Crown West Medical Privacy Policy

Document Control

Document Title: Privacy Policy

Version: 2026

Document Owner: Practice Manager

Privacy Officer: Nicole Mayo

Approved By: Practice Owners

Last Review Date: June 2026

Next Review Date: June 2027

Version History

Version	Date	Author	Summary of Changes
2022	July 2022	Crown West Medical	Initial Privacy Policy adopted.
2026	June 2026	Nicole Mayo	Comprehensive review and update to align with current Privacy Act requirements, RACGP Standards, telehealth services, My Health Record, electronic communications, AI-assisted documentation systems, cybersecurity requirements and contemporary practice operations.

Purpose

Crown West Medical is committed to protecting the privacy, confidentiality, integrity and security of personal and health information collected, used, stored and disclosed in the course of providing healthcare services.

This Privacy Policy outlines how Crown West Medical manages personal and health information in accordance with applicable privacy legislation, professional obligations and accreditation standards.

This policy applies to all doctors, nurses, reception staff, contractors, students and other authorised persons who access information held by Crown West Medical.

Practice Details

Crown West Medical is a privately billing general practice located in Wollongong, New South Wales.

Practice Address:
330 Crown Street
Wollongong NSW 2500

Telephone:
(02) 4228 4155

Website:
www.crownwestmedical.com

Email:
reception@crownwestmedical.com

This Privacy Policy applies to all services provided by Crown West Medical including face-to-face consultations, telehealth consultations, nursing services, treatment room services, online booking systems and electronic communications.

Scope

This policy applies to all personal and health information collected by Crown West Medical in any format, including:

- Electronic records
- Paper records
- Telephone communications
- Email communications
- SMS communications
- Telehealth consultations
- Online booking systems
- Website enquiries
- My Health Record interactions
- Clinical documentation systems
- Artificial intelligence assisted documentation systems

This policy also applies to contractors, students, visiting healthcare providers and temporary staff who access practice information or systems.

Legislative and Regulatory Framework

Crown West Medical manages personal and health information in accordance with:

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- My Health Records Act 2012
- Healthcare Identifiers Act 2010
- Health Practitioner Regulation National Law
- RACGP Standards for General Practices
- Relevant Commonwealth and State legislation relating to health records and privacy

Definitions

Personal Information

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Health Information

Health information includes information about a person's physical or mental health, medical history, diagnosis, treatment, medications, investigations, referrals and healthcare services.

Sensitive Information

Health information is considered sensitive information under privacy legislation and is afforded a higher level of protection.

Collection of Information

Crown West Medical collects personal and health information that is reasonably necessary to provide healthcare services and manage the operation of the practice.

Information collected may include:

- Name, date of birth and gender
- Residential and postal address
- Telephone numbers and email addresses
- Emergency contact details
- Medicare, DVA and health fund information
- Healthcare Identifier information

- Medical history
- Family history
- Medication history
- Allergies and adverse reactions
- Immunisation records
- Investigation results
- Referral letters
- Specialist reports
- Hospital correspondence
- Care plans and health assessments
- Financial and billing information
- Other information relevant to healthcare delivery

How Information is Collected

Information may be collected directly from patients through:

- New patient registration forms
- Consultations
- Telephone calls
- Email communications
- SMS communications
- Telehealth consultations
- Online booking systems
- Website enquiries
- Patient surveys and feedback

Information may also be collected from:

- Parents and guardians
- Carers and authorised representatives
- Treating specialists
- Allied health providers
- Hospitals
- Pathology providers
- Radiology providers
- My Health Record
- Government agencies
- Other healthcare providers involved in patient care

Purpose of Collection

Personal and health information is collected to:

• Provide safe, effective and appropriate healthcare
• Maintain accurate clinical records
• Communicate with patients regarding their healthcare
• Coordinate care with other healthcare providers
• Arrange referrals and investigations
• Process Medicare and health fund claims
• Conduct recalls and reminders
• Manage preventative healthcare activities
• Meet legal and regulatory obligations
• Facilitate quality improvement activities
• Support accreditation requirements
• Manage the operation of the practice

Where lawful and appropriate, patients may choose not to provide certain information. However, this may affect the practice's ability to provide healthcare services.

