

PORT MEDICAL AESTHETICS CLINIC

and Kempsey Medical Aesthetics Clinic

PRIVACY POLICY

Port Medical Aesthetics Clinic and Kempsey Medical Aesthetics Clinic

Document Code	PMAC-POL-PR-001
Version	1.0
Effective Date	1 July 2026
Applies To	All personal information collected by PMAC and KMAC — patients, website users, staff, and contractors
Review Date	Annually or following any legislative change
Approved By	Dr Kristy Kostalas, Medical Director
Privacy Officer	Kristie Arnold, Practice Manager
Note	This policy satisfies obligations under the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and the Privacy and Health Records legislation applicable in NSW. It applies to the main clinic website (portmedicaaesthetics.com.au), the PMAC online shop (shop.portmedicaaesthetics.com.au), Dapple CRM, Heidi AI clinical documentation, and all in-clinic data collection processes.

1. OUR COMMITMENT

Port Medical Aesthetics Clinic (PMAC) and Kempsey Medical Aesthetics Clinic (KMAC) are committed to protecting the privacy and confidentiality of all personal information we collect. We recognise that the information you share with us — particularly your health information — is sensitive, and we treat it with the care and discretion it deserves. This Privacy Policy explains what information we collect, why we collect it, how we use and store it, who we may share it with, and how you can access, correct, or raise concerns about your information. PMAC operates in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Health Records and Information Privacy Act 2002 (NSW), and the My Health Records Act 2012 (Cth) where applicable.

2. WHO THIS POLICY APPLIES TO

This policy applies to:

- Patients and prospective patients of PMAC and KMAC
- Users of the PMAC website (portmedicaaesthetics.com.au)
- Users of the PMAC online shop (shop.portmedicaaesthetics.com.au)
- Subscribers to the PMAC email list
- PMAC and KMAC staff, contractors, and treating practitioners

It applies to all personal information collected in person at our clinics, through our online platforms, and through any communication channel including phone, email, and SMS.

3. WHAT INFORMATION WE COLLECT

Type of Information	Examples	How Collected
Identity and contact information	Name, date of birth, address, phone number, email address	Consultation forms, online booking (Timely), Dapple CRM patient portal, website contact form, email list signup
Health information	Medical history, current medications, allergies, contraindications, treatment notes, adverse events, diagnoses relevant to treatment planning	Consultation forms, Heidi AI clinical documentation, verbal history during consultations
Treatment records	Procedure details, products used (including batch numbers), injection sites, depth settings, clinical findings, follow-up notes	Heidi AI at time of treatment; recorded by treating practitioner
Photographs and images	Pre- and post-treatment photographs, progress images, consented marketing images	In-clinic photography with signed consent; separately consented for clinical use and/or marketing
Financial and payment information	Payment method type, billing address, transaction records	Timely, EFTPOS terminal, online shop checkout — PMAC does not store full card numbers
Online and website data	IP address, browser type, pages visited, time on site, referring site	Automatically via website analytics (Cloud Concepts platform); online shop (Shopify)
Email marketing data	Email address, name, engagement data (opens, clicks)	Email list signup on website; confirmed opt-in only
Employment information (staff)	Name, contact details, qualifications, employment records, training records	Provided directly by staff during onboarding

PMAC collects only the information that is reasonably necessary for the purposes described in this policy. We do not collect personal information we do not need.

Sensitive Information

Health information is classified as sensitive information under the Privacy Act. We collect health information only with your consent and only for the purpose of providing you with safe, effective cosmetic medical treatment. You are not required to provide health information, but if you choose not to, we may be unable to treat you safely.

Anonymity and Pseudonymity

Where possible and lawful, you may deal with PMAC anonymously or by pseudonym — for example, when making a general website enquiry. However, we are unable to provide clinical treatment without verifying your identity and collecting relevant health information.

