Plexus Medical & Cosmetic Privacy Policy

Current as of: Thursday 18th August 2022

All information collected by this practice is deemed to be private and confidential. The right of every patient is respected.

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.

What personal information do we collect?

The information we will collect about you includes:
• names, date of birth, addresses, contact details, next of kin, emergency contact, ethnicity and religion
• 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 will collect your personal information:
1. When you attend for your first appointment, our practice staff will collect your personal and demographic information via our registration form.
2. During the course of providing medical services, we may collect further personal information. We may also collect information through Electronic Transfer of Prescriptions (eTP) or MyHealth Record/PCEHR system
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 Veteran's Affairs (as necessary)

Who do we share your personal information with?

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 account keeping and billing purposes, including debt recovery
• 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)
• Complying with the requirements of the National Childhood Immunisation Register
• during the course of providing medical services, through Electronic Transfer of Prescriptions (eTP), MyHealth Record/PCEHR system (eg via Shared Health Summary, Event Summary).

Only people that 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.

Under no circumstances are members of the practice team to discuss or in any way reveal patient conditions or documentation to unauthorised staff, colleagues, other patients, family or friends, whether at the practice or outside it, such as in the home or at social occasions. This includes patient's accounts, referral letters or other clinical documentation.

General practitioners and other practice team members are aware of confidentiality requirements for all patient encounters, and recognise that significant breaches of confidentiality may provide grounds for disciplinary action or dismissal.

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. This may be in the form of your electronic patient record, paper records, pathology results, imaging results (such as X-rays or CTs) or finally, audio recordings.
Our practice stores all personal information securely. All the data within the practice management system which is password protected. All the information is backed up daily to a 'cloud' server based offsite at a

secure location. Backups are routinely tested to ensure daily duplication processes are valid and retrievable. At no stage will any information be used for the purpose of direct marketing.

How can you access and correct your personal information at our practice?

You have the right to access and correct your personal information.
Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing and make this to the attention of administrative staff and our practice will respond to your request within 30 days. You will not be charged for making a request however if results are required to be printed or photocopied, an administration fee will be charged.
Our practice takes all 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 up-to-date. You may also request that we correct or update your information, and you should make such requests in writing to the Practice Manager.
Where you dispute the accuracy of the information Plexus Medical & Cosmetic has recorded, you are entitled to submit a written request to the doctor to correct that information. Please be advised that the request and a note will be placed on your file but Plexus Medical & Cosmetic will not erase the original record. You will be notified once this correction has been made.

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 send all requests to:
• The Practice Manager, Plexus Medical & Cosmetic, 663 Chapel Street, South Yarra, VIC 3141
• All received letters will be acknowledged and a response will be sent to you within 30 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 OAIC on 1300 336 002.

Privacy and our website:

A copy of this privacy policy is also available on the Plexus Medical & Cosmetic website. Please feel welcome to visit www.ogam.com.au

This privacy policy is reviewed regularly to ensure it is in accordance with any changes that may occur. Plexus Medical & Cosmetic also endeavours to notify our patients wherever possible when amendments are made to this policy.

Australian Privacy Principles:

The Commonwealth Privacy Act was amended in 2012 and from March 2014 incorporates 13 Australian Privacy Principles (the APP's) that set out the rules for the handling of personal information in Australia. The APP's replace the previous National Privacy Principle (NPP).

In the interests of providing quality health care this practice has developed a privacy policy that complies with the privacy legislation and the APPs. The provision of quality health care is our principle concern. It requires a doctor patient relationship of trust and confidentiality. Your doctor regards patient health information as confidential and will only collect this information with patient consent.

A patient's personal information is handled in accordance with this practice's privacy policy and consistent with the privacy legislation. Patients are entitled to know what personal information is held about them, how and under what circumstances they may have access to it; why it is held; it's use; to whom and under what circumstances it may be disclosed; when consent is required for these purposes; and how it is stored.

Every effort will be made to discuss these matters with patient's at the time personal health information is collected from patient's attending this practice. Because there will be occasions when it is not practical to make patient's aware of these matters at the time of collection this document is designed to outline how this practice endeavours to protect privacy of patient's health information.

Correspondence:

There are risks associated with electronic communication in that the information could be intercepted or read by someone other than the

intended recipient. Email communications with other healthcare providers is undertaken securely through the use of encryption. Email communication with patients is discouraged; however, where initiated by the patient, the risks are communicated and patient consent is obtained.

Where patient information is sent by post, the use of secure postage or a courier service is determined on a case by case basis.

Incoming patient correspondence and diagnostic results are opened and viewed only by a designated practice team member.

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 team members. Faxing is point to point and will, therefore, usually only be transmitted to one location.

All facsimiles containing confidential information are sent only after ensuring the facsimile number dialled is the designated receiver before pressing ‘Send’.

Details of confidential information sent by facsimile are recorded in a designated logbook which incorporates the date of transmission, patient name, description of the contents and the designated receiver (name and facsimile number).

A copy of the transmission report produced by the facsimile is kept as evidence that the facsimile was successfully transmitted, and as evidence the information was sent to the correct facsimile number.

Facsimiles received are managed according to incoming correspondence protocols.

The words ‘Confidential’ are to be recorded on the header of the facsimile coversheet and a facsimile disclaimer notice at the bottom of all outgoing facsimiles affiliated with the practice.

Patient consultations:

Patient privacy and security of information is maximised during consultations by closing the consulting room doors. When the consulting, treatment room or administration office doors are closed, practice team members must ensure they knock and wait for a response prior to entering.

Where locks are present on individual rooms, these should not be engaged except when the room is not in use.

It is the general practitioner/healthcare team member's responsibility to ensure that prescription paper, patient health records and related personal information is kept secure if they leave their room during a consultation or treatment, or whenever they are not in attendance in the consulting/treatment room.

Patient health records:

The physical health records and related information created and maintained for the continuing management of each patient are the property of this practice. This information is deemed a personal health record and while the patient does not have ownership of the record, he/she has the right to access under the provisions of the Privacy Act 1988. Requests for access to a patient's health record will be acted upon only if the request is received in written format.

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

A patient health record may be solely electronic, solely paper-based, or a combination (hybrid) of paper and electronic records.