MANAGEMENT OF PATIENT HEALTH INFORMATION POLICY

This policy applies to all practice team members, contractors, students, registrars and other persons who have access to practice or patient information.

1. Purpose

The Practice is committed to protecting the privacy, confidentiality, security, accuracy and integrity of patient health information.

This policy outlines how patient and practice information is collected, recorded, accessed, used, disclosed, stored, transferred, retained and securely destroyed.

The policy supports the requirements of the RACGP Standards for general practices – 5th edition, particularly Core Standard 6: Information management, as well as applicable privacy and health records legislation.

2. Scope

This policy applies to information held by the Practice, including:

- patient health records;
- pathology and imaging results;
- correspondence and referrals;
- medication and prescribing information;
- information received from other healthcare providers;
- demographic and contact information;
- Medicare and other administrative information;
- billing and account information; and
- other information that may identify a patient.

It applies to information in electronic, paper or other formats. The Practice is predominantly an electronic-record practice. Any temporary paper patient information must be appropriately secured and incorporated into the electronic patient record and then confidentially destroyed.

3. Legislative and Professional Requirements

The practice manages patient information in accordance with applicable requirements, including:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles;
- Health Records and Information Privacy Act 2002 (NSW);
- applicable NSW health privacy requirements;
- RACGP Standards for general practices – 5th edition;
- relevant professional and ethical obligations; and
- other legislation or legal requirements applying to the Practice.

Where legislation or professional requirements change, this policy and related procedures will be reviewed and updated.

4. Confidentiality and Privacy

Patient information is confidential and must only be accessed, used or disclosed for an authorised purpose. Patient information must not be disclosed to:

- family members;
- friends;
- other patients;
- practice staff who do not require the information for their role; or
- external persons or organisations

unless the patient has provided appropriate authority or the disclosure is otherwise permitted or required by law.

The same confidentiality requirements apply when a member of staff is also a patient of the practice. Unauthorised access, use or disclosure of patient information may result in disciplinary action and, where appropriate, legal or regulatory action.

5. Staff Confidentiality and Training

All staff and other persons with access to patient information must:

- sign a confidentiality agreement on commencement;
- complete privacy and confidentiality training as part of induction;
- receive refresher training as required;
- understand their responsibilities for protecting patient information;
- only access information required for their role; and
- report suspected privacy or information security incidents promptly.

Staff must not access patient records out of curiosity or for any unauthorised purpose.

Staff must not access their own records, or those of family, friends or colleagues, unless this is specifically authorised and appropriate to their role.

Students, registrars, contractors and visiting personnel must comply with the same confidentiality requirements.

6. Patient Identification – RACGP C6.1

The Practice uses at least three patient identifiers to confirm patient identity.

The Practice's primary identifiers are:

1. Full name
2. Date of birth
3. Address

Patient identification is undertaken when:

- registering a new patient;
- booking or confirming an appointment where appropriate;
- the patient presents for an appointment;
- information is provided over the telephone;
- a patient sees a different healthcare provider;
- information is transferred or handed over;
- providing telehealth services; and
- releasing or transferring information where identity must be confirmed.

A Medicare number is not used as one of the Practice's three patient identifiers.

Patients may request anonymity or use of a pseudonym where this is lawful and reasonably practicable. This may not be possible where identification is required for clinical, Medicare, legal or other legitimate purposes.

7. Patient Health Records – RACGP C6.2

The Practice uses Best Practice as its primary clinical information system.

Patient records must be:

- accurate;
- complete;
- current;
- legible;
- factual and professional;
- recorded in a timely manner; and
- maintained in accordance with applicable legislation and professional standards.

Information relevant to patient care must be recorded in the patient's health record, including information received from external healthcare providers where appropriate.

Clinical records must not be inappropriately altered or deleted.

Where a correction is required, the original information must remain identifiable and the correction or additional information must be appropriately documented.

Staff who identify an error or discrepancy in a patient record must refer the matter to the appropriate healthcare provider or Practice Manager.

Staff receive training in the use of Best Practice as part of induction and when significant system changes occur.

8. Use and Disclosure of Patient Information

Patient information may be collected, used and disclosed where this is:

- necessary for providing healthcare;
- directly related to the purpose for which the information was collected and reasonably expected by the patient;
- authorised by the patient;
- required or authorised by law; or
- otherwise permitted under applicable privacy legislation.