4. WHY WE COLLECT YOUR INFORMATION — PURPOSES OF COLLECTION

Primary Purposes

- Providing safe cosmetic medical treatment, including clinical assessment, consultation, treatment planning, and follow-up
- Maintaining accurate and complete clinical records as required by law and professional standards
- Obtaining and recording your informed consent before treatment
- Communicating with you about your appointments, treatment, and aftercare
- Processing payments for treatments and retail products

- Dispensing prescription products where applicable
- Mandatory reporting to regulatory bodies — including adverse event reporting to the TGA and mandatory notifications to AHPRA

Secondary Purposes

- Sending you clinic updates, skincare information, and promotional content — only if you have opted in to email marketing
- Improving our services and treatment protocols through de-identified clinical data review
- Managing complaints and feedback
- Staff training and clinical governance
- Legal, insurance, and indemnity purposes where required

Photography

Clinical photographs are taken for treatment planning and outcome assessment. Photographs are only used for marketing, social media, or educational purposes with your separate, specific written consent. You may consent to clinical photography without consenting to marketing use. Withdrawal of marketing consent does not affect your clinical care.

5. HOW WE STORE AND PROTECT YOUR INFORMATION

Clinical Records

Clinical records — including treatment notes, consent forms, and photographs — are stored securely in Heidi AI (clinical documentation) and Dapple CRM (patient portal and consent management). Both platforms are selected for their Australian data standards and compliance with the Privacy Act.

Physical Records

Any physical documents are stored in locked filing at the clinic. Access is restricted to authorised clinical and administrative staff.

Access Controls

Access to patient records is restricted on a need-to-know basis. Clinical records are accessible only to treating practitioners and authorised administrative staff. All staff are trained in their privacy obligations and bound by confidentiality.

Security Measures

- Password-protected systems with role-based access controls
- Encrypted data transmission where applicable
- Physical security at both clinic locations
- Staff training in privacy obligations
- Incident response procedures for data breaches

Data Breach Response

If a data breach occurs that is likely to result in serious harm, PMAC will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as required under the Notifiable Data Breaches scheme (Part IIIC of the Privacy Act 1988). Notification will occur as soon as practicable.

6. HOW LONG WE KEEP YOUR INFORMATION

Record Type	Minimum Retention Period
Adult patient clinical records (including treatment notes and photographs)	7 years from date of last entry
Child patient clinical records	Until the patient turns 25, or 7 years from last entry — whichever is longer
Consent forms	7 years from date of signing (or as per clinical record above)
Complaint records	7 years from date of closure

Record Type	Minimum Retention Period
Adverse event records	7 years from date of event
Financial and billing records	7 years (Australian Taxation Office requirement)
Staff records	7 years from end of employment
Email marketing records (opt-in evidence)	Duration of subscription plus 3 years
Website analytics data (non-identifiable)	As per Cloud Concepts platform standard — typically 26 months rolling

When information is no longer required and the retention period has passed, it is securely destroyed or de-identified in accordance with our records management procedures.

7. WHO WE MAY SHARE YOUR INFORMATION WITH

PMAC does not sell, rent, or trade your personal information. We share information only in the circumstances described below.

Platform / Third Party	Purpose	Data Shared
Dapple CRM	Patient portal, consent forms, aftercare delivery, CRM communications	Name, contact details, treatment history, consent records
Heidi AI	Clinical documentation and treatment note generation	Health information — clinical use only. Heidi AI processes data under its own privacy framework; PMAC selects Heidi AI for its Australian data handling standards.
Timely	Appointment booking, scheduling, retail sales recording	Name, contact details, appointment history, retail purchases
Cloud Concepts Australia	Website hosting and management for portmedicaaesthetics.com.au	Website visitor data (non-identifiable analytics)
Shopify (via shop.portmedicaaesthetics.com.au)	Online retail — skincare products	Name, delivery address, email, payment method (processed by Shopify's payment gateway)
Merz Aesthetics Australia	Product adverse event reporting where required by TGA or manufacturer	Minimum identifiable information required for regulatory reporting only
TGA (Therapeutic Goods Administration)	Mandatory adverse event reporting for therapeutic goods	Minimum required for regulatory compliance
AHPRA / HCCC / regulatory bodies	Regulatory investigations and complaints	Information relevant to the complaint or investigation only — disclosed when legally required
Medical indemnity insurer	Insurance, medico-legal, and complaint management	Relevant clinical and patient information when required for a specific matter
Pathology and referral providers	Clinical care — when referrals or investigations are ordered by PMAC doctors	Clinical information relevant to the referral
Compounding pharmacies	Dispensing PMAC Renew prescription skincare	Prescription information, patient name — minimum required

Overseas Disclosure

Where any platform or service provider processes data outside Australia (including cloud services), PMAC takes reasonable steps to ensure that overseas recipients handle information in accordance with the Australian Privacy Principles. PMAC will not send health records overseas without your consent except where legally required.

