Images

Clinical photographs may be taken for the following purposes:

- Pre-operative assessment and surgical planning
- Intra-operative documentation
- Post-operative monitoring and review of outcomes
- Medicolegal documentation and clinical record-keeping
- Internal quality review and clinical audit (de-identified where practicable)
- Patient education — to assist you in understanding your planned procedure or expected outcome

5.2 Consent for Clinical Photography

Separate written consent is required before any clinical photographs are taken. Your consent form will specify:

- The purpose for which the photographs are being taken
- Where and how the images will be stored
- Who may view the images
- Whether the images may be used for any purpose beyond your direct clinical care (e.g. education or marketing)
- Your right to withdraw consent at any time

You have the right to decline photography. Declining will not affect the quality of care you receive, and your surgeon will discuss alternative documentation methods with you.

Consent for photography does not imply consent for any secondary use. If we wish to use your images for education, research, or marketing purposes, we will seek your explicit, separate written consent for that specific purpose.

5.3 Storage and Security of Clinical Images

All clinical photographs and visual records are stored securely as part of your medical record. The following standards apply:

- Images are stored within our secure, encrypted practice management or clinical imaging system — not on personal devices, personal cloud storage accounts, or unsecured shared drives
- Access to clinical images is restricted to treating clinical staff only — on a strict need-to-know basis
- Images are not stored, shared, or transmitted via personal mobile phones, personal email accounts, or social media platforms under any circumstances
- Where images must be transmitted (for example, to a hospital or specialist), they will be sent via secure, encrypted channels only
- Images are retained in accordance with the minimum legal retention periods applicable in your state or territory (generally seven years for adults, and until age 25 for patients who were minors at the time of treatment)
- Upon expiry of the required retention period, images will be destroyed securely in a manner that prevents reconstruction or identification

5.4 Use of Images for Marketing or Promotional Purposes

Important — Marketing Use Requires Separate Express Consent

We will never use your clinical photographs, videos, or before-and-after images for any marketing, advertising, website, or social media purpose without your separate, explicit, written consent. This consent is entirely voluntary, may be refused without consequence, and may be withdrawn at any time by written notice to the Practice Manager. Any withdrawal of consent will be honoured promptly and the relevant images removed from use. In accordance with AHPRA advertising guidelines, testimonials and before-and-after images used in advertising must comply with applicable professional standards.

5.5 Images Taken by Patients

Patients are welcome to take photographs of their own results for personal records. However, patients must not photograph other patients, staff, or any part of the clinical environment without explicit permission. Photographs of staff or of clinical procedures — including surgical procedures — require prior written approval from the Practice Manager and the individual concerned.

6. Sensitive and Confidential Information

All health information is classified as sensitive information under the Privacy Act 1988 (Cth) and is afforded the highest level of protection. In a plastic and reconstructive surgery practice, this includes information relating to:

- The nature and reason for surgical procedures (including cosmetic surgery, reconstruction after cancer, trauma, or conditions that may be of a deeply personal nature)
- Mental health history, where relevant to surgical assessment or anaesthetic risk
- Body image, weight, and appearance-related matters discussed during consultations
- Sexual or reproductive health history, where relevant to clinical assessment

We recognise that many patients attend our practice for procedures that are highly personal. All staff are trained to handle enquiries and records with the utmost discretion. Patient identity, attendance, and the nature of any procedure will not be disclosed to any party without consent — including family members, unless the patient has provided written authorisation.

Caller Enquiries

If a third party contacts our practice enquiring about whether a person is, or has been, a patient, we will not confirm or deny this. We will advise the caller that our practice operates under a strict confidentiality policy and that no patient information can be disclosed. This applies regardless of the caller's relationship to the patient.

7. Anonymity and Pseudonymity

Under APP 2, individuals have the right to interact with us anonymously or under a pseudonym where practicable. However, given the nature of surgical care, the requirements of Medicare and health fund billing, and our professional obligations for clinical documentation, it is generally not practicable for us to treat patients anonymously or under a pseudonym.

If you wish to discuss this option, please raise it with us prior to your appointment and we will give your request genuine consideration.

