The National Disability Insurance Agency (NDIA) has developed NDIA application programming interfaces (APIs) for:

- registered providers
- plan managers
- software developers.

These NDIA APIs allow controlled and secure access to specific NDIA data, for approved entities in support of the delivery of services to NDIS participants. It is everyone's responsibility to protect the confidentiality, integrity and availability of NDIS data when they gain access to the APIs.

We will approve access to the APIs based on the:

- type of entity requesting access
- cyber security maturity of the entity.

If you want to access the NDIA APIs, you should contact the NDIA Digital Partnership Office (DPO) at dpo@ndis.gov.au before you apply.

Do not fill out any documents or start the cyber assessment before you contact us. This helps to reduce any delays to the process.

Applying for access to these APIs does not guarantee we will grant you access.

Direct integration process

The process to apply for direct integration is as follows:

1. Download and complete the Digital Provider questionnaire

- NDIA Digital Providers Questionnaire (DOCX 110KB)
- NDIA Digital Providers Questionnaire (PDF 223KB)

2. Provide the evidence needed in the cyber clearance framework

- Cyber Clearance Document (DOCX 64KB)
- Cyber Clearance Document (PDF 196KB)

3. Provide a copy of your planned architecture to connect to the NDIA APIs.
4. Complete a current ASIC company extract. You can buy this on the ASIC website . The date on the current company extract should be within 4 weeks of the date you provide these documents to us.

5. Read, understand and sign the terms and conditions.

- NDIA API Terms and Conditions (DOCX 39.3KB)

You must send all completed documents and evidence to the DPO.
You can do this via:

- email
- by hard copy to:

Attention: Digital Partnership Office
National Disability Insurance Agency
GPO Box 700
Canberra ACT 2601

When you apply

We will start assessing your application when we receive all the required documents.

We use the company extract to confirm the signing authorities (registered Director/s and Secretaries) on the terms and conditions.

If you sign the terms and conditions under a Power of Attorney, or alternative signing authority, you must include a copy of the supporting evidence.

If required, entities may request the release of data under a Non-Disclosure Agreement
.
We may ask for further information, subject to your application.

We will work with you to finalise the architectural review and cyber clearance process.

Software developers or aggregators must partner with a registered provider if they want to access the NDIA APIs. They will also need to complete additional cyber security activities.

API testing

Entities must test against ALL NDIA APIs regardless of their individual requirements.

Once the cyber clearance processes have started, the DPO, at its discretion, may allow entities to start API testing early.

Early testing does not mean that the NDIA has approved your application.

Standards

Entities must meet the following standards to connect to the NDIA APIs:

1. You must agree to the standards detailed in api.gov.au.
2. You must have a suitable ICT certification for their ICT Systems as specified in the cyber clearance framework e.g. ISO 27001:2022.
3. You must have an appropriate level of cyber security maturity.
4. Where appropriate, you must display secure coding practices.
5. Where appropriate, we may require penetration testing.

Transitioning in

If your application is successful, we will send you a technical pack with:

- Onboarding guide.
- NDIA Provider Digital Access (PRODA) step-by-step guide API connect.
- PRODA B2B software developers guide.

You can then register for a PRODA test account. The instructions are in the technical pack.

We will email you a link so you can activate your account in the vendor developer portal. You can then read the API specifications in the portal.

To help with the process, please communicate with us in a timely and accurate way. If you have any questions, please email the DPO.

Indirect integration

Indirect integration is for registered providers who would like to connect with our APIs through a software developer or aggregator.

The process for indirect integration is as follows:

1. Registered provider connects with an aggregator who is an existing digital partner.
2. The aggregator submits an application to the DPO.

The application must include the following information:

- Registered provider details (ABN, provider number, address, email, telephone).

- A primary contact.
- Data residency information (stored within Australia).
- Signed declaration with signatures from the registered provider and aggregator.

The DPO will then complete a technical review. The DPO will contact the aggregator about the outcome of the application.

Further information

For more information, please contact dpo@ndis.gov.au

This page current as of
19 June 2024