Deepdene Surgery Privacy Policy

Current as of: 2025

The objective of this document 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.

1. Who can I contact about this policy?

For enquiries concerning this policy, you can contact **Imogen Lovick-McGarry.**

2. When and why is your consent 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 outlined in this document, 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.

By acknowledging this Privacy Policy you consent to us collecting, holding, using, retaining and disclosing your personal information in the manners described below.

3. Why do we collect, use, store, and share your personal information?

The practice collects, uses, stores, and shares your personal information primarily to manage your health safely and effectively. This includes providing healthcare services, managing medical records, and ensuring accurate billing and payments. Additionally, we may utilise your information for internal quality and safety improvement processes such as practice audits, accreditation purposes, and staff training to maintain high-quality service standards.

4. What personal information is collected?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details
- medical information including medical history, medicines, allergies, and adverse reactions immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifier numbers
- health fund details.

5. Can you deal with us anonymously?

You can 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.

⚠

Dealing with general practices anonymously

The Privacy Act requires patients to be provided with the option of not identifying themselves, or of using a pseudonym, when dealing with a practice unless it is impracticable to do so. Information about this should appear in the practice privacy policy.

The Privacy Act 1988 requires practices to consider whether it is practical to give patients the option of not identifying themselves, or using a pseudonym. However, practices do not have to deal with patients anonymously or pseudonymously. The OAIC website provides further information in this topic here.

6. How is personal information collected?

The practice may collect your personal information in several different ways:

When you make your first appointment, the practice team will collect your personal and demographic information via your registration.

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.

In some circumstances, personal information may also be collected from other sources, including:

- 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 (if relevant).
- While providing medical services, further personal information may be collected via:
    - electronic prescribing
    - My Health Record
    - online appointments. Various types of images may be collected and used, including:

CCTV footage: Collected from our premises for security and safety purpose

- **Photos and medical images:** These can be taken using personal devices for medical purposes, following the guidelines outlined in our guide on using personal devices for medical images.

⚠

Compliance with privacy obligations

*To comply with Australian privacy obligations when collecting personal information from third-party sources, you must understand and adhere to the **Privacy Act 1988** and the **Australian Privacy Principles (APPs)** this includes:*

- verifying third-party compliance

- ensuring informed consent

- collecting only necessary data

- maintaining data accuracy

- updating your privacy policy and notifying patients of these updates as required

- protecting data with strong security measures

- facilitating individuals' rights to their data

- providing regular education and training for the practice team on privacy practices.

To ensure compliance, you can include the following line in the privacy policy:

"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."

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

We sometimes share your personal information:

- with third parties 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 (e.g. In referral letters)
- 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 it is a statutory requirement to share certain personal information (e.g. some diseases require mandatory notification)
- When it is provision of medical services, through electronic prescribing, 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.

8. 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 express consent. If you do consent, you may opt out of direct marketing at any time by notifying the practice in writing.

The Medical Board of Australia has requirements for advertising a regulated health service. If your practice is intending to provide direct marketing for patients please review the guidelines here.

9. How is your information used to improve services?

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

We may provide de-identified data to other organisations to improve population health outcomes. If we provide this information to other organisations patients cannot be identified from the information we share, the information is secure and is stored within Australia. You can let reception staff know if you do not want your de-identified information included.

At times, general practices are approached by research teams to recruit eligible patients into specific studies which require access to identifiable information. You may be approached by a member of our practice team to participate in research. Researchers will not approach you directly without your express consent having been provided to the practice. If you provide consent, you would then receive specific information on the research project and how your personal health information will be used, at which point you can decide to participate or not participate in the research project.

Definitions of de-identified and personal information

The RACGP Three key principles for the secondary use of general practice data by third parties defines de-identification as: the removing or altering information that identifies an individual or is likely to do so. Where information has been appropriately de-identified, it is no longer considered 'personal information' and can therefore be used or shared in ways that might not otherwise be permitted under the Privacy Act 1988 (Cwlth). A general practice can therefore lawfully share de-identified patient data without specific or express patient consent.

When personal information (i.e., data has not been de-identified) is requested by a third party, specific patient consent is usually needed, and the requesting entity will need to meet the requirements of a human research ethics committee.

Use of de-identified patient data

If the practice routinely provides patient health information to other organisations for secondary use the practice should make patients aware that this is occurring by including this information as part of the privacy policy. Practices should give patients assurances and advice on their rights and how their data is protected and must state the practice's approach to collection of healthcare information for primary and secondary purposes. Whilst patient consent for sharing de-identified practice data is not a legal requirement, it is good practice to have a procedure for ensuring patients who do not consent

to secondary use of data are removed from any data extraction process. Most data extraction tools have this functionality.

10. How are document automation technologies used?

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.

These document automation technologies are used through secure medical software Best Practice.

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.

All data, both electronic and paper are stored and managed in accordance with the Royal Australian College of General Practitioners Privacy and managing health information guidance.

11. How are Artificial Intelligence (AI) Scribes used?

The practice (some GPs) use an AI scribe tool to support GPs take notes during their consultations with you. The AI scribe uses an audio recording of your consultation to generate a clinical note for your health record. The practice AI scribe service is Heidi.

Heidi:

- does not share information outside of Australia
- destroys the audio file once the transcription is complete.
- removes sensitive, personal identifying information as part of the transcription

The practice will only use data from our digital scribe service to provide healthcare to you.

Use of artificial intelligence (AI) scribes

It is important practices understand the new and relatively high potential risks when considering the use of commercially available artificial intelligence (AI) scribes. Practices and GPs choosing to deploy AI scribes need to consider the implications both when selecting and using these tools.

The RACGP guidance on Artificial Intelligence (AI) Scribes provides more information on AI scribes.

GP's should also give individual patients the option to opt out of the use of AI scribes when required.

12. How is your personal information stored and protected?

Your personal information may be stored in various forms.

- Paper records
- Electronic Records

The practice stores all personal information securely.

- All paper records are secured in the vault under passcode
- Electronic records are password stored

All staff and personell have signed confidentiality/privacy agreements.

Our CCTV is recording are closed to the practice and are password protected onto the server.

- Parking lot
- Waiting room
- Entry way

13. How can you access and correct your personal information at the practice?

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

The practice acknowledges patients may request access to their medical records.

Formal requests for medical records must be made in writing and signed. Verbal consent will be taken as well to confirm.

The practice will respond to any requests to access or correct your personal information within a week.

The practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. Sometimes, we will ask you to verify your personal information held by the practice is correct and current. You may request we correct or update your information. To do this please contact via **Practice Manager recepion@deepdenesurgery.com.au.**

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

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have. We will then attempt to resolve it in accordance with the resolution procedure.

If you do not feel we have resolved your issue you may also contact the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner will require you to give them time to respond before they investigate. For further information visit **www.oaic.gov.au** or call the OAIC (Office of the Australian Information Commissioner) on 1300 363 992.

15. How is privacy on the website maintained?

At Deepdene Surgery, any personal information you share with us through website, email, and social media, is handled securely and confidentially. This practice uses analytics and cookies.

16. Policy review statement

Our privacy policy is regularly reviewed to ensure compliance with current obligations.

If any changes are made:

- They will be reflected on the website.
- Significant changes may be communicated directly to patients via email or other means.

Please check the policy periodically for updates. If you have any questions, feel free to contact us.