Privacy Policy

PIONEER HEALTH ALBANY

Introduction

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.

Why and when your consent is necessary

When you register as a patient of our practice, you provide consent for our GPs and practice staff to access and use your personal information so they can provide you with the best possible healthcare. Only staff who need to see your personal information will have access to it. If we need to use your information for anything else, we will seek additional consent from you to do this.

Why do we collect, use, hold and share your personal information?

Our practice will need to collect your personal information to provide healthcare services to you. Our main purpose for collecting, using, holding and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (eg staff training).

What personal information do we collect?

The information we will collect about you includes your:

- names, date of birth, addresses, 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.

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.

Please be aware that should you choose to deal with us anonymously or under a pseudonym, you will be required to pay for consults in full and that no rebate will be payable through Medicare if you do not use the name on your Medicare card.

How do we collect your personal information?

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

- When you make your first appointment our practice staff will collect your personal and demographic information via your registration.
- During the course of providing medical services, we may collect further personal information. Information can also be collected through My Health Record, eg via Shared Health Summary, Event Summary or through a Discharge Summary via NACS.
- We may also collect your personal information when you contact us via 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. 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).

Otos Health, Better Consult Application and Heidi Health

At the practice, you may choose to utilise software which is owned and operated by a third-party provider that will allow you to provide information to your general practitioner prior to your consult.

Otos Health App

The information collected will be stored securely on Amazon Web Services (AWS) cloud platform, hosted in Sydney, Australia. The app is designed for the safe management of patient data and securely integrated with third party providers, including Deepgram and OpenAI. If your data is no longer required, it is permanently deleted from AWS servers.

For further information regarding the Otos Health application and its use, storage and disclosure of the personal information which it collects, please refer to their privacy policy.

Better Consult

The information collected by BetterConsult is stored in Australian data centres in accordance with the Australian Privacy Act . All identifiable patient information is stored encrypted, so no personal data can be revealed.

Information collected via the BetterConsult application is secured safely on your medical record and the application permanently deletes your responses.

For further information regarding the BetterConsut application and its use, storage and disclosure of the personal information which it collects, please refer to their privacy policy.

Heidi Health

Heidi is a transcription tool that doctors at Pioneer Health Albany utilise during patient consults to assist them to accurately capture medical information. Heidi is compliant with the Australian Privacy Principles and the Privacy Act. All data is encrypted and securely stored on servers located within Australia.

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

We sometimes share your personal information:

- with other healthcare providers
- when it is required or authorised by law (eg 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 (eg some diseases require mandatory notification)
- during the course of providing medical services,
- My Health Record (eg via Shared Health Summary, Event Summary)
- 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 the Australian Privacy Principles (APP) and this policy.

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.

Pioneer Health provides aggregated, de-identified health data to the WA Primary Health Alliance for population health review purposes. This data contains no information that is identifiable to an individual patient and is sent securely with encryption.

Pioneer Health participates in various research projects and provides de-identified health data in relation to research activities. All research activities have been granted ethical approval by the required Research Ethics Committee. You can opt out of participating at any time by advising our administration team.

How do we store and protect your personal information?

Your personal information may be stored at our practice in various forms. Our practice stores information as electronic records and archived paper records.

Our practice stores all personal information securely via the use of passwords, encrypted back-ups, confidentiality agreements for staff and secure cabinets.

All records will be retained until the earlier of 7 years from your last contact with the practice, or until you reach the age of 25.

Pioneer Health's server security policy is designed to protect the servers from unauthorized access, data breaches, and other security threats. Pioneer Health uses the following security measures to ensure the personal information which it holds is secured:

- Antivirus software is installed on all servers and updated regularly.
- Firewalls are configured to block unauthorized traffic.
- Servers are placed on their own subnet to prevent direct access from the workstation to the server.
- Access to servers is restricted to authorized users.
- Physical access to the servers are limited, with servers located in a locked room and security cameras installed around the building..
- Servers are patched regularly to fix security vulnerabilities.
- Backups are created regularly every hour onsite with daily offsite backups.

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. You can lodge this request either via email (admin@pioneerhealth.com.au) or telephone. Our practice will acknowledge your request within 3 business days. We can post the requested information to your postal address, or we can email the information to you in accordance with our Email Policy.

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, and you should make such requests in writing to admin@pioneerhealth.com.au

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. We will then attempt to resolve it in accordance with our resolution procedure. Complaints should be addressed to the General

Privacy Policy (cont.)

Manager, 2 Pioneer Road, Pioneer Health, Albany WA 6330 or admin@pioneerhealth.com.au. Alternatively, you can call the practice on 9842 2822. We will respond with acknowledgement of your complaint within 3 business days and have your complaint fully investigated within 30 business days.

You may also contact the Office of the Australian Information Commissioner (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.

Privacy and our website

If you "like" or comment on our Facebook page, we will have your social media name. No information is collected via our website unless you explicitly provide it (e.g. your email address).

Data breach

In the event of a privacy breach, the practice will respond in accordance with our Data Breach Response Plan.

Policy review statement

This privacy policy will be reviewed annually to ensure it is in accordance with any changes that may occur.

The Practice will:

- provide a copy of this policy upon request
- ensure staff comply with the APP and deal appropriately with inquiries or concerns
- take such steps as are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance with the APP and deal with inquiries or complaints
- collect personal information for the primary purpose of managing a patient's healthcare and for financial claims and payments.

The Practice staff will take reasonable steps to ensure patients understand:

- what information has been and is being collected
- why the information will be used or disclosed
- why and when their consent is necessary
- the Practice's procedures for access and correction of information, and responding to complaints of information breaches, including this privacy policy.