

Digital Health Records Policy

1. Policy Title

Digital Health Records Policy

2. Purpose

This policy describes how [Practice Name] creates, stores, secures, and manages digital health records. It implements the digital-first health records requirements of the RACGP Standards for general practices (6th edition): criterion CG1 – Clinical information systems, under which paper-only clinical records are no longer acceptable, and criterion CG3 – Facilitating complete patient health records, which requires clinical information to be recorded in codable fields.

3. Scope

This policy applies to all clinical and administrative staff and to all systems used to create, store, transmit, or back up patient health information.

4. Definitions

- Electronic health record (EHR): The digital record of a patient's health information held in the practice's clinical information system.
- Clinical information system (CIS): The software used to record, manage, and share clinical information.
- SNOMED CT-AU: The Australian version of the Systematized Nomenclature of Medicine Clinical Terms — the national clinical terminology used to code clinical data.
- My Health Record: The national digital health record system operated by the Australian Digital Health Agency.
- Secure messaging: Encrypted, standards-based transmission of clinical correspondence between systems.

5. Principles

- Clinical records are digital-first; paper-only clinical records are not acceptable.

- Clinical data is recorded in codable fields using a nationally recognised clinical terminology (SNOMED CT-AU) to support safety, decision support, and quality improvement (criterion CG3).
- Records are accurate, complete, current, attributable, and secure.
- Records support continuity of care, including through My Health Record and secure messaging.
- Records are backed up, recoverable, and retained for the period required by law.

6. The Clinical Record

- All clinical encounters, assessments, plans, results, and communications are recorded in the CIS at the time of care.
- Each entry is attributable to the author with date and time.
- Clinical entries use SNOMED CT-AU coded diagnoses, problems, medications, allergies, and procedures where a code exists.
- Corrections are made by amendment that preserves the original entry; data is not deleted in a way that hides the history.

7. Coding and Data Quality

- Diagnoses, problems, medications, allergies, immunisations, and procedures are coded with SNOMED CT-AU.
- Past medical history, allergies, and medicines are reconciled at registration and at transitions of care (see Medication Management policy).
- Data quality (completeness of smoking, alcohol, weight, BP, allergy status) is monitored as part of PIP-QI and quality improvement.

8. My Health Record

- The practice is registered for and uses My Health Record in accordance with the My Health Records Act.
- Patients are informed about My Health Record, including their choices about what is uploaded.
- Where the practice uploads shared health summaries, event summaries, or specialist letters, the GP verifies the content before upload.
- Staff are trained in the appropriate use of My Health Record, including handling records with restricted access.

9. Secure Messaging and Sharing

- Clinical correspondence (referrals, results, letters) is transmitted via secure messaging where possible.
- Fax and unencrypted email are used only where secure messaging is not available and only with appropriate safeguards.
- Sharing of records with other treating clinicians follows the Privacy and Confidentiality policy.

10. Security, Backups, and Business Continuity

- Digital records are protected under the IT Security Policies and Procedures, including MFA, encryption, audit logging, and role-based access.
- Backups are automated, encrypted, offsite, and tested for restorability at least quarterly.
- Business continuity arrangements ensure access to critical records during a system outage.

11. Records Retention and Disposal

- Records are retained for the period required by state/territory law and the practice's record retention schedule.
- Disposal of records at end of life follows a documented process with appropriate authorisation.

12. Roles and Responsibilities

Practice Manager / IT Security Officer:

- Maintain the CIS, coding configuration, backups, and access controls.

Clinicians:

- Record clinical encounters promptly and accurately using coded entries.
- Reconcile histories, allergies, and medicines at transitions of care.

Practice nurses:

- Record clinical activity using coded entries and support data quality improvement.

13. Monitoring, Audit, and Review

- Quarterly audit of data quality (coding rates for key data sets).
- Quarterly test of backup restorability.
- Annual review of this policy, retention schedule, and My Health Record usage.

14. Documentation and Record Keeping

The practice maintains:

- Records of CIS configuration, coding version, and updates.
- Backup and recovery test reports.
- Records retention and disposal schedule and disposal authorisations.
- My Health Record usage and training records.

15. 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>
- Australian Digital Health Agency. Available at: <https://www.digitalhealth.gov.au>
- My Health Records Act 2012 (Cth).
- Australian Digital Health Agency. SNOMED CT-AU. Available at: <https://www.digitalhealth.gov.au/healthcare-providers/initiatives-and-programs/national-clinical-terminology>

Version Control

Policy title: Digital Health Records Policy

Version: 2.1

Effective date: 27 August 2026

Next review date: 27 August 2027

Policy owner: Practice Manager / IT Security Officer

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