



PRIVACY POLICY

Introduction

The privacy policy is to provide information about how we collect, use and store the information you provide to the clinic. It also includes the circumstances we may be required to share information to a third party.

When you provide your personal information and register as a patient of Kings Park Clinic you give consent for our GP's and practice staff to access and use your personal information accordingly to provide you with healthcare. Only staff employed by Kings Park Clinic will be able to access your information and consent from you will be sought when asked for information about you from a third party.

All employees and contractors of Kings Park Clinic are able to access all patient information and are bound by strict confidentiality agreements.

Why we need your personal information

To manage your health appropriately we need to collect certain personal information. The information is used for healthcare, financial claims and payments, practice audits and accreditation.

What we need to know

To assist with your healthcare and claiming of refunds from Medicare or direct billing of some accounts we need to know.

- Your full name and date of birth
- Your contact address and contact details including contact details of a relative/friend we can contact in case of an emergency
- Medicare number for billing purposes and identification

We need you to disclose any medical information including history, medication use, allergies and any other information that may be relevant to your ongoing healthcare.

We only collect information that is needed for the services we provide.

What happens if you do not want to disclose your information.

If you do not disclose your personal information it will impact on our ability to provide you with the correct healthcare and it will impact our ability to claim Medicare benefits on your behalf.

How you can provide us with your information

When you make your first appointment at Kings Park Clinic, we will ask you to fill out a "New Patient Form." You can do this either at the clinic when you come in, you can download the document from our website, fill it in and bring it to your first appointment.



We will ask you to confirm your identity when you attend the clinic or phone the clinic, to identify we are speaking to the correct patient.

We may also collect information when you contact us by email or social media. Patients must understand the risks of unsecure emailing. It is encrypted when an email is sent on our end, although we are unsure if the receiving end is also encrypted. There is a risk that the information sent could be read by an unauthorised third party and/or sent to another email address. It is automatically assumed consent is given if the patient is to email us first.

If you are not able to provide information for yourself, we may ask for a guardian or responsible person to assist in providing information.

Other care providers may send us information about you, such as specialists, hospitals, allied health providers, community health services, pathology and diagnostic imaging services and this information will be added to your patient health file.

Information provided to other doctors or healthcare professionals

When information is to be sent to another health provider (e.g. a specialist doctor or allied health provider) your doctor will seek your consent in the context of a referral being made to the healthcare provider.

The doctor involved in your care will seek consent before uploading to your My Health Record or the electronic transfer of prescriptions.

Information provided to Third Parties.

Our policy around the provision of information to Third Parties is very strict. We will not disclose information of any kind to a Third Party without your consent, except in exceptional circumstances.

These may include;

- If you are at risk of harm without treatment and you are unable to give consent.
- If we are legally obliged to disclose information e.g. notification of infectious diseases, subpoena or court order, or mandatory reporting of child abuse.
- The information is necessary to obtain Medicare payments or other health insurance payments.

Your consent may be verbal or written directly to us.

Commonwealth Government Quality Improvement Initiatives.

Recent changes to Commonwealth Quality Improvement programs make it necessary for us to review and submit data as part of legislation. This Commonwealth legislation safeguards our data collection and the information we provide. Only information necessary to achieve the Quality Improvement Objective will be provided.



Artificial Intelligence

Our clinic uses AI to take notes, which means there is less writing of notes and more time focusing on patients.

Patient consent – The use of AI is a part of our clinic. Patient consent to use AI is essential and all clinicians are strongly encouraged to obtain consent before using AI. Patients can withdraw their consent at any time if they feel uncomfortable with our doctors using AI.

Securing information – We currently use Heidi as our AI platform; however, other platforms may be used. Heidi uses strict and robust controls and comply with Australian privacy laws. They use certified global standards like SOC 2 and ISO 27001, which ensures patients and practices the highest level of data security and confidentiality.

Data storing – While ensuring compliance with Australian data protection regulations, storing data locally in Australia is how they prioritise data sovereignty and enhance data security.

Data usage – Our clinic uses the data collected through AI to complete notes to streamline consultations to improve time spent. We only collect data that is essential to the quality of care we endeavour to provide. No recordings of these consultations are stored, only transcribed into computers notes, that are then added onto patients progress notes through our Practice Management System.



Computer Services and your health information

From time to time, we need to obtain the services of our IT Professionals; he will access our computers and only access areas as needed to rectify any IT issues we may have as well as upgrades. Our IT professionals are bound to a strict Non-Disclosure Agreement.

Protecting your personal information.

In the year 2000 we started storing our medical files as electronic records. Prior to that year all records had been stored in paper form. These paper records are still held at the clinic in a secure area, when not occupied the building is locked and protected by a monitored alarm system.

Our computer system has rigorous security systems in place with passwords and firewall security set by our IT professionals.

Our health records are kept for at least 7 years from the last time we have provided a health service to a patient if the patient is 18 years or older. If the service was provided to a patient under the age of 18 the records must be kept until the patient is 25 years old. This clinic does not destroy notes and currently patient records are held indefinitely in our secure storage area.

Accessing your personal information at Kings Park Clinic

Patients have the right to access their personal information. We understand that you may request access to your records. This can be done through a medical appointment with your doctor or if you require your records to be sent to another clinic we require the request in writing and there may be a fee for the collating and sending of notes.

Kings Park Clinic takes all steps to ensure your records are up to date. If you find any information we do not have correct we also appreciate your input into correcting your case notes. Please talk to your doctor during your consult to update your records.

Data Breaches

Data breaches are required by law to be reported to the Office of Australian Information Commissioner.

If you have any concerns about data breaches please write or email the Practice Manager at pracmanager@kingsparkclinic.com.au. Your concern will be handled promptly and responded to in a timely manner.

For further information on Data Breaches you can visit www.oaic.gov.au