

Fact sheet

Data Breach Information Sheet

January 2026

This information sheet is provided to assist people affected by the RivMed data breach to understand what has happened, what we have done, and what options are available. The nature of the information that has been taken means you may be at risk of scams.

What support is available?

DCJ is working with ID Support NSW (**'ID Support'**), an identity and cyber security support service, to assist anyone affected or concerned about the potential misuse of their personal information.

ID Support can provide personalised advice and support to help reduce the risk arising from a data breach. ID Support is a free service.

If you believe that you, or members of your family or household, may have been affected by this breach, please contact ID Support.

To access free support, call ID Support on 1800 001 040. The ID Support team is available Monday to Friday from 9am to 5pm.

Help in languages other than English

This is important information about your privacy.

If you need assistance translating this information, please call ID Support on 1800 001 040 Monday to Friday from 9am to 5pm. ID Support will connect you with an interpreter.

What should I do?

You need to be aware that scammers may try to capitalise on this incident, for example, by claiming to be from NSW Government agencies.

You should stay alert for fraudulent e-mails, letters, phone calls, and text messages.

We've briefly outlined some general precautions that you can take to protect your personal information below.

- Use long, complex passwords, especially for online services such as banking, email, and social media. You should change and strengthen your passwords if you currently use the same password for multiple accounts and services.

- Implement multi-factor authentication on digital services where available. For example, where you receive an additional code sent to your phone by SMS before you can log into your account.
 - Don't open messages or click links if you don't know the sender or if you're not expecting the message (phishing emails).
 - If you believe that your personal information has been misused (for example, as part of a scam, identity theft, or fraud), we recommend that you contact the NSW Police Force and ID Support using the details given above.
-

What actions have been taken?

On 14 January 2025, DCJ was notified of a suspected data breach affecting Riverina Medical and Dental Aboriginal Corporation ('RivMed') where a threat actor accessed a RivMed employee's system and downloaded a number of documents in October 2024. The incident was identified by Cyber NSW, which located documents relating to RivMed on the dark web.

RivMed first advised the community of this incident on 26 February 2025. RivMed has also notified medical and dental clients who were affected by this breach.

DCJ and RivMed acted immediately to contain and investigate the incident, including:

- taking steps taken to ensure the data is not made publicly available.
- continued monitoring of the web and dark web.
- reporting the incident to the NSW Police Force for investigation.

Since the incident occurred, DCJ has been continuously monitoring for any indication that personal information has been published or shared, and we can confirm there is no evidence of this.

RivMed and DCJ's investigations are now complete. We are contacting you so you can take the appropriate precautions and, if needed, access various support services.

If you are not satisfied with our response

You may also lodge a privacy complaint or an application for privacy internal review with DCJ.

Visit [Privacy complaints and internal review](#) or [DCJ's Privacy Management Plan](#) for more information and to lodge a complaint or review.

When emailing or corresponding with DCJ about this data breach, please put "**RIVMED**" in the subject line of your email.

DCJ acknowledges the seriousness of this incident and regrets any distress or inconvenience you may experience. We are committed to ensuring that best practice standards and legal obligations are met in the management of personal information.