Disclosure Required by Law

PMAC may be required to disclose information without your consent where required or authorised by Australian law — for example, mandatory reporting obligations, court orders, or regulatory investigations. We will not disclose more information than is legally required.

8. PHOTOGRAPHY AND MARKETING USE OF IMAGES

Clinical photographs taken at PMAC are used for treatment planning and outcome review. They are stored securely in your patient record.

PMAC may request your separate consent to use photographs for marketing, social media, educational presentations, or other promotional purposes. This consent is:

- Always separate from your clinical photography consent
- Entirely voluntary — declining does not affect your clinical care
- Revocable at any time by contacting the Practice Manager in writing

Images used for marketing will not identify you without your specific consent. If you have consented to identifiable marketing use and later withdraw that consent, PMAC will remove images from future use. Images already published cannot be retrospectively removed from all platforms but will not be used again after withdrawal.

PMAC complies with AHPRA's advertising guidelines for before-and-after images, including requirements for balanced representation of outcomes and prohibition on misleading depictions of results.

9. WEBSITE AND ONLINE SHOP

Website Analytics

The PMAC website (portmedicaaesthetics.com.au) automatically collects non-identifiable usage data including IP address, browser type, pages visited, and referring site. This data is used to improve the website and is not linked to individual identities. It is managed by Cloud Concepts Australia under their privacy framework.

Online Shop

The PMAC online shop (shop.portmedicaaesthetics.com.au) is hosted on Shopify. When you make a purchase, your name, delivery address, email, and payment information are collected and processed by Shopify in accordance with their privacy policy. PMAC retains purchase records for financial and customer service purposes. PMAC does not store your full payment card details.

Cookies

The PMAC website may use cookies to improve your browsing experience. You may disable cookies in your browser settings, though this may affect the functionality of some website features. The PMAC website does not use cookies for targeted advertising.

Email Marketing

PMAC sends email updates, skincare information, and promotional content to subscribers who have opted in via the website email list signup. You may unsubscribe at any time using the link in any email or by contacting us directly. PMAC does not share your email address with third parties for marketing purposes.

10. DAPPLE CRM AND PATIENT PORTAL

PMAC uses Dapple CRM as its patient relationship management platform. Dapple CRM is used to store consent forms, send aftercare instructions, and manage patient communications. When you create a Dapple CRM patient portal account, your information is stored and managed in accordance with Dapple's privacy framework.

PMAC selects its clinical software platforms on the basis of their data security standards and compliance with Australian privacy law. Where Dapple CRM processes data, it does so as a data processor on behalf of PMAC. PMAC remains responsible for the personal information it holds.

11. HEIDI AI — CLINICAL DOCUMENTATION

PMAC uses Heidi AI to assist with clinical documentation and treatment note generation. Heidi AI processes health information entered by treating practitioners to produce clinical notes. PMAC uses Heidi AI on the basis of its Australian data handling standards and its compliance with health information privacy requirements.

Health information processed through Heidi AI is used solely for clinical documentation purposes. It is not used for training Heidi AI's models without PMAC's explicit consent. Patients may ask their treating practitioner about how their consultation is documented.

12. YOUR RIGHTS

Access

You have the right to request access to the personal information PMAC holds about you. Requests must be made in writing to the Privacy Officer. PMAC will respond within 30 days. In most cases, access is provided free of charge. Where access requires significant time or resources, PMAC may charge a reasonable fee — this will be communicated to you before any fee is incurred.

