

Privacy policy

Your information, your care and your choices

Prepared 31 August 2026 • Version 1.0

About this policy

Golden City Surgical is a six-surgeon specialist surgical practice in Bendigo, Victoria. This policy explains how our surgeons and authorised practice team collect, hold, use and disclose personal information, including sensitive health information, when providing and administering care. It covers our shared practice systems, clinical documentation and communications.

We are committed to handling information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles and the Health Records Act 2001 (Vic). Hospitals and other independent providers involved in your care may also hold records under their own privacy policies.

Information we collect

We collect identifying and contact details, date of birth, emergency contact and authorised representative details, Medicare and health-fund information, referrals, medical and family history, allergies, medicines, examination findings, investigation results, diagnoses and treatment plans. Records may also include clinical images where relevant and authorised, operation and hospital information, correspondence, appointment details, billing and payment records.

We collect only information reasonably necessary for our work or otherwise permitted or required by law. Please help us keep your contact, medication and other relevant details current.

How we collect information

We usually collect information directly from you, including through registration, consultations, telephone calls, correspondence and any telehealth care. We may also receive relevant information from your referring doctor, general practitioner, other specialists, hospitals, pathology or imaging providers, and an authorised representative, where you consent or the law permits.

You may ask about dealing with us anonymously or using a pseudonym where practical and lawful. For clinical care, accurate identification is usually necessary for safe treatment, record matching and claiming. If you choose not to provide information needed for care, we will explain any limits this places on the services we can safely provide.

Why we use information

We use information to assess your health, plan and provide surgical and other treatment, arrange hospital care and follow-up, communicate with your treating team, prepare clinical records, manage appointments and reminders, process accounts and claims, and meet legal, professional and patient-safety obligations.

Care, communication and systems

Consent and sharing for your care

We explain relevant information handling and seek consent where required. We may share information needed for your care with your GP, referring doctor, other treating specialists, anaesthetists, assistant surgeons, hospitals, pathology and imaging providers, pharmacists and allied health professionals. Access within our six-surgeon practice is limited to legitimate care or administrative needs; membership of the practice does not justify unrelated access.

We may disclose necessary information to Medicare, health funds, billing providers and other service providers for authorised claims and administration. Other disclosures occur with your consent or where required or permitted by law, such as a valid legal demand or a serious threat to health or safety. We do not sell your identifiable health information or use it for unrelated marketing without consent.

Gentu: clinical records and SMS

We use Gentu, supplied by Magentus Practice Management Pty Ltd, for patient records, appointments, referrals, results, correspondence, billing and SMS reminders. Magentus describes Gentu's core hosting as Australian, with encryption in transit and at rest and backup safeguards. Optional Practice Intelligence processing is explained on the next page.

Fastmail and electronic communication

We use Fastmail for practice email, and Gentu for SMS appointment and administrative messages. Ordinary email and SMS carry privacy risks, including delivery to an incorrect address or viewing on a shared device. We seek to limit sensitive content in reminders and use secure clinical messaging where appropriate and available.

Please tell reception your preferred contact method, whether messages can be left, and whether someone else can access your phone or email. Providing an email address is not consent to unrelated AI use. Fastmail uses international infrastructure; email information may be stored or processed overseas.

Overseas processing and service providers

Fastmail identifies possible transfers to the United States, United Kingdom, India and Austria, as well as Australia. Magentus says its partners or integrated services may transfer information to the United States, United Kingdom and countries in the European Union. Its public policy does not identify every EU country. Australian core hosting therefore does not mean all related processing stays in Australia.

We take reasonable steps to assess privacy and security arrangements, restrict access to what providers need, and comply with applicable overseas-disclosure requirements. Ask our Privacy Officer for information about the providers and locations relevant to your care. No electronic system is entirely risk-free.

Gentu Practice Intelligence

Golden City Surgical has elected to participate in Gentu Practice Intelligence. These optional data and AI-assisted features operate on information held in Gentu, including existing clinical notes, letters and results—not only information collected at your next visit.

What the features do

Depending on the features enabled, processing may support patient summaries, clinical decision-support messages, searches for patients meeting clinical criteria and identification of possible clinical-trial candidates. Magentus and its technology partners may process patient information to deliver these functions. This may involve sensitive health information and identifying details within our clinical system.

Magentus states that personal information is not provided to the language models used to structure clinical data, and that practice data is not used to train those models. These assurances concern that particular processing; they do not mean no patient information is accessed anywhere in the service. Provider privacy information is listed at the end of this policy.

Clinical judgement remains with your surgeon

AI can produce inaccurate or incomplete information. Summaries and prompts are advisory and require clinical assessment. Your surgeon remains responsible for clinical decisions and for reviewing AI-generated documentation before it enters your final record. We do not permit AI to independently diagnose you, determine treatment or decide whether you receive care.

