Marulan Medical Centre

Privacy Policy

1. Overview

We respect your privacy and are committed to protecting the confidentiality of your personal information. We are also committed to practicing good privacy governance and to ensuring our information handling and collection practices comply with the *Privacy Act 1988* (Cth) (**Privacy Act**), the Australian Privacy Principles constituted under the Privacy Act (**APP's**) and the *Health Records and Information Privacy Act 2002* (NSW) (**Health Records Act**). This Privacy Policy outlines how personal information (including health information) is collected, stored, used and disclosed by Marulan Medical Centre Pty Ltd ACN 099 052 963 (**Marulan Medical Centre, we, us** or **our**). This Privacy Policy also provides information on how you can access and correct the information we hold about you and our complaints process.

Please read this statement carefully and contact us if you have any questions.

2. The types of personal information we collect and hold

(a) Personal information is information or an opinion about you or from which you can be reasonably identified.

(b) The types of personal information we collect includes:

(i) information about your private or family life such as your name, signature, home address, email address, telephone number, country of birth, date of birth, your family history and lifestyle factors;

(ii) information about your working habits and practices such as your employment details and job title;

(iii) recordings of your image on Closed Circuit Television (CCTV) footage; and

(iv) sensitive information such as information about your health or mental health (including notes about the symptoms you describe or your doctor's observations and opinions of your health, prescription information, contact and billing details, test results and reports, your Medicare number), your health history, ethnicity, sexuality or religion (**Health Information**).

(c) We collect personal information:

(i) from patients and prospective patients – when they make an enquiry, book an appointment, attend our practice, access our website, subscribe to our newsletter, and/or at any other time from time-to-time in the course of providing our services;

(ii) from third party service providers – when they are engaged to supply services to us, provide information to us or invoice us for the provision of services;

(iii) when we receive enquiries through our website and when the website is otherwise accessed or used;

(iv) when we receive enquiries via email or telephone.

(d) The kind of personal information we may collect will depend on who you are (e.g. a client or third party service provider) and the nature of your interaction with us.

(e) Unless required or permitted by law, we will only:

(i) collect your personal information if it is reasonably necessary for us to carry out our functions or activities (such as diagnosing or treating your illness);

(ii) collect your Health Information if:

(A) that information is reasonably necessary for us to carry out our functions or activities; and

(B) you have consented to us doing so.

3. Cookies

Our website www.marulanmedicalcentre.com.au may use “cookies”; technology to store data on your computer or browser. Many websites do this because cookies allow the website publisher to do useful things like find out whether the computer has visited the site before. You can modify your browser to prevent cookie use – but if you do this our service (and our website) may not work properly. The information stored in the cookie is used to identify you. This enables us to operate an efficient service and to track the patterns of behaviour of visitors to the website.

In the course of serving advertisements to the website (if any), third-party advertisers or ad servers may place or recognise a unique cookie on your browser. The use of cookies by such third party advertisers or ad servers is not subject to this Privacy Policy, but is subject to their own respective privacy policies

4. What happens if you don’t consent to us collecting your personal information?

You can choose not to provide us with your personal information or Health Information. However, this may prevent us from providing you the assistance or services you require or from otherwise interacting with you.

5. Can you use our services anonymously or pseudonymously?

we are not obliged to provide services to individuals who do not identify themselves or use a pseudonym if it is impractical to do so or otherwise inconsistent with our obligations under any law.

6. How we collect and hold your personal information

6.1 How we collect your personal information

(a) We will always use fair, reasonable and lawful means to collect your personal information.

(b) We will only collect your personal information directly from you. Occasionally, we may collect your personal information from a third party such as another health service

provider, a member of your family or your carer but only if it is unreasonable or impractical for us to collect the information directly from you.

6.2 How we hold and protect your personal information and Health Information

(a) We hold your personal information in your medical record, in both hardcopy and encrypted electronic forms in secure databases that we own and operate or that are owned and operated by our service providers.

(b) We have implemented security measures to protect personal information we hold about you from misuse, loss, unauthorised access, modification or disclosure. These measures include:

Virus software including firewalls, Individual password protection, locked storage areas out of public view, numbered filing system rather than alphabetic for the provision of greater security, Physical files are never out of direct view of staff

Access privileges to networked PCs, and in particular clinical and billing software, is granted on a 'need to know' basis.