8. Data Security and Retention

8.1 How We Protect Your Information

We implement robust technical and administrative measures to protect your personal and health information from misuse, interference, loss, and unauthorised access. These measures include:

- Secure, encrypted electronic medical record and practice management systems with role-based access controls
 - Unique individual login credentials for all staff — never shared
-

-
- Password management systems and multi-factor authentication where available
 - Regular staff training on privacy, cybersecurity, and confidentiality obligations
 - Physical security measures for clinical records and paper files
 - Secure disposal of all paper records and electronic media containing patient information
 - Regular review and updating of IT security systems and policies

8.2 Retention of Records

Your health records — including clinical notes, correspondence, consent forms, and clinical images — will be retained in accordance with applicable legal and professional requirements. As a general guide:

- Adult patient records: minimum seven years from the date of last entry
- Records relating to patients who were minors: retained until the patient reaches age 25, or for seven years from the date of last entry, whichever is longer
- Records subject to ongoing legal or insurance matters: retained until the matter is fully resolved

When records are no longer required to be retained, they will be destroyed securely and in a manner that protects your privacy.

9. Research, Education, and Quality Improvement

9.1 Quality Improvement and Audit

We may use de-identified patient information for internal clinical audits, accreditation processes, and quality improvement activities. Where practicable, information is de-identified before use. These activities help us maintain and improve the quality and safety of our surgical care.

9.2 Research

If our practice participates in research projects — including clinical trials or academic research — we will only use your identifiable information with your express written consent. Research involving patient data requires appropriate ethics approval in accordance with the National Statement on Ethical Conduct in Human Research.

You will never be approached directly by external researchers without your prior consent, and you may decline to participate in any research without it affecting your care.

9.3 Education and Training

Clinical cases, surgical techniques, and outcomes may be discussed in an educational context — for example, at professional conferences, in journal publications, or in teaching settings. Where identifiable information is included, your express written consent will be obtained beforehand. De-identified information may be used without consent, provided you cannot be identified.

9.4 Marketing

We will not use your personal information for direct marketing without your express consent. If you provide consent, you may withdraw it at any time by contacting us in writing or using the opt-out mechanism provided in any marketing communication.

All marketing materials produced by this practice, including website content and social media, comply with AHPRA advertising guidelines and the relevant provisions of the Health Practitioner Regulation National Law.

10. Use of Technology and Artificial Intelligence

Our practice uses clinical and administrative technology — including practice management software, electronic health record systems, telehealth platforms, and clinical imaging systems — to support the delivery of surgical care.

Where AI-enabled tools are used in any clinical or administrative context, the following principles apply:

- Patient information will not be used to train or develop AI models without express patient consent
- All outputs generated by AI tools are subject to clinical review and oversight by a qualified practitioner — no clinical decision will be made solely by an automated system
- AI tools used in our practice are selected and governed in accordance with the Australian Privacy Principles and relevant ethical standards

Following amendments to the Privacy Act 1988 (Cth) effective 10 December 2026, we will ensure our documentation and practices reflect obligations regarding automated decision-making that affects individual rights.

11. Access to and Correction of Your Information

You have the right to request access to the personal and health information we hold about you, and to request correction of any information that is inaccurate, incomplete, or out of date.

To make a request, please contact our Privacy Officer in writing using the contact details in Section 13. We will respond within 30 days. In some limited circumstances, access may be declined — for example, where access would pose a serious risk to your health or the health of another person. Where access is declined, we will provide written reasons and advise you of your review options.

A reasonable administrative fee may apply to cover the cost of retrieving, copying, or preparing records. You will not be charged for making the request itself.

Requesting a Copy of Your Records

Requests for copies of medical records, including clinical images, should be made in writing to the Practice Manager. Please allow adequate time for the request to be processed, particularly for imaging files. We can provide records in electronic or paper format as appropriate.

12. Data Breach Response

In the event of an actual or suspected data breach involving your personal or health information, we will take immediate steps to contain the breach and assess its impact. Under the Notifiable Data Breaches (NDB) scheme established by the Privacy Act 1988 (Cth), we are required to notify you and the Office of the Australian Information Commissioner (OAIC) if a breach is likely to result in serious harm.

All data breach incidents — regardless of scale — will be recorded in our internal Data Breach Register and assessed by the Privacy Officer. If notification is required, we will contact you promptly with information about what occurred and what steps we are taking to protect your information.

13. Privacy Enquiries and Complaints

We take all privacy concerns seriously. If you have a question about how your information has been handled, or you wish to make a formal privacy complaint, please contact our Privacy Officer in the first instance. We will acknowledge your complaint within five business days and aim to resolve it within 30 days. Please email admin@dranthonybarker.com

If you are not satisfied with our response, you may escalate your complaint to the Office of the Australian Information Commissioner (OAIC):

- Website: www.oaic.gov.au
- Phone: 1300 363 992
- Post: GPO Box 5218, Sydney NSW 2001

For complaints relating to the professional conduct of a registered health practitioner, you may also contact AHPRA:

- Website: www.ahpra.gov.au
 - Phone: 1300 419 495
-