Your choice: participate or opt out

You may decline, or later withdraw from, some or all Practice Intelligence features without affecting your access to or standard of medical or surgical care. Tell reception, your surgeon or our Privacy Officer. We will explain the features, record your choice and notify Magentus to arrange the relevant exclusion. We will follow up implementation and explain any limitations or delay; a request is not a guarantee of an immediate technical change.

Opting out of Practice Intelligence does not remove your medical record from Gentu or stop ordinary record keeping, appointments, billing or care communications. Withdrawal applies to future optional processing and does not undo lawful processing already completed. Previously irreversibly de-identified information may not be retrievable or attributable to you.

Separate decisions about scribes and research

Practice Intelligence consent does not authorise a scribe to listen to your consultation. If i-scribe or another approved ambient scribe is proposed, we ask separately before each consultation in which it is used. Gentu Scribe is not automatically authorised by this policy.

Trial matching does not enrol you in a trial. This policy and the registration addendum do not authorise participation in the separate Magentus Research Program or external data projects. Such proposals require separate practice review and any necessary patient information and consent.

i-scribe and record protection

i-scribe during consultations

Some of our surgeons use i-scribe, supplied by Akuru Pty Ltd, to help draft notes and letters. With your permission, consultation audio is transmitted for transcription and preparation of draft documentation. The content may include your identifying details and sensitive health information. Akuru advises that audio files are not retained.

Your surgeon will explain the proposed use and obtain and document your consent before i-scribe is used at each consultation. You can decline or ask for it to stop at any time, without affecting your care. The surgeon will document the consultation another way. A registration signature or counter sign does not replace this consultation-level consent.

Our i-scribe retention setting is 14 days. Akuru's policy provides for automatic deletion or de-identification at the selected retention period; de-identified information may be used for quality control or platform improvement. The final notes and letters approved by your surgeon and saved to your medical record are retained separately and are not deleted after 14 days.

Akuru advises that platform clinical information is processed and stored in Australia, including contracted AI processing, and that patient information is not used to train general-purpose or foundation AI models. These are provider statements, which we review as part of our ongoing assessment of the service.

Security and retention of your medical record

We take reasonable steps to protect electronic and paper information from misuse, loss, interference and unauthorised access, change or disclosure. Safeguards include appropriate access restrictions, staff confidentiality requirements, secure handling, physical protection, backup arrangements and review of technology-provider security. Access is limited to authorised people with a legitimate purpose.

We retain medical records for the periods required by law and professional obligations. In Victoria, this generally means at least seven years after the last health service for an adult, or until age 25 where the last service was provided while the patient was under 18. A longer period may be needed for legal or clinical reasons. Information no longer needed is securely destroyed or de-identified where lawful.

If a privacy incident occurs

We investigate suspected breaches, take steps to contain harm and meet applicable notification duties. Where required under the Notifiable Data Breaches scheme, we notify affected individuals and the Office of the Australian Information Commissioner and explain practical protective steps.

Your rights and privacy enquiries

Access and correction

You may ask for access to your information or request a correction through our Privacy Officer. We may verify your identity and ask you to describe the records sought. We respond within applicable legal timeframes and aim to respond within 30 days. Any lawful access charge will be explained in advance; there is no charge for requesting correction.

If access or correction is refused, we provide reasons where lawful and explain complaint options. Clinical records are usually corrected by an amendment or notation rather than erasing the original entry. If we disagree about a correction, you may ask us to associate a statement of your concern with the record.

Children, representatives and other uses

We consider a young person's capacity, privacy and applicable law when involving parents or guardians. We verify the authority of anyone acting for a patient who requires assistance. We share information with family or carers with authority or as the law permits, rather than assuming an emergency contact has unrestricted access.

Clinical audit, teaching, quality improvement and research must have an appropriate legal basis. We use de-identified information where practical and seek separate consent when required for identifiable information or research participation. Optional AI consent is not blanket consent to these other uses.

Questions, choices or complaints

Contact the Privacy Officer via the practice manager at Golden City Surgical. You can ask questions, record an AI opt-out or make a complaint in person, by telephone or in writing. We aim to respond to complaints within 30 days and will explain any delay.

Telephone: 03 5407 2228

Email: reception@goldencitysurgical.com.au

In person: Level 2, St Francis House, 138–140 Lily Street, Bendigo VIC 3550

Post: PO Box 119, North Bendigo VIC 3550

If unresolved, you can contact the Office of the Australian Information Commissioner (oaic.gov.au) or the Health Complaints Commissioner Victoria (hcc.vic.gov.au). We can help you locate their complaint processes or arrange assistance to understand this policy.

We review this policy when our services, AI tools or legal obligations change. Copies are available free from reception. Ask us for the current version and for further details about any proposed new processing.

Further information

Magentus: Practice Intelligence and patient choices

Magentus: privacy and overseas processing

i-scribe: privacy and retention

Fastmail: privacy and international transfers

OAIC: access to health information

Victorian Health Complaints Commissioner: health records