Information may be shared between members of the patient's healthcare team where this is appropriate for the patient's care and permitted by privacy legislation. Patient consent is not necessarily required for every transfer of information between healthcare providers where the disclosure is part of the patient's healthcare and is otherwise permitted by law. Where consent is required, appropriate consent must be obtained and documented.

Information must not be disclosed simply because a person claims to be a family member, friend or carer. Where a patient wishes another person to be involved in their care or receive information, the patient's authority should be documented. This can be achieved by completing and signing a ‘Permission for Nominated Representative to access Medical File’ form.

Requests from police, courts, insurers, solicitors, government agencies or other third parties must be referred to the Practice Manager and/or appropriate GP before information is released, unless the authority to disclose is clear and established.

9. Research, Quality Improvement and Use of Patient Data

The practice recognises that patient information may be used for legitimate quality improvement, clinical audit, education and research activities, if privacy, confidentiality and applicable consent and ethical requirements are maintained.

9.1 Quality Improvement and Clinical Audit

Patient information may be used for practice quality improvement and clinical audit activities where permitted by applicable privacy requirements and the patient has been appropriately informed.
The practice's patient registration form includes information about the use of patient data for quality improvement activities and captures the patient's consent where required.

Quality improvement activities may include:

- reviewing clinical care and outcomes;
- monitoring practice performance;
- clinical audits;
- accreditation activities;
- identifying opportunities to improve patient safety and quality of care; and
- evaluating practice programs and services.

Patient information used for quality improvement should be limited to the information reasonably necessary for the activity. Where practicable, information should be de-identified or aggregated.

9.2 Research

Research involving practice patients or patient information must be undertaken in accordance with the practice's Research Policy.

Where patient participation or the use or disclosure of identifiable patient information requires consent, appropriate informed consent must be obtained before participation or disclosure occurs.

Patients must be provided with sufficient information to understand, where applicable:

- the purpose of the research;
- what participation involves;
- what information will be collected or used;
- who the information may be shared with;
- how the information will be stored and protected;
- whether participation is voluntary;
- that declining participation will not affect their access to healthcare; and
- any other information required by the relevant research or ethics requirements.

Patient consent for research participation or sharing of identifiable patient information must be documented in accordance with the Research Policy.

Where research involves external organisations or researchers, information must only be provided where appropriate authority, consent, ethics approval and/or another lawful basis for disclosure exists.

Research and quality improvement activities must not compromise the confidentiality of patients or the quality of their care.

The practice's Research Policy provides further detail about the approval, consent, ethical and information-sharing requirements for research activities.

10. Sharing Information Within the Practice

Access to patient information is based on the staff member's role and responsibilities. Staff must only access the information necessary to perform their duties. Clinical staff may access information required for patient care. Administrative staff may access information required to perform their administrative responsibilities.

Staff must not:

- browse records without a legitimate reason;
- access records of family or friends without appropriate authority;
- share passwords;
- use another person's login;
- leave patient information visible to unauthorised persons; or
- disclose information to other staff who do not have a legitimate need to know.

11. Access to Patient Records – RACGP C6.3

Patients may request access to their health information in accordance with applicable privacy legislation. Requests for access should:

- be directed to the Practice;
- be appropriately documented;
- include verification of the patient's identity;
- include appropriate authority where the request is made by a legal representative or another person; and
- be managed within the applicable legal timeframe.

Access may be limited where an applicable legal exemption applies.

Where appropriate, patients may be provided with information in a suitable electronic or printed format.

Further information is included in the practice's 'Request to Access Personal Information Policy'.

12. Correction of Information

Patients may request correction of information held about them where they believe it is inaccurate, incomplete, out of date or misleading. Requests for correction will be considered and managed in accordance with applicable privacy legislation.

Clinical information must not be removed simply because a patient disagrees with it. Where appropriate, the patient's concerns or additional information should be documented in the record.

13. Transfer of Patient Information – RACGP C6.3

Patient information must be transferred using secure and appropriate methods. Where electronic transfer is available, the practice uses approved secure messaging systems for communication with healthcare providers.

