

Cumberland Street Clinic

PRIVACY POLICY

Effective date: August 2026 / Version [3.0] /

Our Commitment to Your Privacy

Cumberland Street Clinic ("we", "us", "our", "the practice") is committed to protecting the privacy and confidentiality of personal and health information we hold about our patients, staff and visitors. As a provider of general practice health services in New South Wales, we are bound by:

- the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs);
- the Health Records and Information Privacy Act 2002 (NSW) (HRIP Act) and the Health Privacy Principles (HPPs) set out in it;
- the My Health Records Act 2012 (Cth) and its associated rules, where applicable; and
- relevant professional obligations, including the RACGP Standards for General Practice and the Privacy and Managing Health Information in General Practice guide.

This policy explains how we collect, hold, use, disclose and protect personal and health information, and how you can access, correct or make a complaint about your information.

What is Personal and Health Information?

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

Health information is a specific category of personal information, and includes information about a person's physical or mental health, disability, health services provided or to be provided, and other information collected in providing a health service (such as appointment or billing details). Health information is given a higher level of protection under both the Privacy Act and the HRIP Act.

Information We Collect

The type of information we collect depends on the services provided, but generally includes:

- Identifying details: name, date of birth, gender, address, contact numbers and email address
- Medicare, Department of Veterans' Affairs (DVA), private health insurance and pension/concession card details
- Emergency contact and next-of-kin details
- Medical history, including past and current conditions, medications, allergies, immunisations, family history and lifestyle information
- Consultation notes, clinical observations, investigation results (pathology, imaging), specialist and allied health correspondence
- Appointment, recall and reminder information
- Billing, payment and claiming information
- Information you provide through online forms, patient portals or SMS/email communications

Where practical, we collect information directly from you. We may also collect information from a person responsible for you (such as a parent, guardian or carer), other treating practitioners, specialists, allied health providers, hospitals, pathology and diagnostic imaging providers, Medicare/DVA, your health fund, or (in an emergency, or where you have consented) family members.

Why We Collect, Hold, Use and Disclose Your Information

We collect and use personal and health information primarily to provide you with safe, high-quality medical care. This includes:

- assessing, diagnosing, treating and managing your health care, and coordinating care with other treating providers;
- administrative purposes, including making appointments, sending reminders and recalls, and billing and claiming through Medicare, DVA or your health fund;
- clinical audit, quality improvement and accreditation activities;
- practice management, reporting and business analytics to improve the services we provide;
- complying with our legal obligations, including mandatory reporting, notifiable disease reporting and responding to a subpoena or court order; and
- training, teaching or research purposes, but only with your consent or where information is de-identified.

We will not use or disclose your information for any other purpose without your consent, unless permitted or required by law (for example, where there is a serious threat to health or safety, or under public health legislation).

The Software We Use to Manage Your Information

We use a small number of trusted software systems to manage patient information securely. The table below summarises the main systems and the role each plays.

System	Function	Personal Information Involved
Best Practice (Bp Premier)	Our core clinical and practice management software, used to record patient health records, appointments, prescriptions, pathology and imaging results, billing and Medicare/DVA claiming.	Full clinical record: demographics, Medicare/DVA/health fund details, medical history, consultation notes, investigations, medications, correspondence and billing information.
Cubiko	A practice analytics and business intelligence platform that connects to our Best Practice database to generate reports on practice performance, clinical care gaps, recall compliance and financial metrics.	De-identified and aggregated data wherever possible. Where patient-level data is used (for example, to identify patients overdue for a health check), access is restricted to authorised staff for legitimate practice management and quality improvement purposes.
Automated Systems	A patient booking, recall, reminder and engagement platform used to book appointments, send SMS/email appointment reminders, recalls (e.g. for immunisations, chronic disease reviews and screening), and patient satisfaction or intake forms.	Patient contact details (mobile number, email), appointment details and recall/reminder categories necessary to deliver the relevant communication. Any online forms completed by patients are transmitted securely back into our clinical record.
Lyrebird Health (AI clinical tool)	An AI-powered ambient scribe used, with your consent, to listen to and transcribe consultations, producing a draft clinical note that the	Audio and/or transcript of the consultation, generated clinical note. Recordings and transcripts are processed to produce the note and are not used to train

