DEAKIN MEDICAL CENTRE

135 Deakin Avenue
Mildura Vic 3500

Phone: 03 5022 1488
Fax: 03 5023 6838
www.deakinmedical.com.au

Deakin Medical Centre – Cyber Incident

On 10 June 2025, we discovered that Deakin Medical Centre was involved in a pending data leak on a web site called Ransom Look. Upon investigation from our IT provider, it was discovered that an account password was compromised and access to the Remote Desktop Gateway Server was gained via the account and data was downloaded from the server.

Our IT provider and antivirus software blocked the IP address where the ransomware was detected. The majority of this data was business data and not related to patients, and the breach did not involve our Practice Management Software, which is where patient health records are securely stored. Our IT provider continued to monitor our systems, but no other malicious activity occurred. We are aware that the data was released on 11 June 2025.
Deakin Medical Centre's system has since been secured and notifications have been issued to the Office of the Australian Information Commissioner and any individuals likely to have been affected.

We would like to reassure all patients that Deakin Medical Centre does not transfer medical records via email and all patient records are secured within a secure patient management system. Access to this patient management system is separate to the email accounts and there was no unauthorised access to the patient management system.

Queries

If you have any queries, please contact us at pm@deakinmedical.com.au
Deakin Medical Centre takes cyber security and privacy of personal information seriously, and we remain highly alert and continue to monitor our systems for signs of any suspicious activity.

Protection against theft of personal information

We have taken the cautious approach and have outlined some simple steps below that you can take if you have any concerns:

Check your bank account statements for suspicious activity and contact your bank if you see any unusual activity. If necessary, discuss options with your bank regarding replacement cards as required.

Contact IDCARE - Australia's national identity and cyber support community service. They have expert Case Managers who can work with you in addressing concerns in relation to personal information risks and any instances where you think your information may have been misused. IDCARE's services are at no cost to you. If you wish to speak with one of their expert Case Managers, please complete an online 'Get Help' form at https://www.idcare.org/contact/get-help, or call 1800 595 160 (Monday to Friday 8am – 5pm AEST excluding public holidays).

Obtain a free credit report to identify whether there is any suspicious activity on your bank accounts (for example, Equifax credit reports are available at https://www.equifax.com.au/personal/products/credit-and-identity-products).

Ensure that you have sufficiently complex passwords on your computer systems, your email and your social media accounts.

Ensure that you have up-to-date anti-virus software and any recommended software patches installed on your computer systems.

Visit Scamwatch (at https://www.scamwatch.gov.au/) to keep up with current scam trends.

Kind Regards,
Directors of Deakin Medical Centre