The Internal Systems Administrator is responsible for assessing, approving and reviewing what privileges should be assigned to each doctor and staff member. The Internal Systems Administrator is also responsible for assigning access privileges for each doctor and staff member. Doctors and staff are required to log out of their systems while away from their PCs.

Passwords

To prevent unauthorised access, passwords will be used for the practice's network and its programs. Software is configured so that there is a limit to the number of incorrect passwords that can be entered. Doctors and staff members will be responsible for all computer transactions made with his/her user ID and password.

Passwords will be changed if another person knows them. If doctors or staff members are unable to change their own passwords, they will advise the Internal Systems Administrator.

Doctors and staff are required to choose passwords that are difficult to guess and are at least six characters in length. Password-protected screen savers will be used, and screen-savers will automatically initiate after 3 minutes of inactivity.

Doctors and staff must not disclose a password to a computer technician who is working on the practice's system. If required, the staff member is to log-on on the technician's behalf or the Internal Systems Administrator will create a temporary account if the work is likely to take some time or involve a number of log-ons.

The Internal Systems Administrator will immediately revoke doctor or staff member passwords when they leave the employ of the practice.

To avoid loss of data, it is the policy of this practice that data held on the practice's computer system is backed up on a regular basis and that these backups are periodically tested to verify they can be restored if necessary. Backup media is rotated before being used. Media are stored securely when in use and destroyed when no longer used.

Backups and backup media are the responsibility of the *Internal Systems Administrator*.

Backups are performed every day the practice is open and are usually performed overnight by our external system administrator.

Scheduled Backup

This practice performs backups using scheduling software to automatically initiate and perform the backup (ie. backups are performed without the need for human intervention). It is the responsibility of the reception staff member nominated by the *Internal Systems Administrator* to remove the previous days backup media, replace it with the current days backup media, ensure the computer being backed up is left logged on, has no programs open and is left in a secure state before the scheduled backup. It is the responsibility of the reception member nominated by the *Internal Systems Administrator* to take the previous day's backup media off-site and return the previous backup media to the on-site secure location.

This practice overwrites existing data on the media with each new backup and always performs a full backup, regardless of whether the files have been changed or not.

Backup Testing

Backup logs are checked on a daily basis and any problems reported to the *Internal Systems Administrator*.

Trial Restore and backup is undertaken by Onsite Computer professionals by the use of shadow protect software. Information is backed up in 100megabyte chunks which are then checked to ensure they're not corrupted. A new volume is done daily using this procedure. Computer Care is advised if there is a problem and they will take the necessary steps to rectify this.

Anti-Virus Management

This practice uses AVG anti-virus software on all computers. The anti-virus software is initiated on start-up and runs in the background to provide continuing protection. The *Internal Systems Administrator* will be responsible for ensuring anti-virus software is updated and distributed promptly. The frequency of updates will depend on the software manufacturer's releases, but are to be kept up-to-date to prevent or minimise damage and data loss to the practice's systems and prevent computer viruses from spreading to other systems via infected e-mail or media.

Your treating doctor may hold their own separate medical record about you.

7. How do we use your personal information?

(a) We only use your personal information for the primary purpose for which it was collected. We may use your personal information for purposes other than the primary purpose but only if we are required or permitted by law to do so.

(b) Some ways we use your personal information are:

(i) to provide you with health care services;

(ii) to communicate with you;

(iii) to communicate with Medicare and other government agencies;

(iv) to communicate with your insurer;

(v) to perform accounting, billing and other administrative and operational functions; and

(vi) to comply with any legal requirements.

8. Disclosure of your personal information

Disclosure of patient health information to a responsible person

The *Privacy Act 1988* permits an organisation to disclose necessary health information to an individual's responsible person (such as a carer), providing:

- it is reasonably necessary, in the context of providing a health service to that individual
- the individual is physically or legally incapable of consenting or communicating that consent.

If a carer is seeking access to a patient's health information, it is a good idea to seek advice from your medical defence organisation before giving the carer access to the information.

8.1 To whom do we disclose your personal information?

(a) We only disclose your personal information for the primary purpose for which it was collected. We may disclose your personal information for purposes other than the primary purpose but only if we are required or permitted by law to do so.

(b) Some third parties to whom we disclose your personal information are WITHOUT THE EXPRESSED PERMISSION OF THE PATIENT

(i) to government and law enforcement agencies;

(ii) an immediate member of your family;

(iii) private health insurance providers;

(iv) Medicare Australia;

(v) to other health care professionals and providers; and

(vi) to our service providers.