Staff must not send patient health information through:

- personal email accounts;
- personal messaging applications;
- social media; or
- other unsecured communication methods.

Where another method of transfer is necessary, staff must use an appropriately secure method and comply with applicable privacy requirements.

Before releasing records, staff must confirm:

- the identity of the recipient;
- the authority for release;
- the information being requested; and
- that the information is being sent to the correct destination.

The Practice maintains appropriate secure messaging arrangements and keeps relevant healthcare provider contact details and endpoints current where practicable.

14. Physical Security of Information – RACGP C4.2 and C6.4

Patient and confidential information must be protected from unauthorised viewing or access.

The Practice ensures that:

- computer screens are positioned so patients and visitors cannot readily view confidential information;
- privacy screens are used where appropriate;
- computer screens are locked when unattended;
- confidential paperwork is not left in public or patient-accessible areas;
- patient information awaiting collection or courier transfer (e.g. pathology samples) are kept secure;
- confidential information is not placed in general waste; and
- confidential documents are securely destroyed when no longer required.

Reception and clinical areas must be managed to protect the privacy of conversations and patient information.

15. Electronic Information Security – RACGP C6.4

The Practice takes reasonable steps to protect electronic patient information from:

- unauthorised access;
- loss;
- misuse;
- alteration;
- accidental disclosure;
- malware and viruses;
- cyberattack; and
- other security threats.

Security measures include, where applicable:

- individual user accounts;
- password protection;
- role-based access;
- password-protected screen locking;
- antivirus and security software;
- firewall protection;
- secure networks;
- system updates;
- secure messaging; and
- appropriate encryption and security controls.

Passwords must be kept confidential and must not be shared.

Staff must lock or log out of systems when leaving a computer unattended.

16. Access Management, Backup and Information Recovery

The Practice's Business Continuity and Information Recovery Plan sets out the Practice's arrangements for:

- authorised user access and access levels;
- management of user accounts, passwords and system permissions;
- access to information during normal operations and periods of system disruption;
- backup of practice information;
- restoration and recovery of practice information;
- business continuity arrangements in the event of an IT system failure, cyber incident or other disruption; and
- restoration of access to patient and practice information following an outage.

Access to patient information is restricted according to staff roles and responsibilities. Staff are only permitted to access information required for their role.

The Business Continuity and Information Recovery Plan is maintained separately from this policy and reviewed regularly to ensure it remains current and effective.

17. Mobile and Portable Devices

Where mobile phones, tablets, laptops or other portable devices are used to access practice information, appropriate security measures must be applied.

Devices must:

- be password or passcode protected;
- have appropriate security controls enabled;
- be kept secure when not in use;
- not be shared with unauthorised persons; and
- be reported immediately if lost or stolen.

Practice information must not be stored on personal devices unless specifically authorised and appropriately secured.

18. IT Provider and System Security

The Practice's external IT provider assists with maintaining the security and reliability of practice information systems.

IT arrangements include appropriate measures for:

- network and firewall security;
- antivirus and malware protection;
- system updates and maintenance;
- user access and permissions;
- secure remote access;
- system monitoring;
- cyber security;
- data protection; and
- technical support and recovery.

The practice's IT provider is expected to maintain appropriate confidentiality and security arrangements when accessing practice systems or information.
The Practice Manager liaises with the IT provider regarding significant information security risks, incidents, system failures and recovery requirements.

Detailed backup, restoration and recovery arrangements are documented in the Business Continuity and Information Recovery Plan.

19. Health Identifiers and My Health Record

Where relevant to patient care, authorised users may use Individual Healthcare Identifiers (IHIs), My Health Record and other approved digital health systems, with patient consent.

These systems are accessed and used only for authorised purposes and in accordance with applicable legislation, system requirements and practice procedures.

Staff must ensure that patient identity is confirmed before accessing or uploading information to a patient's digital health record.

Further information is included in the practice’s My Health Record Policy.

20. Business Continuity

The practice maintains a Business Continuity and Information Recovery Plan to support continued operation and access to information during:

- computer or clinical software failure;
- internet or network outage;
- power failure;
- cyber security incident;
- loss of access to practice systems;
- equipment failure; or
- other events that may disrupt normal Practice operations.

