

Colour City Medical Practice

Privacy Policy



Revised: 08/09/2025

Introduction

The objective of this privacy notice is to provide you, our patient, with clear information on how your personal information is collected and used within the practice. Occasionally we also need to share your personal information to involve others in your healthcare and this policy outlines when, how, and why we share your information.

Why and when your consent is necessary

When you register as a patient of this practice, you provide consent for the GPs and practice staff to access and use your personal information to facilitate the delivery of healthcare. Access to your personal information is restricted to practice team members who require it for your care. If we ever use your personal information for purposes other than healthcare provision, we will obtain additional consent from you.

It is important to us that as our patient, you understand why we collect and use your personal information.

Why do we collect, use, hold and share your personal information?

Our practice will need to collect your personal information to provide healthcare service to you. Our main purpose for collecting, using, holding, and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims (Medicare related/Insurance company claims and payments), practice audits and accreditation, and business processes such as staff training. The practice may use your personal information for quality improvement of our services offered to patients through surveys, research, and patient data analysis and for training activities with the practice team. We may provide de-identified data to other organisations to improve population health outcomes. The information is secure, patients cannot be identified, and the information is stored within Australia. You can let reception staff know if you do not want your information included.

What personal information do we collect?

The information we collect about you includes but is not limited to:

- Name, date of birth, address, contact details, gender(at birth/ assigned), pronouns
- Medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number for identification and claiming purposes
- Healthcare identifiers.

How do we collect your personal information?

Our practice may collect your personal information in several different ways but not limited to:

1. When making a first appointment our practice staff will collect your personal and demographic information via your registration.
2. When providing medical services, we may collect further personal information. We use electronic transfer of prescriptions (eTP) and My Health Record; the upload of shared health summaries and event summaries where consent is given.
3. We may also collect your personal information when you visit our website, send us an email or SMS, telephone us or communicate with us using social media.
4. In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from you directly. This may include information from but not limited to:
 - a. Your guardian or responsible person
 - b. Other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
 - c. Medicare, or the Department of Veterans' Affairs (as necessary)
5. Various types of images may be collected and used, including:
 - a. **CCTV footage:** Collected from our premises for security and safety purpose
 - b. **Photos and medical images:** These can be taken using personal devices for medical purposes, please see the outline below on using personal devices for medical images.

Photos and medical images

Clinical photos may be taken with the consent of the patient. This is for the purpose of patient management and as a component of the patient's health record. These are treated like any other personal health information collected, disclosed and stored/destroyed subject to the same conditions under the Privacy Act 1988 (please see storage retention and record destruction policy).

Potential Hazards

A clinical photo is likely to capture details of a sensitive nature. In the digital age, a photo can be a permanent record and if it ends up in the public domain, it has the potential to cause embarrassment or psychological harm.

Photos can be sent to the wrong person by accident and there is a risk that they may be intercepted during transmission to other devices. When clinical photos are sent to another clinician for consultation or second opinion, there is no guarantee they will be stored securely on that person's device.

Clinical photos taken on a personal mobile device should be treated with particular care. A clinician's own phone or tablet might not be as secure as other devices used in the practice for storing sensitive medical information.

A personal device is perhaps more likely to be lost, stolen or accessed by other people. Another hazard is that a clinician might simply forget to transfer the photos from the personal mobile device to the patient's medical record or to delete the photo from the device after the photo has been transferred.

CCTV Footage

Another way the practice may capture images is with the utilisation of CCTV footage. The images and recordings cover certain areas of the practice including the side entrance leading into reception and the car, north side of the building. There are signs of CCTV cameras being used on the premises at the entrance to the practice for all visitors' awareness.

Compliance with privacy obligation

We will always comply with privacy obligations when collecting personal information from third-party sources. This includes ensuring transparency with patients, obtaining necessary consents, maintaining data accuracy, securing the information, and using it only for specified purposes.

When, why and with who do we share your personal information?

We sometimes share your personal information with but not limited to:

- With third parties who work with our practice for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with our policy of confidentiality, APP's and this policy
- With other healthcare providers
- When it is required or authorised by law e.g. court subpoenas
- When it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the patient's consent
- To assist in locating a missing person
- To establish, exercise or defend an equitable claim
- For the purpose of confidential dispute resolution process
- When there is a statutory requirement to share certain personal information, e.g. some diseases require mandatory notification
- During the course of providing medical services, through eTP, My Health Record, e.g. via Shared Health Summary, Event Summary.

Only people who need to access your personal information will be able to do so. Other than providing medical services or as otherwise described in this policy, the practice will not share personal information with any third party without your consent. We do not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

My Health Record

My Health Record is an electronic summary which may contain some of a patient's key health information. This allows information to be shared securely between the patient and registered healthcare providers involved in their care, to support improved decision making and continuity of care. Every person known to Medicare or the Department of Veterans' Affairs (DVA) automatically had a record created for them in early 2019, unless they chose to opt out or previously cancelled their record. Individuals can permanently delete their My Health Record at any time and can re-register for a new record if they decide they want one in the future.

How do we store and protect your personal information?

Your personal information may be stored at our practice in various forms. We are a “paperless” practice, meaning that the bulk of your health records are stored electronically. Our computers are secured by passwords and timed screen savers. We use encrypted software programs for use in a healthcare setting where confidentiality and security of medical information is paramount.

