30 July 2025

This statement provides an update on a cyber incident that occurred in April 2023 involving the unauthorised access of personal information held by HWL Ebsworth in relation to certain NDIS participants, prospective participants, their families and carers, and staff who were involved with NDIA legal matters represented by HWL Ebsworth. This statement does not relate to a new or different event.

Why are we publishing this statement?

The NDIA has an obligation under the *Privacy Act 1988 (Cth)* to notify any individuals potentially impacted by this cyber incident. The NDIA has notified all affected individuals who it has been able to identify and for whom the NDIA holds current contact details.

However, the NDIA has been unable to notify some individuals because it has either not been able to identify them or the NDIA does not hold their current contact details. These individuals are not NDIS participants but may be either a former participant, or related to a current NDIS participant, or someone who had previously applied for access to the NDIS.

The information about these individuals that was disclosed during the cyber incident involved details such as:

- Name
- Signature
- Date of birth
- Phone number
- Address
- Email address
- Health information
- Disability information
- Medical records/Medical reports
- Employment details
- Bank details

We would also like to reassure everyone that this will not impact any participant's ability to receive services and that participants can continue to receive their disability supports in the usual way.

The NDIA is continuing to actively monitor and investigate the cyber incident.

The NDIA recognises that news of the cyber incident may be distressing and concerning for

participants, families, carers and supporters. We sincerely apologise for this.

What can you do?

If you suspect that you or someone you know falls within the category of persons identified above, we recommend you take, or advise the person you know to take, the following actions to help reduce the risk of harm associated with the unauthorised disclosure of personal information:

- Stay alert to increased scam activity, particularly email and SMS or telephone phishing scams. Contact Scamwatch for information about how to recognise, avoid and report scams.
- The NDIA will never ask participants or their representatives for personal details by SMS. Do not click on any suspicious links or provide your passwords or any personal information to anyone you do not know. Always refuse any unprompted request from an individual to access your computer even if they say they are from a credible organisation.
- Consider changing your online account passwords. The Australian Cyber Security Centre has guides on good password practices.
- Enable multi-factor authentication for your accounts where possible. This means using extra checks to prove your identity.
- Install up-to-date anti-virus software on any devices you use to access your online accounts.
- Monitor your bank account transactions and check your credit report to see if it has any unauthorised loans or applications.
- The Office of the Australian Information Commissioner has general information about how to respond following a data breach. It also has information on ways to protect your privacy.

Further information about the actions you can take to reduce the risk of harm from a data breach can be found on our website at the Protecting your personal information after a data breach webpage.

There is no need to contact us. However, if you wish to contact us about this incident, please contact us at 1300 216 807 (Monday to Friday, 9:00am to 6:00 pm AEST) or NOTIFICATIONS@ndis.gov.au.

Background

The NDIA released a statement on 25 July 2023 in relation to the cyber incident involving HWL Ebsworth.

Related articles

Category

- News

November 2023 data breach: an update from the NDIA

Date
23 September 2024
Category

- Fraud and compliance
- News

HWL Ebsworth data breach update

Date
25 July 2023
Category

- News

NDIA detects data breach

Date
28 November 2023
Read more news