Use and Disclosure of Information

Crown West Medical uses and discloses personal and health information only for purposes directly related to the provision of healthcare services, the operation of the practice, or as otherwise permitted or required by law.

Information may be used or disclosed for the following purposes:

• Provision of healthcare services
• Coordination of patient care
• Communication with patients regarding appointments and healthcare needs
• Referrals to specialists and allied health providers
• Requests for pathology and diagnostic imaging services
• Processing Medicare, DVA and health fund claims
• Management of recalls and reminders
• Preventative healthcare activities
• Accreditation and quality improvement activities
• Legal and regulatory compliance
• Clinical auditing and risk management
• Emergency situations where disclosure is necessary to lessen or prevent a serious threat to health or safety

Information may be disclosed to:

• Treating doctors within the practice
• Specialists
• Allied health providers
• Hospitals

• Pathology providers
• Radiology providers
• Community healthcare providers
• Medicare and other government agencies where required
• Medical indemnity insurers
• Legal representatives where authorised or required by law
• Accreditation agencies where permitted by legislation
• Service providers supporting practice operations

Crown West Medical will only disclose information to third parties where appropriate consent has been obtained or where disclosure is otherwise authorised by law.

Electronic Communications

Crown West Medical uses electronic communication systems to support patient care and practice operations.

These communications may include:

• Appointment reminders
• Appointment confirmations
• Clinical recalls
• Preventative health reminders
• Vaccination campaigns
• Health assessment invitations
• Screening program reminders
• Information regarding healthcare services available within the practice
• Practice operational updates

Communications may be provided by:

• SMS
• Telephone
• Email
• HotDoc
• Secure messaging systems

Patients may opt out of receiving non-clinical communications at any time by notifying the practice.

Clinical recalls, safety notifications and communications necessary for patient care may continue to be provided where clinically appropriate.

Telehealth Services

Crown West Medical offers telehealth services where clinically appropriate.

Telehealth consultations may be conducted using:

- Telephone consultations
- HotDoc Telehealth
- Best Practice Telehealth
- Other approved telehealth platforms as required

Telehealth consultations are subject to the same privacy and confidentiality obligations as face-to-face consultations.

Patients should be aware that while reasonable measures are taken to protect privacy and security, no electronic communication system can be guaranteed to be completely secure.

My Health Record

Crown West Medical participates in the My Health Record system.

Doctors may access information available within My Health Record where clinically appropriate and permitted by legislation.

Doctors may upload information including:

- Shared Health Summaries
- Event Summaries
- Other permitted clinical documents

Patients maintain control over their My Health Record and may apply access controls in accordance with My Health Record legislation.

Further information regarding My Health Record is available at:

www.myhealthrecord.gov.au

Online Bookings and Patient Engagement Platforms

Crown West Medical utilises HotDoc to support appointment bookings, appointment reminders, telehealth services and patient communications.

Patients using online booking services may provide personal information directly through these platforms.

The practice takes reasonable steps to ensure that service providers maintain appropriate privacy and security protections.

Patients are encouraged to review the privacy policies of third-party platforms they choose to use.

Website and Social Media

Crown West Medical maintains a website and social media presence to provide information regarding healthcare services, practitioners, practice updates and health promotion activities.

The practice website may collect limited technical information including:

- Browser type
- Device information
- Date and time of access
- Website usage information

Information submitted through website enquiry forms may be used to respond to patient enquiries and provide requested information.

Patients should avoid submitting sensitive health information through unsecured website forms or social media platforms.

Social media platforms are not monitored for urgent clinical matters and should not be used for emergency healthcare concerns.

The practice website may utilise cookies and similar technologies to improve website functionality and user experience. Patients may adjust browser settings to manage cookie preferences.

Artificial Intelligence Assisted Documentation

Crown West Medical may utilise approved artificial intelligence (AI) assisted documentation systems to support clinical note taking, workflow efficiency and administrative functions.

Current approved systems may include:

- Lyrebird
- Heidi

These systems are used solely to support healthcare delivery and practice operations.

The use of AI-assisted documentation does not replace clinical judgement or professional responsibility.

Patients are informed of the use of AI-assisted documentation through practice consent processes and may decline participation where clinically appropriate.

Any information processed by AI-assisted documentation systems remains subject to the same privacy, confidentiality and security obligations that apply to all patient health information held by the practice.