Within the practice reports and information from third parties regarding your medical information are received via post and fax services. These are kept in a secure location until scanned electronically into the doctor’s inbox or patient file. After information is scanned this information is securely disposed of through a trusted shredding service that is contracted by us and upholds the same strict confidentiality and privacy laws as we do. All staff and health professionals are trained in the confidentiality of patient information and sign a confidentiality agreement on employment or entry to the practice. Our practice stores all personal information securely.

How do we maintain your privacy during telehealth consults?

The practice maintains your privacy in telehealth by requiring secure environments for both the patient and clinician, using secure technology, verifying patient identity, ensuring patient consent, using secure methods for information exchange, having clear policies on data handling, and providing staff training on privacy obligations and procedures.

Remote and wireless access

Remote access is achieved by utilising a virtual private network connection (VPN), which then provides a restricted user group with a secure remote desktop experience.

Wireless connectivity is available at a need to have basis only, primarily for the availability of continuous communication and internet access.

Please see remote and wireless access policy.

Dealing with us anonymously

You have the right, under The Privacy Act (1988), to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorised by law to only deal with identified individuals. In this case you will be privately charged for any visits to the health professionals in this practice. Without identification we cannot charge under Medicare. As a general rule, we deem this to be impracticable for the purpose of safe and appropriate healthcare in this practice.

Release of clinical information in document automated technologies

The management and release of sensitive Clinical information is managed directly by the settings within our Clinical Software package. These settings are reviewed on a regular and need to basis, therefore maintained in consultation with the Clinical oversight team. This control over the release of sensitive clinical information defines that only the relevant information is included documents i.e. Health Summaries, referral letters.

What trans-border disclosures do we make?

We operate and communicate with organisations throughout Australia. We may therefore disclose personal information outside the State or Territory in which the individual resides.

Will your information be used for marketing purposes?

The practice will not use your personal information for marketing any goods or services directly to you without your expressed consent. If you do consent, you may opt out of direct marketing at any time by notifying the practice in writing.

Third party sources

We will always comply with privacy obligations when collecting personal information from third-party sources. This includes ensuring transparency with patients, obtaining necessary consents, maintaining data accuracy, securing the information, and using it only for specified purposes.

How if your information used to improve services?

The practice may use your personal information to improve the quality of the services offered to patients through analysis of patient data for quality improvement and for training activities within the practice team.

We may be required to release de-identified data to other government organisations to improve population health outcomes. The information is secure and is stored within Australia.

Document automation technologies

Document automation is where systems use existing data to generate electronic documents relating to medical conditions and healthcare. The practice uses document automation technologies to create documents such as referrals, which are sent to other healthcare providers. These documents contain only your relevant medical information.

Document automation technologies are used in our clinical medical software BP-Premier provided by BestPractice. All users of the medical software have their own unique user credentials and password and can only access information that is relevant to their role in the practice team. The practice complies with the Australian privacy legislation and APPs to protect your information.

How are artificial intelligence (AI) scribes used?

The practice uses AI scribe in a limited pilot use capacity. Currently this tool is being used to a test basis for the purposes of consultation notes recording with further enhancements to be employed in the future.

The AI scribe utility requires a microphone to transcribe the consultation notes and to generate other clinical note for your health record. The practice utilizes multiple AI platforms at this point.

These AI transcribing tools:

- Do not share information outside of Australia
- The audio file is destroyed once the transcription is complete.

Audio/ Visual

We will always seek your informed consent should real-time audio/visual equipment is used during the consultation. Video may be used for some Telehealth consults, no recordings are ever made or stored by Colour City Medical Practice.

How can you access and correct your personal information at our practice?

You have the right to request access to, and correct, your personal information. Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing by either post or by email (practice@colourcitymedicalpractice.com.au) and our practice will respond within 30 days. A transfer of medical information form will need to be signed and verified to allow records to be transferred between practices. There may be a cost to the provision of paper records depending on the size of the file.

Our practice will take all reasonable steps to ensure your personal information collected is accurate and up to date. We also take reasonable steps to update your details and ensure they are current and complete. A request to correct or update your personal details can be made at any time by contacting us on the details listed below. You should make such requests in a timely manner after any changes. There may be circumstances in which we may have to refuse a request for correction. If this happens, we will notify the individual in writing of our reasons for refusal and explain how the individual can complain if not satisfied.

How can you lodge a privacy-related complaint, and how will the complaint be handled?

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with our resolution procedure in a timely manner, within 30 days.

Our contact details are:

Attention: Practice Manager

Address: Colour City Medical Practice
71 Dalton Street, Orange NSW 2800

Telephone: 02 6360-2388

Email: practice@colourcitymedicalpractice.com.au

You can also contact the OAIC, they will require you to give them time to respond before they will investigate.

For Further information visit www.oaic.gov.au or call OAIC on 1300 363 992.

Privacy and our website

Colour City Medical Practice website is not used to collect any patient information. Appointments can be made through the website by clicking the "Book Appointment" tab. This will take you to the HotDocs website developed exclusively for the use of Healthcare Providers for online appointments, recalls and reminders. HotDoc follows strict privacy and confidentiality guidelines and legislation. Any information provided to them will be used for the practice only and not for third parties or advertising of any kind.

Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. Patients will be made aware of any changes through the website or by notice posted in the practice from time to time.