CORP Skye Medical

Printed: 22/08/2025
Created: 18/08/2025
Last Revised: 19/08/2025
Next Review Date: 18/08/2026

PRINTED COPIES ARE NOT CONTROLLED

Policy

Privacy & Information Security Policy

Privacy & Information Security Policy

1. Purpose

This policy describes how Skye Medical protects the privacy, confidentiality, and security of patient health information. It ensures our compliance with the **Privacy Act 1988**, **Australian Privacy Principles (APPs)**, and the **RACGP Standards for General Practices (5th edition, C6.3 & C6.4)**.

2. Scope

This policy applies to:

- All staff, contractors, students, and locums working at our practice.
- All patient health information, whether electronic, paper-based, or verbal.
- All communication platforms, including email, secure messaging, telehealth, and staff personal devices used for work-related communication.

3. Policy Statements

3.1 Privacy & Confidentiality

- We collect, store, use, and disclose patient health information only when necessary for safe and appropriate care, and in accordance with the APPs.
- Patients can access or request corrections to their health information, and we provide this in a secure and timely manner.
- We do not disclose health information to third parties without informed consent, unless legally required.
- All staff sign confidentiality agreements that are stored in their HR file.

3.2 Security of Records

- We secure all patient records so they are not accessible to unauthorised persons.

- Prescription pads, referral pads, and official documents are kept in locked or restricted-access areas.
- We retain and destroy records according to legal and RACGP requirements.

3.3 Information Security

- We appoint a designated IT/Security Officer who oversees information security and liaises with external IT providers - this person is the Clinical Services Manager.
- Each staff member uses a unique login with role-based access appropriate to their responsibilities.
- We use strong passwords, automatic screen locks, and up-to-date antivirus and firewall protection.
- We back up information regularly, store backups securely offsite, and test them to ensure data recovery is possible.

3.4 Mobile & Personal Devices

- We do not store patient health information on personal staff devices.
- Staff may use personal mobiles for internal operational communication (e.g. rosters, shift swaps), but not for sharing identifiable patient information.
- We prohibit screenshots, forwarding, or storing patient information in personal apps (e.g. WhatsApp, Messenger, SMS).
- We use approved secure messaging systems for clinical communication.

3.5 Electronic Communication (Email, Secure Messaging, Telehealth)

- We use email to communicate with patients only when they have provided informed consent, and we explain the risks of unencrypted communication.
- We use secure messaging as our preferred method of transferring clinical information.
- We verify recipient details before sending patient information electronically.
- We use auto-responses on patient-facing email accounts to advise patients of response times.
- We do not make audio or video recordings of consultations without documented patient consent.

3.6 Information Sharing & Transfers

- We transfer patient health information only in response to valid and authorised requests.
- We use secure transfer methods such as secure messaging, encrypted email, or My Health Record.
- We document each transfer in the patient file, including the method, recipient, and date.

3.7 Data Breach & Incident Management

- Staff report suspected or actual data breaches immediately to the Practice Manager.
- We investigate all breaches promptly, take steps to contain them, and assess whether they must be reported under the Notifiable Data Breach Scheme.

- If required, we notify affected patients and the Office of the Australian Information Commissioner (OAIC).

3.8 Physical & Environmental Security

- We protect our facilities from unauthorised access through locked doors, restricted staff-only areas, and secure storage.
- We position computer screens to prevent patient information being viewed by the public.
- We securely wipe or destroy hardware, photocopiers, and data storage devices before disposal.
- We use secure document disposal services for paper records containing sensitive information.

4. Roles & Responsibilities

- **Practice Principal/Clinical Services Manager**: ensures compliance, oversight, and adequate resources.
- **IT/Security Officer (Clinical Services Manager)**: manages system security, backups, and staff training.
- **All Staff**: comply with this policy, complete privacy and security training, and report risks or breaches immediately.

6. Review

We review this policy **annually**, or sooner if legislation, RACGP standards, or technology requirements change.

Practice Specifics