Privacy Policy

Introduction

Coffs and Moonee Medical Centre is dedicated to protecting the privacy and security of personal and sensitive health information. This Privacy Policy outlines how personal information is collected, used, disclosed, stored and safeguarded in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).
This policy is available on the practice website, displayed in clinic waiting areas, and available at reception on request. This policy applies to all staff, contractors, students and visitors.

Consent

Upon registration as a patient, consent is obtained for General Practitioners and authorised staff to access and use personal information for the purpose of providing safe and effective healthcare services. Access to personal information is limited to individuals who require it to perform their role.
Any use of personal information beyond the primary purpose of care requires additional consent, unless otherwise permitted or required by law. Consent may be withdrawn at any time, subject to legal and clinical obligations.

Why Personal Information is Collected, Used, Held and Shared

Personal information is collected, used, held and shared to support the delivery of healthcare services. This includes diagnosis, treatment, follow-up and continuity of care. Personal information may also be used for directly related business activities such as billing, Medicare and health fund claims, accreditation, quality improvement, audits and staff training.

Information Collected

The types of information collected include:
- **Personal information:** Name, date of birth, address, contact details, Medicare number and health identifiers. Personal information is regularly reviewed to ensure accuracy.
- **Medical information:** Medical history, medications, allergies, test results, referrals, correspondence and other health-related information required for care.

Dealing with the Practice Anonymously

Patients may interact anonymously or using a pseudonym were lawful and practicable. Identification may be required where necessary to provide healthcare or where required or authorised by law.

How Personal Information is Collected

Personal information may be collected through:
- **Registration and appointments:** Verbal, written or electronic collection during registration or consultations
- **Medical services:** Information provided during consultations or treatment
- **Electronic systems:** Electronic transfer of prescriptions, My Health Record, or transfer of records from other healthcare providers
- **Online interactions:** Website enquiries, emails, SMS, phone calls and online appointment bookings
- **AI transcription tools:**
  General Practitioners may use AI-powered transcription tools to assist with generating consultation notes. These tools are used to improve documentation accuracy and efficiency. Information processed through these tools is handled in compliance with Australian privacy law and accessed only by authorised personnel. Patients are informed of this process, and consent is obtained where required. No clinical decisions are made solely by artificial intelligence systems. This policy will be updated in line with legislative and regulatory changes.
  Other sources:
- Parents, guardians or responsible persons
- Other healthcare providers including specialists, allied health professionals, hospitals, pathology and diagnostic imaging services
- Medicare, health funds or the Department of Veterans' Affairs, where necessary

How Personal Information is Sent and Received

Medical correspondence is exchanged using secure clinical software and ADHA-approved secure messaging systems, including Best Practice, HealthLink and encrypted platforms such as HotDoc.
With patient education and consent, some correspondence may be transmitted using less secure methods, including:
- General email
- Email secured with a non-ADHA-approved certificate
- Electronic faxing
- Unsecured web-based forms

Sharing Personal Information

Personal information may be disclosed in the following circumstances:

- With patient consent
- To other healthcare providers involved in patient care
- For billing, Medicare and insurance purposes
- Where required or authorised by law
- In emergency situations to prevent serious threat to life, health or safety
- Through the My Health Record system, where applicable

Access to personal information is restricted to authorised individuals. Personal information is not disclosed to third parties outside these circumstances without consent. Information is not disclosed outside Australia without consent unless permitted or required by law.

How Personal Information is Protected

Both electronic and paper-based records are used.

- Electronic information is protected using secure systems, encryption, password protection and two-factor authentication. Access is role-based and limited to authorised users.
- Audit and access controls are maintained in accordance with clinical software capabilities.
- Server rooms are secured, with access restricted to authorised management personnel.
- Paper records are stored in locked containers with restricted access and are securely destroyed when no longer required.
- All staff, contractors, students and visitors are required to sign confidentiality agreements.
- Privacy training is provided on commencement and periodically thereafter.

AI transcription tools operate under strict confidentiality protocols. AI-generated content forms part of the clinical record and is protected under the same security and privacy standards as all other health information. Personal health information is not stored offshore or shared outside Australia without consent unless permitted or required by law.

Patient Rights

- **Access:** Patients may request access to personal health information and obtain copies.
- **Correction:** Patients may request correction of inaccurate, incomplete or outdated information.
- **Restriction:** Patients may request limits on the use or disclosure of personal information, where practicable.

Requests must be made in writing using a practice form or during a consultation. A response will be provided within **30 days or less**. If reasonable fees apply, patients will be informed prior to processing. Where corrections require clinical input, a consultation may be requested. If access or correction is refused, written reasons will be provided along with available review options.

Data Retention

Personal health information is retained in accordance with legislative requirements and for as long as necessary to fulfil its purpose. Information that is no longer required is securely destroyed or de-identified.

Changes to This Policy

This Privacy Policy is reviewed **at least annually** and updated as required to reflect changes in legislation, technology or practice operations.

Privacy Complaints and Contact Details

Questions, concerns or complaints regarding privacy or the handling of personal information may be directed to the Privacy Officer:

Privacy Officer: Karen
Role: Practice Manager
Coffs Medical Centre
42–44 Gordon Street
Coffs Harbour NSW 2450
Email: practicemanager@coffsmedical.com.au
Phone: (02) 6648 5222

Complaints will be acknowledged and managed within 30 days in accordance with the resolution process.

If concerns are not resolved, a complaint may be made to the **Office of the Australian Information Commissioner (OAIC)**. The OAIC generally requires an opportunity for the practice to resolve the matter first. Further information is available at www.oaic.gov.au or by calling 1300 363 992.