	treating clinician reviews, edits and approves before it is saved to your record in Best Practice. An AI-powered document sorter which helps staff allocate the correct incoming documents to the correct patient file.	Lyrebird's underlying AI models on our patients' data, consistent with our agreement with the vendor.
Heidi (AI clinical scribe)	An alternative AI-powered ambient scribe, used in the same way as Lyrebird Health — to transcribe consultations and draft clinical documentation for clinician review — depending on which tool the treating clinician uses.	Audio and/or transcript of the consultation, generated clinical note. As with Lyrebird Health, output is reviewed and approved by your clinician before it forms part of your permanent record, and recordings/transcripts are not used to train the vendor's models on our patients' data, consistent with our agreement with the vendor.

All software platforms are provided by third-party vendors who access or process data on our behalf under contractual arrangements that require them to protect your information and use it only for the purpose of providing their service to us — they are not permitted to use your information for their own marketing or other purposes. These providers store data on secure, access-controlled servers, and we have assessed their security and privacy practices as part of choosing to work with them.

Best Practice: our clinical records remain the authoritative source of your health information. Best Practice data is stored on [servers located at our practice premises / a secure Australian-hosted cloud environment — delete as applicable] with role-based access restricted to authorised clinical and administrative staff.

Cubiko: connects securely (read-only) to our Best Practice database to produce practice-level and, where clinically relevant, patient-level reports (for example, identifying patients who may be overdue for a health assessment). Access to patient-identifiable Cubiko reports is limited to staff who need it to carry out recalls, quality improvement or practice management functions.

Automed: is used to contact you by SMS or email for appointment reminders and health recalls, and to send secure links for online patient intake or satisfaction forms. Automed only receives the contact and appointment/recall information needed to deliver these communications; clinical information you complete on an online form is transmitted back into your Best Practice record.

Heidi and Lyrebird Health: our clinicians may use one of these AI-powered ambient scribe tools to help produce consultation notes. See section 6 below for more detail on how these tools are used and the choices you have.

AI-Assisted Clinical Documentation (Heidi and Lyrebird Health)

Some of our clinicians use an AI clinical scribe — either Heidi or Lyrebird Health — during consultations to help produce clinical notes. These tools listen to (and/or transcribe) the conversation during your appointment and generate a draft note summarising what was discussed.

- We will let you know if an AI scribe is being used in your consultation and seek your verbal consent beforehand. You may decline, and the consultation will simply be documented manually as usual — this will not affect the care you receive.

- The treating clinician always reviews, edits and approves the AI-generated note before it is saved into your permanent clinical record in Best Practice. The AI-generated draft does not become part of your record unless the clinician confirms it is accurate.
- Recordings and transcripts are transmitted securely to the vendor's servers for processing and are handled under our agreement with that vendor, which requires them to protect the information and restricts them from using it to train their underlying AI models on our patients' data, or for any purpose other than providing the transcription/note-generation service to us.
- Both vendors do not store audio recordings and transcripts are deleted from the vendor's systems after the note has been generated and reviewed, in line with the vendor's data retention settings that we have configured (<7 days).
- If you would prefer your consultation is not recorded or processed by an AI scribe, please let your clinician or our reception staff know at any time — no explanation is required.

Storage and Security of Your Information

We take reasonable steps to protect personal and health information from misuse, interference, loss, and unauthorised access, modification or disclosure. These steps include:

- restricting access to records to authorised staff on a need-to-know basis, using individual logins and role-based permissions;
- requiring staff, contractors and software vendors to comply with confidentiality obligations;
- using secure, encrypted connections for data transmitted to and from Best Practice, Cubiko and Automed;
- maintaining firewalls, antivirus protection and regular software updates on practice systems;
- secure backup and disaster recovery arrangements for our clinical database;
- physical security measures for paper records and practice premises; and
- staff training on privacy and confidentiality obligations.

