DR MARCIA MICKELBURGH PRIVACY POLICY

Current as of 30th August 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 Dr Marcia Mickleburgh's rooms, 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 Medical Practitioners, Clinicians, 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 /Veterans affairs 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.

Tracking & Cookies Data

We use cookies and similar tracing technologies to track the activity on our service and hold certain information.

Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyse our Service.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our service.

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, through electronic transfer of prescriptions (etp), My Health Record, e referrals and Shared Health Summary.
3. We may also collect your personal information when you visit our website, send us an email or SMS, or telephone us.
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
- 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)

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 is stored electronically at our practice.

Patient information is securely stored on servers in Australia, by Envisage IT
Envisage IT - Employs robust security measures to ensure the safety and integrity of the data stored on our servers. Here are some of the key security measures we have in place:

- Secure Server Infrastructure: We store your data on Microsoft Australia servers, which adhere to the stringent privacy legislation in place. This ensures that your information is handled with utmost care and compliance.
- Advanced Threat Protection: To safeguard against unauthorized access by malicious entities, we employ the XDR platform Crowdstrike. This cutting-edge technology actively monitors the systems and provides an additional layer of defense against bad actors.
- Encryption: Your data is encrypted both while at rest on the server and during transit. This ensures that even in the unlikely event of a breach, the information remains unintelligible to unauthorized individuals.
- Multi-Factor Authentication (MFA): The system is protected by MFA at all times. This means that access to the data requires multiple layers of authentication, minimizing the risk of unauthorised entry and enhancing the overall security of the systems.

Our practice stores all personal information securely, in password protected electronic format, all computers and programs are password protected.

Computers, printers and electronic devices and information contained on same, is not accessible, from reception or the waiting room area. Any paper documentation is kept away from the reception area and is shredded, after it has been transferred to the computer.

It is a condition of employment that all employees sign a confidentiality agreement.

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 7 working 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 our Practice Manager.

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. Please submit any complaints to the:

Practice Manager
Dr Marcia Mickelburgh
Level 1 207 Lake Street
CAIRNS 4870
P: 07 4281 6846
E: reception@drmarciamickelburgh.com.au

We will respond to your complaint within 5 business days.

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 Officer of the Australian Information Commissioner - OAIC on 1300 363 992

Data Breach

Should the practice become aware of a data breach, we will notify the individual whose personal information has been breached. This will provide a reasonable step in the protection of this information against misuse, loss, or unauthorized access. As a practice we will explain what went wrong and what has been implemented to avoid a repeat situation, as well as what has been done to remedy any potential harm We will help patients regain control of information e.g. change password and request re-issue of identifiers We will endeavor to regain public trust. We take the protection of our personal information seriously. Our data breach response includes notifying the patient.

Serious breaches will involve notifying the OAIC and relevant 3rd parties. If a patient believes there has been a breach of the Australian Privacy Principles (APP), in the first instance they should make the practice aware. If the patient is not satisfied with Practice response, they can lodge a complaint with OAIC (Office of the Australian Information Commissioner)

Phone 1300 363 992 – GPO Box 5218Sydney NSW 1001

Privacy and electronic communication

Emails

Patient information will only be sent via email if it is securely encrypted according to industry standards, (The Privacy Act 1988) and where the patient has consented to this form of direct communication. The following disclaimer is used for all practice emails.

(The information in this e-mail may be privileged and confidential, intended only for the use of the addressee(s) above. Any unauthorized use or disclosure of this information is prohibited. If you have received this e-mail by mistake, please delete it and immediately contact the sender)

Fascimile

Dr Marcia Mickelburgh uses Go Fax. Faxes are received directly into the email inbox, eliminating confidential faxes sitting in a fax machine .

All fax data stored with GoFax is encrypted at rest and in transit to/from GoFax to our line carriers.

GoFax is **ISO/IEC 27001 certified**

GoFax complies with the global information security standards for Information Security Management Systems (ISMS).

The following disclaimer is used for all practice faxes:
The information in this facsimile may be privileged and confidential, intended only for the use of the addressee(s) above. Any unauthorized use or disclosure of this information is prohibited. If you have received this facsimile by mistake, please delete it and immediately contact the sender.

ELECTRONIC CORRESPONDENCE

Dr Marcia Mickelburgh uses medical objects for Electronic correspondence (e.g. reports to referring Medical Practitioner, specialist referrals, specialist letters, results etc.)

Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. Updated copies of our Privacy Policy will be available in the waiting room and on our website.