Central Highlands Healthcare: Privacy Policy

1 Purpose

Central Highlands Healthcare collects information on its patients as necessary to provide a high quality health service. Central Highlands Healthcare is committed to protecting your personal information. We are bound by the Information Privacy Act 2009 (Qld) and the Australian Privacy Principles.

This privacy policy is to provide information to you, our patient, on how your personal information (which includes your health information) is collected and used within our practice, and the circumstances in which we may share it with third parties.

2 What Personal Information we collect

'Personal health information' a particular subset of personal information and can include any information collected to provide a health service. This information includes:

- name, address, and contact details
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifiers
- health fund details
- family information,
- Information on your My Health record
- employment and other demographic data,
- and any health information such as a medical or personal opinion about a person's health, disability or health status.

It includes the formal medical record whether written or electronic and information held or recorded on any other medium e.g., letter, fax, or electronically or information conveyed verbally.

3 Dealing with us anonymously

You have the right 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.

4 How we collect your personal information

Our practice may collect your personal information in several different ways.

1. When you make your first appointment our practice staff will collect your personal and demographic information via your registration.
2. During the course of providing medical services, we may collect further personal information.
3. We may also collect your personal information when you visit our website, send us an email or SMS, telephone us, make an online appointment 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:
    - your guardian or responsible person
    - other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
    - your health fund, Medicare, or the Department of Veterans' Affairs (as necessary).
5. Information collected through third party access such as My Health record.

4.1 Patient Health Record

For each patient, the Practice has an individual patient health record. This is an electronic record containing all clinical information held by the Practice relating to that patient.

Central Highlands Healthcare ensures the protection of all information contained therein. Patient health records can be accessed by an appropriate team member when required. Central Highlands Healthcare ensures information held about the patient in different records (e.g., at a residential aged care facility) is available when required.

5 How we store and protect your personal information

Your personal information may be stored at our practice in various forms including:

- Paper records
- Electronic records
- Visual records,
- Audio recordings.

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

We sometimes share your personal information:

- 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 APPs and this policy
- with other healthcare providers
- when it is required by law
- when it is 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, e.g., via Shared Health Summary, Event Summary, GPMP Tool, Primary Sense, My Health Record, Reshealth).

Only people who need to access your information will be able to do so.

Other than in the course of providing medical services or as otherwise described in this policy, our practice will not share personal information with any third party without your consent.

We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

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

Our practice may use your personal information to improve the quality of the services we offer to our patients through research and analysis of our patient data.

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 our reception staff know if you do not want your information included.

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

You have the right to request access to, and correction of, your personal information.

Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing via email or in hard copy to the practice. Our practice will respond within a reasonable time. There may be fees associated with providing this information. If so, we will contact patients to discuss the cost before proceeding. These costs are associated with the request may include:

- The time taken to locate, retrieve and review which information is relevant to the request,
- Staff reproducing and sending the information,
- Postage and materials involved in completing the request
- Using an intermediary, if required

Our practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. From time to time, we will ask you to verify that your personal information held by our practice is correct and current. You may also request that we correct or update your information.

If you are making a request on behalf of another person, your request must be made in writing, and must include evidence of your authority to act on the other person's behalf.

Requests to access information or update information should be made in writing to:

- By post to Emerald Medical Group, PO Box 1844 Emerald Qld 4720.
- By email to enquiries@chhealth.com.au

Your request should include:

- Your full name, address and date of birth.
- For access requests: a description of the information you're requesting and whether you require a summary, a full copy or if you want to view your records in person.
- For correction requests: a description of the information you want to correct, the correct information and proof the existing information is inaccurate, incomplete, misleading or out-of-date.

7.1 Can we refuse your request?

Your request for access to your health information may be refused in some situations, such as if:

- it may threaten your or someone else's life, health or safety
- it may impact someone else's privacy
- giving access would be unlawful

If so, the reason for refusal will be advised in writing.

8 Who is responsible for privacy at CHH?

The organisation has a CEO with primary responsibility for the Central Highlands Healthcare's electronic systems, computer security and adherence to protocols. The CEO is supported in this role by the Clinical Education Coordinator and other staff and contractors of CHH. This responsibility is documented in the Position Description. Tasks may be delegated to others.

Security policies and procedures regarding the confidentiality of patient health records and information are documented and the Practice Team is informed about these at induction and when updates or changes occur.

9 Maintenance of Privacy

Doctors, nurses, allied health practitioners and all other staff and contractors associated with this Practice have a responsibility to maintain the privacy of personal health information and related financial information. The privacy of this information is every patient's right.

Members of the Central Highlands Healthcare team have different levels of access to patient health information (refer to Compute Information Security). To protect the security of health information, GPs and other practice staff do not give their computer passwords to others in the team.

The maintenance of privacy requires that any information regarding individual patients, including staff members who may be patients, may not be disclosed either verbally, in writing, in electronic form, by copying either at Central Highlands Healthcare or outside it, during or outside work hours, except for strictly authorised use within the patient care context at Central Highlands Healthcare or as legally directed.

Any information given to unauthorised personnel will result in disciplinary action and possible dismissal. Each staff member is bound by his/her privacy clause contained with the employment agreement which is signed upon commencement of employment at this Practice.

10 Our IT Systems

Practice computers and servers comply with the RACGP computer security checklist and the Practice has a sound back up system and a contingency plan to protect Central Highlands Healthcare from loss of data (refer to Computer Information Security).

Care should be taken that the general public cannot see or access computer screens that display information about other individuals. To minimise this risk automated screen savers should be engaged.

Reception and other Practice staff should be aware that conversations in the many areas of the practice can often be overheard by others and as such staff should avoid discussing confidential and sensitive patient information in open areas to ensure auditory confidentiality.

Our medical software is user-unique password protected. Authorised access via individual passwords has been granted on a role-specific basis.

11 How do we use document automation technologies?

Our practice has implemented a clinical information system that uses document automation technology to assist in our workflows and internal systems. Our selected medical software utilises document automation technologies so that documents drafted by us, such as referrals, contain only your relevant medical information.

These document automation technologies are established through our secure medical software built-in word processor. The built-in word processor allows the practice to set up automated, simple and computed variables. These automated variables are set up to strictly disclose only relevant medical information related to and required in the document selected.

12 Discarding of information

Whenever sensitive documentation is discarded, Central Highlands Healthcare uses an appropriate method of destruction, all personal information is shredded or disposed of in the blue secure document bin in front reception once entered in to the patient's file.

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

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have in writing either via our feedback section on our website, completing a feedback form in the practice or via email to enquiries@chhealth.com.au. We will then attempt to resolve it in accordance with our resolution procedure.

You may also contact the OAIC. Generally, the OAIC will require you to give them time to respond before they will investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992.

Alternatively, you can also contact the Office of the Health Ombudsman Queensland via telephone on: 133 646

14 Document Management

Document last updated: 22nd March 2024.

Document Review Date: 22nd March 2025