Correction

If you believe information PMAC holds about you is inaccurate, out of date, incomplete, or misleading, you may request a correction. PMAC will correct the information promptly or, if we disagree that a correction is warranted, we will note your request alongside the record.

Complaints

If you have a concern about how PMAC has handled your personal information, you may:

- Contact PMAC's Privacy Officer (Practice Manager Kristie Arnold) — see Section 14
- Lodge a complaint with the Office of the Australian Information Commissioner (OAIC): www.oaic.gov.au | 1300 363 992
- Lodge a complaint with the NSW Information and Privacy Commission: www.ipc.nsw.gov.au | 1800 472 679

PMAC will acknowledge privacy complaints within 5 business days and endeavour to resolve them within 30 days.

Withdrawal of Consent

Where PMAC processes your information on the basis of your consent — for example, email marketing or marketing photography — you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing that occurred before withdrawal. Withdrawal of consent for clinical purposes may affect our ability to treat you safely.

Opt-Out of Marketing

You may opt out of email marketing at any time by using the unsubscribe link in any email or by contacting us directly. Opting out of marketing does not affect your clinical records or treatment.

13. SPECIAL CIRCUMSTANCES

Children

PMAC does not provide cosmetic injectable treatments (botulinum toxin or dermal fillers) to patients under 18 years of age in accordance with AHPRA guidelines and the Therapeutic Goods Administration regulations. Where a patient under 18 attends for other services, a parent or legal guardian must provide consent. Records relating to minors are retained in accordance with Section 6.

Deceased Patients

The privacy of deceased patients is protected under applicable law. PMAC will consider requests for access to deceased patient records from authorised representatives on a case-by-case basis, having regard to the sensitivity of the information and the interests of all parties.

Research and Quality Improvement

Where PMAC participates in clinical research or quality improvement activities, patient data is de-identified before use unless you have provided specific consent for identifiable research use. Any research conducted by or involving PMAC staff complies with the National Statement on Ethical Conduct in Human Research and applicable HREC requirements. See the PMAC BoNT-A Patient Knowledge Study (iRECS10578, UNSW HREC) as an example of ethically approved research conducted in accordance with these requirements.

14. CONTACT US — PRIVACY ENQUIRIES

Privacy Officer	Kristie Arnold — Practice Manager
Clinic	Port Medical Aesthetics Clinic
Address	5/12 Highfields Circuit, Port Macquarie NSW 2444
Phone	0421 253 025
Email	reception@portmedicaesthesia.com.au
Medical Director	Dr Kristy Kostalas (escalation for clinical privacy matters)
Response timeframe	PMAC will acknowledge privacy enquiries within 5 business days

15. CHANGES TO THIS POLICY

PMAC reviews this Privacy Policy annually or following any significant legislative change, data breach, or change in our systems and platforms. Updated versions will be published on the PMAC website and made available in clinic. The effective date of each version is noted on the cover of this document. Continued use of PMAC's services following an update constitutes acceptance of the revised policy.

16. REGULATORY FRAMEWORK — REFERENCE

- Privacy Act 1988 (Cth) — including the Australian Privacy Principles (Schedule 1)
- Health Records and Information Privacy Act 2002 (NSW)
- My Health Records Act 2012 (Cth)
- Notifiable Data Breaches scheme — Part IIIC, Privacy Act 1988
- AHPRA Guidelines for Registered Health Practitioners Who Perform Non-Surgical Cosmetic Procedures (2 September 2025)
- Therapeutic Goods Act 1989 (Cth) — adverse event reporting
- Spam Act 2003 (Cth) — email marketing obligations
- Office of the Australian Information Commissioner (OAIC): www.oaic.gov.au
- NSW Information and Privacy Commission: www.ipc.nsw.gov.au

17. RELATED PMAC DOCUMENTS

- PMAC Internal Complaints Management Policy (PMAC-POL-CG-001)
- PMAC Consent and Photography SOP (PMAC-SOP-CG-003)
- PMAC Adverse Event SOP (PMAC-SOP-CG-001)
- PMAC Advertising Compliance SOP (PMAC-SOP-CG-005)
- PMAC Safety and Quality Framework (PMAC-FW-SQ-001)