Patients who do not consent to the use of AI-assisted documentation during their consultation should advise their treating practitioner or a member of the practice team.

The use of AI-assisted documentation does not replace clinical judgement or professional responsibility.

All AI-assisted documentation systems used by the practice must comply with privacy, confidentiality and information security requirements.

Third-Party Service Providers

Crown West Medical utilises a number of third-party providers to support healthcare delivery and practice operations.

These may include:

- Best Practice Clinical Software
- HotDoc
- Cubiko
- Heidi
- Lyrebird
- Secure messaging providers, including HealthLinks
- Cloud backup providers
- Information technology support providers
- Website service providers
- Payment processing providers, including Tyro

Reasonable steps are taken to ensure service providers implement appropriate privacy, confidentiality and information security protections.

Information disclosed to third-party providers is limited to that necessary for the provision of services.

Information Security

Crown West Medical takes reasonable steps to protect personal and health information from misuse, interference, loss, unauthorised access, modification or disclosure.

Security measures may include:

- Secure clinical software systems
- Password protected devices and systems
- User access controls and permissions
- Multi-factor authentication where available
- Secure cloud backup systems
- Firewall and antivirus protections
- Managed information technology support
- Physical security controls
- Staff confidentiality agreements
- Staff privacy and cybersecurity training
- Business continuity and information recovery planning

Access to patient information is restricted to authorised personnel who require access to perform their duties.

All staff, contractors and students are required to maintain the confidentiality of patient information.

Staff Confidentiality

All employees, contractors, students and healthcare practitioners working within Crown West Medical are required to maintain the confidentiality of personal and health information.

Access to patient information is limited to individuals who require access in order to perform their duties.

Unauthorised access, use or disclosure of patient information may result in disciplinary action and may constitute a breach of privacy legislation or professional obligations.

Overseas Disclosure of Information

Crown West Medical takes reasonable steps to ensure that personal information remains protected when utilising third-party service providers.

Some third-party software providers or technology platforms used by the practice may store or process information using infrastructure located outside Australia.

Where information may be transferred outside Australia, Crown West Medical will take reasonable steps to ensure that providers maintain privacy and security protections consistent with Australian privacy requirements.

The practice will only utilise service providers that have appropriate privacy, confidentiality and information security safeguards in place.

Data Retention, Archiving and Record Management

Crown West Medical retains patient records in accordance with legislative, professional and medico-legal requirements.

Inactive patient records are securely retained and archived. Patient records are not routinely destroyed and remain accessible to authorised personnel where required for healthcare delivery, legal obligations or other authorised purposes.

Archived records continue to be protected by the same privacy and confidentiality requirements that apply to active patient records.

Where records are eventually destroyed, destruction will occur only in accordance with applicable legislation and professional requirements and in a manner that protects patient confidentiality.

Data Breach Response

Crown West Medical maintains procedures for responding to actual or suspected privacy breaches, cybersecurity incidents and unauthorised access to information.

In the event of a suspected or confirmed data breach, the practice will:

- Identify and contain the incident
- Assess the nature and extent of the breach
- Determine potential risks to affected individuals
- Implement measures to minimise harm
- Notify affected individuals where required
- Notify relevant authorities where required
- Document and investigate the incident
- Implement corrective actions to reduce future risk

Where a breach is considered an eligible data breach under the Privacy Act 1988, Crown West Medical will comply with the requirements of the Notifiable Data Breaches Scheme.

Crown West Medical maintains a separate Data Breach Response Procedure which provides detailed guidance for the management, investigation, notification and review of actual or suspected privacy breaches and cybersecurity incidents.

Access to Personal and Health Information

Patients have the right to request access to their personal and health information held by Crown West Medical.

Requests should be made in writing to the Privacy Officer.

Access requests will be managed in accordance with privacy legislation, professional obligations and clinical considerations.

In certain circumstances access may be refused or limited where permitted by law.

Where access is provided, reasonable administrative fees may apply in accordance with applicable legislation and professional guidelines.

Correction of Information

Crown West Medical takes reasonable steps to ensure that information held by the practice is accurate, complete, relevant and up to date.

Patients are encouraged to advise the practice if any information requires correction or updating.