The plan sets out responsibilities, communication arrangements, access management, backup and recovery processes and alternative arrangements for maintaining patient care.

Staff are made aware of the Business Continuity and Information Recovery Plan and receive relevant training or information as required.

The plan is reviewed regularly and following significant incidents or changes to practice systems.

21. Privacy and Data Breaches

All staff must immediately report suspected or actual:

- unauthorised access to patient information;
- accidental disclosure;
- loss or theft of patient information;
- incorrect transmission of information;
- cyber security incidents;
- phishing or suspected malware; or
- other privacy or information security incidents

to the Practice Manager and/or Practice Principal.

The practice will assess and manage information security and privacy breaches in accordance with applicable legislation.

Where required, affected individuals and relevant regulatory authorities will be notified.

22. Storage, Retention and Disposal – RACGP C6.4

Patient health information must be retained for the period required by applicable legislation.
For private health service providers in NSW, patient health information is generally retained for:

- at least 7 years from the last occasion on which a health service was provided; or
- where the patient was under 18 when the health information was collected, until the patient reaches 25 years of age, whichever is later.

Records must not be destroyed while they are required for ongoing patient care, legal proceedings, investigations, audits, complaints or other legitimate purposes.

Inactive patient records may be retained within the Practice's electronic system or securely archived as appropriate.

23. Secure Destruction

When information is no longer required and may lawfully be destroyed, it must be disposed of securely.
Depending on the format, this may include:

- secure electronic deletion by the Practice's IT provider;
- secure shredding of paper records;

- use of a secure document destruction service; or
- other approved destruction methods that prevent reconstruction or unauthorised access.

Patient information must never be placed in general waste or recycling.

24. Patient Information About Privacy

Patients are informed about the practice's management of their personal information through the practice's Privacy Policy.

The Privacy Policy explains:

- what information the Practice collects;
- why information is collected;
- how information is used and disclosed;
- how information is protected;
- how patients can access and request correction of their information;
- how privacy concerns and complaints can be raised; and
- other relevant privacy rights and responsibilities.

The Privacy Policy is available to patients through the practice and/or practice website.

25. Privacy Complaints

Patients may raise concerns or complaints about the handling of their personal or health information.

Privacy complaints will be:

- treated seriously;
- handled respectfully and confidentially;
- investigated where appropriate;
- responded to within a reasonable timeframe; and
- managed in accordance with the practice's complaints procedure and applicable privacy legislation.

Patients will not be disadvantaged for making a genuine privacy complaint.

26. Responsibilities

Practice Principal

The Practice Principal is responsible for overall clinical and professional oversight of information management and privacy.

Practice Manager

The Practice Manager is responsible for:

- implementing this policy;
- ensuring staff receive appropriate training;
- maintaining appropriate access arrangements;
- coordinating with the IT provider;
- managing privacy and information security incidents;
- monitoring compliance;
- ensuring policies and procedures remain current; and
- ensuring the Business Continuity and Information Recovery Plan is maintained and reviewed.

All Practice Team Members

All staff and other persons with access to Practice information are responsible for:

- maintaining confidentiality;
- protecting patient information;
- following Practice policies and procedures;
- only accessing information required for their role;

- using approved systems and communication methods;
- keeping passwords and login details secure;
- reporting errors, suspected breaches and security incidents promptly; and
- completing required training.

27. Monitoring and Review

The Practice monitors its information management and security arrangements through:

- staff training and education;
- review of privacy and security incidents;
- review of access arrangements;
- review of system and IT security requirements;
- review of relevant legislation and RACGP requirements; and
- regular policy review.

This policy will be reviewed at least every two years, or earlier where there are significant changes to legislation, RACGP Standards, technology, practice systems or identified risks.

28. Related Policies and Documents

This policy should be read in conjunction with:

- Privacy Policy
- Business Continuity and Information Recovery Plan
- Research Policy
- My Health Record Policy
- Request to Access Personal Information Policy
- Clinical Reminders, Results and Recall Policy
- Incident, Near Miss and Adverse Outcome Reporting Policy
- Complaints & Feeback Policy
- Relevant IT/security procedures

Current as of:	3/09/2026	**Version:**	1.0
Amendments			
Date of amendment:	**Version:**	**Details of amendment:**	
9/09/2026	1.0	Original Policy	