We retain health records for the period required by law — in NSW, generally at least 7 years from the last consultation for adult patients, and until a patient turns 25 (or as otherwise required) for records relating to a child. When information is no longer required, it is securely destroyed or de-identified.

CCTV and Practice Security

For the safety and security of our patients, staff and visitors, and to protect practice property, we operate closed-circuit television (CCTV) cameras at reception, waiting areas, car park and external entry points. CCTV is not used inside bathrooms, pathology, consultation or treatment rooms.

- Signage is displayed at practice entrances to notify patients, staff and visitors that CCTV recording is in operation.
- Footage is recorded and stored securely on a local network, with access restricted to the Practice Manager and Principal Doctor.
- Footage is retained for 30 days and then automatically overwritten or securely deleted, unless it is needed for an investigation, an incident report, or as required by law or by police.
- Footage may be disclosed to NSW Police or other authorities where there is a security incident, a threat to safety, or as otherwise required or authorised by law.
- You may request access to footage in which you appear by contacting our Privacy Officer; access may be limited where it would unreasonably impact the privacy of other identifiable individuals captured in the same footage.

Confidentiality and Staff Obligations

All clinicians, administrative staff, students, contractors and volunteers at this practice are bound by strict confidentiality obligations regarding patient information, in addition to their professional and ethical obligations (including, for registered health practitioners, obligations under the Health Practitioner Regulation National Law and the relevant AHPRA Code of Conduct).

- Every staff member signs a confidentiality agreement as a condition of engagement, and receives privacy and confidentiality training as part of their induction and ongoing professional development.
- Access to patient records, Cubiko, Automed, and the AI scribe tools Heidi and Lyrebird Health is granted on a need-to-know, role-based basis, and individual user logins allow us to audit who has accessed or amended a record.
- Staff must not access, use or disclose patient information other than as required to perform their role — browsing your own, a family member's, a colleague's or any other patient's record out of curiosity is strictly prohibited and may result in disciplinary action, and in some circumstances may be reportable conduct.
- Confidentiality obligations continue after a staff member's employment or engagement with the practice ends.
- Contractors and third-party software vendors (including Best Practice Software, Cubiko, Automed, Heidi and Lyrebird Health) are required, by contract, to protect the confidentiality of any patient information they access or process on our behalf.
- Any suspected breach of confidentiality by a staff member, contractor or vendor is investigated by the Practice Manager/Privacy Officer and managed in accordance with our data breach response process (see section 16 below).

Disclosure of Information to Third Parties

We may disclose your information to:

- other treating health professionals involved in your care (for example, specialists, allied health providers, hospitals, pathology and diagnostic imaging services);
- Medicare, DVA and your private health fund, for billing and claiming purposes;
- our software and service providers, including Best Practice Software, Cubiko, Automed, Heidi and Lyrebird Health, and our IT support providers, to the extent necessary for them to provide their services to us;
- our local Primary Health Network (PHN), in de-identified form only — see section 11 below;
- regulatory or government bodies where required or authorised by law (for example, notifiable disease reporting, or in response to a subpoena);
- your nominated emergency contact, in an emergency; and
- other parties where you have provided consent.

We do not sell, rent or trade your personal or health information to third parties for marketing purposes.

Sharing De-Identified Data with Our Local PHN

Like most Australian general practices, we share de-identified patient data with our local Hunter New England Primary Health Network (PHN). This data sharing supports population health planning, needs assessment, and quality improvement activities across our region, and helps the PHN and government understand and respond to local health trends (for example, rates of chronic disease, immunisation coverage or screening participation).

