Remote Rhythm Management Pty Ltd Privacy Policy

Introduction This privacy policy is to provide information to you, our client, on how your personal information (which includes your health information) is collected and used within our company. When you register as a client of our service, you provide consent for our staff to access and use your personal information, so they can provide you with the best possible device monitoring. Only staff who need to see your personal information will have access to it.

Why do we collect, use, hold and share your personal information?
Remote Rhythm Management (RRM) will need to collect your personal information to provide cardiac device monitoring to you. The main purpose for collecting, using and holding your personal information is to manage your cardiac device. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes.

What personal information do we collect?
The information we will collect about you includes your:

- names, date of birth, addresses, NOK/alternate person contact details
- medical information including medical history, previous tests and procedures, medications, allergies, adverse events, and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifiers and health fund details.

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 company may collect your personal information in several different ways.

1. Our company staff will collect your personal and demographic information via methods such as telephone, from a referral or on completion of our patient registration form.
2. During the course of providing medical services, we may collect further personal information.
3. We may also collect your personal information when you send us an email or SMS, 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 GP's, specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
- your health fund, Medicare, or the Department of Veterans' Affairs.

When, why and with whom do we share your personal information?
We sometimes share your personal information:
• with other healthcare providers/hospitals
• with third parties who work with our practice for business purposes, such as accreditation agencies, information technology providers or collection of outstanding accounts via a third party – these third parties are required to comply with Australian Privacy Principles and this policy

Other than in the course of providing monitoring 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 without your consent. (unless under exceptional circumstances that are permitted by law).
Our company will not use your personal information for marketing any of our goods or services.

Your personal information is stored at our company electronically. Remote Rhythm Management takes all reasonable steps to ensure information security. We employ methods such as: complex login passwords and confidentiality agreements for all staff and contractors. Remote Rhythm Management software is hosted by Servers Australia. https://www.serversaustralia.com.au/

Servers Australia currently utilises NSFocus for our DDoS mitigation. From Servers Australia website: *These are physical appliances specifically designed to identify and filter DDoS attacks. Unlike other anti-DDoS products that rely on null routes, traffic thresholds, and packet limits to mitigate DDoS attacks, NSFOCUS ADS uses a multi-stage inspection and analysis process that combines RFC checks, protocol analysis, access control lists, IP reputation, anti-spoofing, L4-L7 algorithmic analysis, user behavior analysis, regular expressions, connection/rate limiting, and more to mitigate attacks.These devices are currently deployed in our Sydney and Melbourne POP's. Additionally we have partners upstream to mitigate DDoS in other locations. In the event that we are not able to mitigate an attack at our network level, we will request our upstream providers to do mitigation, where we have paid contracts in place to clean large and small attacks. In the event that we cannot clean a very large DDoS attack, then we will unfortunately have to Black Hole the IP or shut the service down temporarily.*

Servers Australia is very proud to be able to mitigate some of the largest DDoS attacks

that have been destined to Australian sites hosted on our network, and our aim is to be able to keep clients online during an attack.

This comprehensive approach leads to the lowest rates of both false positives and negatives as compared to any other technology. Not only is it highly accurate, it is also highly effective at mitigating DDoS attack traffic.

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

Any concerns regarding privacy should be expressed in writing to the Manager at: Remote Rhythm Management, PO Box 154 Elsternwick VIC 3185
We will acknowledge your communication as soon as possible and give a time frame (up to 30 days) for when to expect an answer. 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.

RRM may review and amend this privacy policy annually or as required to ensure we are compliant with privacy laws and any other changes that may occur.