

Westgate Health Co-Op Privacy Policy

Current as of: July 2023

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 (e.g. 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.

How do 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.

Information can also be collected through My Health Record, e.g. via Shared Health Summary & Event Summary.

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)

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
- with third parties who are engaged by our practice to collect information for research, planning, teaching and evaluating the healthcare services we provide to our patients as well as our compliance with the National Co-Operative's Law (2013).
- 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 there is a statutory requirement to share certain personal information (e.g. some diseases require mandatory notification)
- during the course of providing medical services, through My Health Record (e.g. via Shared Health Summary, Event Summary).

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.

How do we store and protect your personal information?

Your personal information may be stored at our practice in various forms e.g., electronic records, visual records (X-rays, CT scans, videos and photos).

Our practice stores all personal information securely in electronic format. Our practice has systems in place to protect the privacy, security, quality and integrity of the data held. Appropriate staff are also trained in computer security policies and procedures and complete a Privacy, Confidentiality & Security Agreement upon employment.

GPs and staff have personal and complex passwords to authorise appropriate levels of access to health information. Screensavers or other automated privacy protection devices are enabled.

Antivirus software is installed and updated. All internet connected computers have hardware/software firewalls installed. Our disaster recovery plan has been developed, tested, and documented and data transmission of patient information over a public network is encrypted.

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 and our practice will respond within 30 days.

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 the Executive Officer, PO Box 11, Altona North 3025 or email us directly on info@westgatehealth.coop

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. For any concerns, please contact the Executive Officer at PO Box 11, Altona North 3025 ph. **(03) 9391-6777**. We will make every attempt to resolve the issue within 30 days of receipt of letter. Alternatively, you can choose to complete a feedback form and place in the suggestion box located at reception or email us directly on info@westgatehealth.coop

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 contact the Victorian Health Complaints Commissioner on **1300 582 113** or visit their website www.hcc.vic.gov.au.

Privacy and our website

Our practice also collects information via our website. To ensure the privacy of information our website uses traffic encryption, known officially as hypertext transfer protocol secure (HTTPS), which is a method of securing the transmission of information to and from a website. It ensures the security of website traffic by encrypting the information being transmitted, and by using security certificates to identify and authenticate the website. This is the same technology used by banks worldwide to secure their online banking sites.

Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. Any updates to this policy will be published on our website.