Privacy Policy

Policy Category	Information & Privacy
Manual Reference	Section 7
Applies To	All staff, independent contractors General Practitioners, allied health providers, contractors and workplace participants across all practice locations
Related Standards	RACGP 5th Edition – Information Management RACGP 6th Edition - Information Governance & Digital Health
Document Owner	Practice Manager
Approved By	Practice Manager / Principal GP
Effective Date	19/10/2026
Review Date	19/10/2027
Version	1.1

1. Purpose

This policy outlines how Village Medical collects, uses, stores and protects patient personal and health information.

The practice is committed to maintaining the privacy, confidentiality and security of patient information in accordance with:

- Applicable privacy legislation
- Professional standards
- RACGP standards for General Practices

2. Scope

This policy applies to:

- All practice staff
- All general practitioners (including contractors)
- All individuals who access patient information
- All practice sites operated by Village Medical

3. Principles of Privacy

Village Medical manages patient information in accordance with the following principles:

- Patient information is collected only where necessary for care and practice operations
- Information is used only for legitimate clinical or administrative purposes
- Access is restricted to authorised personnel
- Information is stored securely
- Patient confidentiality is maintained at all times

4. Collection of Information

The practice collects personal and health information necessary to provide healthcare services.

This may include:

- Personal identification details
- Medical history and clinical information
- Contact information
- Billing and Medicare details

Information is collected:

- Directly from patients where possible
- From other healthcare providers with patient consent
- Through clinical interactions and consultations

Where practicable, the practice explains why information is collected, who may receive it, whether collection is required or authorised by law, and how patients can seek access, correction or make a privacy complaint. Collection notices and the patient-facing privacy statement should be checked against actual practice workflows.

5. Use and Disclosure of Information

Patient information is used to:

- Provide clinical care
- Support communication between healthcare providers
- Manage administrative and billing processes

Information may be disclosed:

- To other healthcare providers involved in patient care
- Where required by law
- With patient consent

All disclosures are managed in accordance with privacy obligations.

Patients are informed about the usual purposes of collection and disclosure, including electronic communications and care coordination. Consent for clinical care, My Health Record participation or upload, and Medicare bulk-billing assignment of benefits are separate processes governed by the relevant policies. HotDoc SMS and Tyro in-person consent relate to Medicare billing, not blanket consent to disclose health information.

6. Access to Patient Information

Access to patient information is restricted to authorised individuals.

This includes:

- Treating clinicians
- Relevant practice staff
- Authorised administrative personnel

All staff and contractors are expected to access only the information necessary to perform their role.

Role-based access is defined in the Information Access and Confidentiality Policy. Reception uses PracSoft and must not access clinical notes, diagnoses, medications or pathology results in MedicalDirector. Clinical information requests are referred to authorised clinical or records administration staff.

7. Storage and Security of Information

Village Medical maintains systems to ensure patient information is stored securely.

This includes:

- Secure electronic clinical systems
- Password-protected access
- Controlled user permissions
- Secure handling of any physical records (where applicable)

Patient records are retained in accordance with relevant legislative requirements.

Information security is supported by practice policies relating to information and cyber security.

Paper information is secured until scanned or appropriately disposed of under the Management of Health Information Policy. Access is removed promptly when staff leave or no longer need it; backups, access monitoring and security incidents are managed under the practice information security procedures.

8. Electronic Systems and Digital Records

The practice uses electronic clinical systems (e.g. Medical Director, Pracsoft) to manage patient information.

Electronic records support:

- Continuity of care

- Accurate documentation
- Secure storage of information

Access to systems is controlled and monitored.

MedVault is the practice-approved secure method for sending patient records, referrals, results and other personal health information externally where authorised. Results must be approved by the GP before release. Staff must verify recipient details and follow the practice secure communication procedure. Ordinary email and fax workflows must comply with the Internet, Email and Computer Use Policy.

