Radio Doctor Illawarra privacy policy

Current as of: 15th December 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. This practice is bound by the *Federal Privacy Act 1998* and National Privacy Principles, and also complies with the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

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

As our healthcare services are provided as a rebateable Medicare Benefit Service (bulk billed) we require proof of your identity in order for us to claim for the services from Medicare. If services are provided on a private billing basis then under the Privacy Act you have the right to deal with us anonymously or under a pseudonym.

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. This includes information collected through face to face or telehealth consultations, electronic transfer of prescriptions and My Health Record.

- We may also collect your personal information when you send us a letter, email, 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).

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

We sometimes share your personal information:

- with your regular Medical Practitioner and other healthcare providers
- with your legal guardian or carer
- 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, through eTP and 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 APPs 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.
- Our practice may use de-identified personal information to improve the quality of the services we offer to our patients through research and analysis of our patient data.
- We may provide de-identified data to other organisations to improve population health outcomes. The information is secure, patients cannot be identified and the information is stored within Australia. You can let our reception staff know if you do not want your information included.

How do we store and protect your personal information?

Your personal information may be stored at our practice in various forms.

Patient Health Records are stored electronically within our practice management software and electronic medical record software including 'Medilink' and 'Connect'. Access to this software is protected at three levels by username and individual password for the computer and username and password to open the software and Two Factor Authentication. Connect also provides an audit log for all users of the system allowing tracking of individual user access and actions within the system.

Both active and inactive patient health records are kept and stored securely.

It is a condition of all consultations (including telehealth/telephone consultations) that no recording of these consultations is allowed and must not be stored or electronically transmitted.

Our practice stores all personal information securely. Practice computers and servers comply with the RACGP computer security checklist and we have a sound back up system and a contingency plan to protect the practice from loss of data. (Section 3 Information and IT security P & P)

Care is taken that the general public cannot see or access computer screens that display information about other individuals. Desktop computers are password protected at two levels and automated screen savers are set to display after 3 minutes of inactivity.

Members of the practice team have different levels of access to patient health information. (Refer Section 1.2 Information and IT Security P &P) To protect the security of health information, GPs and other practice staff do not give their computer passwords to others in the team.

Reception and other Practice staff are aware that conversations in the office or in a motor vehicle can be overheard and as such staff and contractors should avoid discussing confidential and sensitive patient information in these places.

Whenever sensitive documentation is discarded the practice uses an appropriate method of destruction by security bin and or shredding or computer drive, memory sticks etc are reformatted)

Correspondence

Electronic information is transmitted over the public network in an encrypted format using secure messaging software. Where medical information is sent by post the use of secure postage or a courier service is determined on a case by case basis. Items for collection or postage are left in a secure area not in view of the public.

Facsimile

Facsimile, printers and other electronic communication devices in the practice are located in areas that are only accessible to the general practitioners and other authorised staff. Faxing is point to point and will therefore usually only be transmitted to one location

All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver. Confidential information sent by fax has Date, Patient Name, Description and Destination recorded in a log. The practice uses a fax disclaimer notice on outgoing faxes that affiliates with the practice.

DISCLAIMER: The information contained in this facsimile message is intended for the sole confidential use of the designated recipients and may contain confidential information. If you have received this information in error, any review, dissemination, distribution or copying of this information is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original message to us by mail or if electronic, reroute back to the sender. Thank you. If you do not receive all pages, please call the sender at the above number.

Faxes received are managed according to incoming correspondence protocols

Emails

Emails are sent via various nodes and are at risk of being intercepted. Patient information is sent via email only to a private or known email address and is securely encrypted using SMIME certificate according to

industry and best practice standards. Our practice configures software so that the confidentiality and privilege notice is automatically added to each outgoing email.

"The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future. The contents of this email are the opinions of the author and do not necessarily represent the views of the Practice."

Our Security policies and procedures regarding the confidentiality of patient health records and information are documented and our practice team are informed about these at induction and when updates or changes occur. Each staff member is bound by a privacy clause contained within the employment agreement which is signed upon commencement of employment. Any private information given to unauthorised personnel will result in disciplinary action and possible dismissal.

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 using the 'request for personal health information form' available from the practice and our practice will respond within 14 days. A fee of $30 will be charged and must be paid at the time of application. Personal health information will not be released without receipt of the fee.

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 Administrative team enquiries@radiodoctor.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 including your name and mailing address. We will then attempt to resolve it in accordance with our resolution procedure. Complaints should be addressed to:

General Manager, Radio Doctor Illawarra, PO Box 214, Fairy Meadow NSW 2519 or by email generalmanager@radiodoctor.com.au Phone 02 4227 3251

A response will be provided to you within 30 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

Personal information is only collected where you provide the information through an online form. No other personal digital data is collected. De-identified website analytics including such things as website visits, pages viewed, time spent on page are collected.

Policy review statement

This policy will be reviewed on an annual basis and any updates will be provide on the website and available in the practice.