- Data is extracted from our Best Practice database using data extraction tools that are configured to de-identify or aggregate information before it leaves the practice — direct identifiers such as your name, date of birth, address and Medicare number are removed or obscured.
- The extracted data is used by the PHN for aggregate reporting, service planning and commissioning of health services, and quality improvement benchmarking (which may be fed back to us, including via Cubiko, to help us improve care for our patient population).
- This sharing is consistent with the PHN Data Governance Framework and relevant government data-sharing arrangements, and does not involve disclosing information that identifies you as an individual to the PHN.
- If you have concerns about de-identified data extraction from our systems, please speak with our Privacy Officer — in most cases this can be managed at an individual patient level upon request.

Cross-Border Disclosure

Our clinical and practice management data is generally stored and hosted within Australia. We ask our vendors to confirm their data hosting and security arrangements as part of our due diligence and only use vendors that handles your information consistently with the Australian Privacy Principles.

My Health Record

If you have a My Health Record, we may upload clinical documents (such as shared health summaries, event summaries and prescription/dispense records) to it as part of your care, unless you have told us not to, or have set access controls on your record. You can manage your My Health Record privacy settings, including who can access it and what is uploaded, via the My Health Record system or by calling the My Health Record Helpline on 1800 723 471.

Access to and Correction of Your Information

You have a right under the Privacy Act, the HRIP Act and, where relevant, the My Health Records Act, to access the personal and health information we hold about you, and to ask us to correct it if it is inaccurate, out of date, incomplete, irrelevant or misleading.

To request access to or correction of your record, please contact our Privacy Officer (details below) in writing. We will respond within a reasonable period (usually within 30 days). In most cases we will provide access, although there are limited circumstances where access may be restricted or refused — for example, where access would pose a serious threat to the life, health or safety of you or another person, or would have an unreasonable impact on the privacy of others. We may charge a reasonable fee to cover the cost of retrieving and copying information. If we refuse a request, we will explain our reasons.

Data Quality

We take reasonable steps to ensure the personal and health information we collect, use and disclose is accurate, complete and up to date, including asking you to confirm your details at each visit and encouraging you to let us know if your circumstances change.

Data Breaches

We have processes in place to identify, contain, assess and respond to data breaches, consistent with the Notifiable Data Breaches scheme under the Privacy Act. If a data breach occurs that is likely to result in serious harm to you, we will notify you and the Office of the Australian Information Commissioner (OAIC) as soon as practicable, in accordance with our legal obligations.

Anonymity and Pseudonymity

Where lawful and practicable, you may interact with us anonymously or under a pseudonym (for example, for general health information enquiries). However, for most clinical services we need to know your identity in order to provide safe and appropriate care, and to meet our Medicare and record-keeping obligations.

Complaints

If you have a concern about how we have handled your personal or health information, please contact our Privacy Officer in the first instance. We will investigate your complaint and respond within a reasonable timeframe (usually 30 days).

If you are not satisfied with our response, you may contact:

- The NSW Information and Privacy Commission (IPC) — for complaints under the Health Records and Information Privacy Act 2002 (NSW): 1800 472 679, or ipc.nsw.gov.au
- The Office of the Australian Information Commissioner (OAIC) — for complaints under the Privacy Act 1988 (Cth): 1300 363 992, or oaic.gov.au

- The Health Care Complaints Commission (NSW) — for complaints about health service delivery: 1800 043 159, or hccc.nsw.gov.au

Changes to This Policy

We may update this policy from time to time to reflect changes in our practices, software systems or legal obligations. The current version is always available at reception and on our website <https://www.cumberlandstreetclinic.com.au/privacy-policy>. This policy was last updated on August 2026.

Contact Us

For any questions about this policy, or to make a request regarding your personal or health information, please contact:

Privacy Officer: Dr Nicolette Holly (Practice Principal)

Practice: Cumberland Street Clinic

Address: 45 Cumberland St, Cessnock, NSW, 2325

Phone: 02 49903222

Email: admin@cumberlandstreetclinic.com.au