MedicalDirector Clinical is used by authorised GPs and nurses for clinical records and My Health Record access. Reception staff use PracSoft for authorised administrative functions and do not have MedicalDirector Clinical or My Health Record access. Other approved roles have only the permissions needed for their duties.

9. Use of Digital and AI-Supported Tools

Where digital tools (including AI-supported documentation tools such as Heidi AI) are used:

- Clinicians remain responsible for the accuracy of the clinical record
- Patient confidentiality must be maintained
- Information must be handled in accordance with this policy

The final clinical record remains the responsibility of the treating practitioner.

AI-assisted clinical documentation, including Heidi AI where approved for use, must be used in accordance with practice-approved settings, patient information and applicable consent requirements. Clinicians review and correct drafts before entering them into the clinical record; unapproved AI tools must not receive identifiable patient information.

10. Patient Rights

Patients have the right to:

- Request access to their health information
- Request correction of inaccurate information
- Be informed about how their information is used

Requests are managed in accordance with practice procedures.

Privacy enquiries, concerns or complaints can be directed to the Practice Manager.

Requests for access or correction, including complaints, are directed to the Practice Manager or authorised records administration staff, verified appropriately, recorded and managed within applicable privacy-law timeframes. The practice will provide information about how to complain to the Office of the Australian Information Commissioner (OAIC) if the patient is dissatisfied with the practice response.

11. Confidentiality

All staff and contractors must:

- Maintain confidentiality of patient information
- Not disclose information without appropriate authority
- Ensure conversations cannot be overheard where possible

Confidentiality obligations apply at all times, including outside the practice environment.

12. Multi-Site Considerations

Village Medical operates across multiple sites.

To ensure consistent privacy practices:

- All sites follow the same privacy policy
- Patient information is managed through shared systems
- Access controls are applied consistently across locations

Shared clinical information must only be accessed where required for legitimate work at the relevant site. Staff must not access their own, relatives', colleagues' or other patients' records out of curiosity.

13. Breaches of Privacy

Any suspected or actual breach of privacy must be:

- Reported to the Practice Manager
- Reviewed in accordance with incident management processes
- Managed appropriately to minimise risk

Where required, appropriate notifications will be made in accordance with legal requirements.

The Practice Manager coordinates containment, documentation, risk assessment and escalation of suspected breaches, including assessment of whether the Notifiable Data Breaches scheme or My Health Record-specific notification requirements apply. The practice must not assume every incident is notifiable; each incident is assessed under applicable law.

14. Staff Responsibilities

All staff and contractors are responsible for:

- Understanding this policy
- Complying with privacy requirements
- Protecting patient information
- Reporting concerns or breaches

Staff and contractors are supported to understand and comply with privacy obligations through practice processes and training.

Privacy and confidentiality training is provided at induction and refreshed at least annually, with attendance or completion recorded. Staff must follow the practice procedure for requests to access or transfer records and refer these to the authorised records administration role.

Failure to comply with this policy may result in disciplinary action.

The practice maintains an accessible patient-facing privacy statement explaining the types of information collected, how it is held, typical uses and disclosures, access and correction pathways, complaint handling, and whether overseas disclosure is likely. Any overseas processing or disclosure through third-party systems must be verified with the provider before the statement is approved.

15.1 Privacy Statement and Patient Information

Practice-approved external service providers, including booking, billing, secure messaging and clinical documentation services, may handle information only for authorised purposes and subject to applicable privacy, security and contractual requirements. The Practice Manager maintains oversight of relevant service-provider arrangements.

15.2 Third-Party Systems and Service Providers

The Practice Manager reviews this policy at least annually and following material privacy incidents, changes in legislation, technology or practice workflow. Identified improvements are recorded and assigned for follow-up.

15.3 Review and Monitoring

16. Related Policies

This policy should be read in conjunction with:

- Information security policy
- Cyber security policy
- Communication policy