Requests for correction should be directed to the Privacy Officer.

Where appropriate, records will be amended or updated to ensure accuracy.

Privacy Complaints

Patients who have concerns regarding the collection, use, disclosure or management of their personal information are encouraged to contact the practice.

Privacy complaints should be directed to:

Privacy Officer

Nicole Mayo
Practice Manager
Crown West Medical

Address:
330 Crown Street
Wollongong NSW 2500

Telephone:
(02) 4228 4155

Email:
reception@crownwestmedical.com

Website:
www.crownwestmedical.com

Alternate Privacy Contacts:

Dr Jennifer Peattie
Practice Owner

Amber Cartner
Second in Charge

Patients may contact the Privacy Officer regarding:

- Privacy complaints
- Requests for access to health information
- Requests for correction of information
- Questions regarding this Privacy Policy
- Concerns regarding the handling of personal information

The practice will acknowledge privacy complaints within 5 business days where reasonably practicable and aims to provide a response within 30 days following investigation of the matter.

The practice will investigate all privacy complaints fairly and confidentially and will inform patients of the outcome of the investigation and any actions taken.

External Complaints

If a patient is dissatisfied with the outcome of a privacy complaint, they may contact the relevant external authority.

Office of the Australian Information Commissioner (OAIC)

The OAIC is responsible for administering the Privacy Act 1988 and investigating privacy complaints relating to personal information.

Website: www.oaic.gov.au

Telephone: 1300 363 992

Health Care Complaints Commission (HCCC)

The Health Care Complaints Commission is responsible for managing complaints about health services and healthcare providers in New South Wales.

Website: www.hccc.nsw.gov.au

Telephone: 1800 043 159

Privacy Officer Responsibilities

The Privacy Officer is responsible for:

- Oversight of privacy management within the practice
- Management of privacy complaints
- Responding to access and correction requests
- Coordination of privacy training and awareness
- Monitoring privacy compliance
- Management of privacy incidents and breaches
- Coordination of privacy policy reviews

Related Policies and Documents

This Privacy Policy should be read in conjunction with:

- Business Continuity, Disaster Recovery and Information Recovery Plan
- Information Security Policies and Procedures
- Data Breach Response Procedures
- Social Media Policy
- Patient Registration and Consent Forms
- My Health Record Policy
- RACGP Standards for General Practices

Policy Review

This Privacy Policy will be reviewed:

- At least annually
- Following significant legislative changes
- Following significant changes to practice operations
- Following implementation of new technology systems
- Following privacy incidents or data breaches
- Following identification of new privacy risks

Approval

This Privacy Policy has been approved by the Practice Owners of Crown West Medical and applies to all staff, contractors, students and healthcare practitioners working within the practice.

Approved By: Jennifer Peattie

Position: Practice Owner

Date: 15/06/2026

Review Date: 15/06/2027

The following appendix provides additional information regarding third-party service providers utilised by Crown West Medical to support healthcare delivery and business operations.

Appendix A – Third Party Providers Register

Purpose

Crown West Medical utilises a number of third-party service providers to support healthcare delivery, communication, information management, business operations and information technology services.

The practice undertakes reasonable steps to ensure that service providers maintain appropriate privacy, confidentiality and information security protections.

Provider	Service Provided	Information Potentially Accessed

Best Practice	Clinical software and patient record management	Personal information, health information, appointment and billing information
HotDoc	Online bookings, telehealth and patient communications	Personal information, appointment information and communication records
Cubiko	Practice analytics and reporting	De-identified and practice performance information
Heidi	AI-assissted clinical documentation	Clinical consultation information where utilised by treating practitioners
Lyrebird	AI-assissted clinical documentation	Clinical consultation information where utilised by treating practitioners
Dainamik IT Consulting	Information technology support, backup management and cybersecurity services	Systems and information required to provide IT support services
Studio Friday	Website management, digital marketing and social media management	Limited business and website information required to provide services

Review of Third Party Providers

Third-party providers are reviewed periodically to ensure continued suitability, privacy compliance and information security standards.

The practice will take reasonable steps to ensure service providers comply with applicable privacy obligations and maintain appropriate safeguards for information security.

Appendix B – Privacy Request Register Template

Date	Patient Name	Request Type	Staff Member	Outcome	Completion date