8.2 Do we disclose your medical records to interstate or overseas recipients?

INFORMATION IS NOT SHARED WITH PARTIES OUTSIDE NSW WITHOUT THE EXPRESSED PERMISSION OF THE PATIENT

9. Direct marketing

(a) Direct marketing means using your personal information to contact you via the phone, SMS or email to promote our services.

(b) You acknowledge that by providing us with your personal information we may contact you to promote and market our services.

(c) We will never use or disclose your sensitive information, including your health information, for direct marketing purposes unless we have received your explicit permission to do so.

(d) You can opt-out at any time from being contacted by us for direct marketing by emailing "unsubscribe" to recpetion@marimamedical.com.au

Access and correction of your personal information

(e) You can make a request for access to or correction of personal information we hold about you by…

Access, corrections and privacy concerns

The Practice acknowledges patients may request access to their medical records. Patients are encouraged to make this request in writing, and the Practice will respond within a reasonable time.

The Practice will take reasonable steps to correct personal information where it is satisfied they are not accurate or up to date. From time to time, the Practice will ask patients to verify the personal information held by the

Practice is correct and up to date. Patients may also request the Practice corrects or updates their information, and patients should make such requests in writing.

The Practice takes complaints and concerns about the privacy of patients' personal information seriously. Patients should express any

privacy concerns in writing. The Practice will then attempt to resolve it in accordance with its complaint resolution procedure.

Resources

Compliance indicators for the Australian Privacy Principles: An addendum to the computer and information security standards (Second edition) www.racgp.org.au/ehealth/privacy

RACGP Computer and information security standards (CISS) and templates (2013) www.racgp.org.au/your-practice/e-health/protecting-information/ciss/

The RACGP Privacy handbook & patient pamphlet www.racgp.org.au/ehealth/privacy

10. SEE Access corrections and privacy concerns

(a) We will endeavour to give you access to your personal information in the way you request. However, we may give you access to your personal information in a different way if the way you want to access your personal information is unreasonable or impractical.

(b) In certain circumstances, we may not give you access to your personal information or correct your personal information. In these circumstances, we will write to you to explain why we cannot comply with your request.

(c) We will try to grant or refuse your request for access within 30 days of receiving your request. It may however take us longer than 30 days to respond to your request. For example, a request relating to personal information achieved in a secure off-site storage area may take longer to respond to than requests about electronically stored information.

(d) While we will try to give you access to your personal information for free, we may charge you a fee to cover costs we incur in giving you access to your personal information. For example, we may charge you for costs we incur in retrieving your personal information or postage and photocopying costs.

11. Complaints

(a) If you believe your privacy has been breached or you have a complaint about our handling of your personal information, please contact us using the details provided below.

(b) We take privacy complaints seriously. If you make a complaint, we will respond within a reasonable time to advise you of the person responsible for managing your complaint. We will try to resolve your complaint within 30 days. When this is not reasonably possible, we will contact you within that time to let you know how long we will take to resolve your complaint.

(c) We will investigate your complaint and, where necessary, consult with third parties about your complaint. We will decide about how to address your complaint and write to you to explain our decision.

(d) If you are not satisfied with our decision, you can refer your complaint to the Office of the Australian Privacy Commissioner and/or to the Office of the Information and Privacy Commissioner. Details about how to file a complaint can be found at www.oaic.gov.au or www.ipc.nsw.gov.au.

12. Changes to this policy

This Privacy Policy forms part of the agreement between you and us (either in your capacity as a patient/prospective patient or a third party service provider). We may, from time to time, amend this Privacy Policy, in whole or part, in our sole discretion. Any changes to this Privacy Policy will be effective immediately upon the posting of the revised Privacy Policy on our website. Depending on the nature of the change, we may announce the change on our website home page or by email (if we have your email address). However, in any event, by continuing to use the website and/or our service following any changes, you will be deemed to have agreed to such changes. If you do not agree with the terms of this Privacy Policy, as

amended from time to time, in whole or part, you must terminate your use of the website and inform us immediately prior to any further receipt of our services.

13. Contact us

All questions or queries about this Policy and complaints should be directed to the Marulan Medical Centre Privacy Officer, whose details are:

Contact Name: The Privacy Officer - Nadia Kitching

Email: practicemanager@marulanmedicalcentre.com.au

For further information on your privacy rights, go to: www.privacy.gov.au

For further information on the Health Records Act, go to: http://www.ipc.nsw.gov.au/hrip-act