# Privacy and Confidentiality Policy

## 1. Policy Title

Privacy and Confidentiality Policy

## 2. Purpose

This policy sets out how [Practice Name] collects, uses, stores, and discloses personal and health information to safeguard patient privacy and confidentiality. It aligns with criterion F9 – Confidentiality and privacy of health and other information of the RACGP Standards for general practices (6th edition), and the enhanced digital health and cybersecurity expectations of criterion F8.

## 3. Scope

This policy applies to all staff, contractors, students, and visitors who may access patient information at [Practice Name].

## 4. Definitions

- Personal information: Information or an opinion about an identified or reasonably identifiable individual.
- Health information: Personal information about a person's physical, mental, or psychological health.
- Sensitive information: A subset of personal information including health, racial or ethnic origin, political opinion, sexual orientation, and gender identity.
- De-identified information: Information from which identifying details have been removed and cannot reasonably be re-identified.
- Permitted health situation: A situation under the Privacy Act in which health information may be collected, used, or disclosed without consent.

## 5. Principles

- Collect only the information necessary for providing care and meeting legal obligations.
- Use and disclose health information primarily for the primary purpose of care, or with consent, or under a permitted health situation.
- Protect information with strong digital and physical security controls.

- Respect patients' rights to access and correct their information.
- Capture and store demographic data accurately and confidentially, in line with the Patient Demographics Policy.

## 6. Collection and Use

- Collect health information directly from the patient wherever possible.
- Inform patients of the purpose of collection at or before the time of collection (collection notice).
- Use health information for the primary purpose of providing care, or a directly related secondary purpose, or with the patient's consent.

## 7. Consent

- Obtain consent for use or disclosure of information for purposes beyond direct care (e.g., marketing, research).
- Record consent in the patient's electronic health record.
- Respect a patient's right to withdraw consent, subject to legal requirements.

## 8. Disclosure to Third Parties

- Disclose information to other treating clinicians for direct care without consent where a permitted health situation applies.
- Disclose to My Health Record in accordance with the patient's choices and the My Health Records Act.
- Disclose to police, courts, or public health authorities only where authorised or required by law.
- Use secure, encrypted transmission for any disclosure of health information.

## 9. Access and Correction

- Patients may request access to their health information.
- Provide access within a reasonable timeframe (commonly 30 days) and at no or minimal cost.
- Allow patients to request correction of inaccurate information; document the outcome.

## 10. Data Security and Digital Health

- Health records are held in a secure, accredited clinical information system with role-based access.
- Unique user credentials and multi-factor authentication are required for all systems containing health information.
- Audit logs are retained and reviewed for unusual access.
- Cybersecurity controls align with the IT Security Policies and Procedures and the 6th edition's strengthened cybersecurity expectations (criterion F8).
- Data breaches are managed under the Data Breach Response Procedure and the Notifiable Data Breaches scheme.

## 11. Roles and Responsibilities

**Privacy Officer (Practice Manager):**

- Maintains this policy and handles privacy complaints and access requests.
- Coordinates breach response and OAIC notification where required.

**All staff:**

- Access only the information needed to perform their role.
- Do not discuss patients outside the practice or in public areas.
- Report suspected privacy or data breaches immediately.

## 12. Monitoring, Audit, and Review

- Quarterly review of access audit logs and any privacy complaints.
- Annual review of this policy, breach response procedures, and access controls.

## 13. Documentation and Record Keeping

The practice maintains:

- Records of patient consents.
- Access and correction requests and their outcomes.
- Privacy complaints and resolutions.
- Data breach reports and OAIC notifications.
- Audit logs of system access.

## 14. References


- The Royal Australian College of General Practitioners. Standards for general practices (6th edition). East Melbourne, Vic: RACGP; published 26 August 2026. Available at: https://www.racgp.org.au/running-a-practice/practice-standards/standards-6th-edition
- Privacy Act 1988 (Cth) and the Australian Privacy Principles. Available at: https://www.oaic.gov.au
- Office of the Australian Information Commissioner. Notifiable Data Breaches scheme. Available at: https://www.oaic.gov.au
- My Health Records Act 2012 (Cth).


---

## Version Control

**Policy title:** Privacy and Confidentiality Policy

**Version:** 2.1

**Effective date:** 27 August 2026

**Next review date:** 27 August 2027

**Policy owner:** Privacy Officer / Practice Manager

**Aligned to:** RACGP Standards for general practices (6th edition, published August 2026)