

Response to the 2023 Privacy Impact Assessment

National Disability Data Asset and Australian National Data Integration Infrastructure

The Department of Social Services is working with the Australian Bureau of Statistics (ABS) and Australian Institute of Health and Welfare (AIHW) to create the National Disability Data Asset. We call these 3 Australian government agencies the Commonwealth Partners.

States and territories and the disability community are also involved in developing the disability data asset. The [National Disability Data Asset Council](#) (the Council) oversees the uses of the disability data asset. It involves shared decision making across government and the disability community. The disability data asset brings together de-identified information from different government agencies about all Australians to better understand outcomes for people with disability.

The underlying system that supports the disability data asset is the Australian National Data Integration Infrastructure. This system allows us to connect and analyse data in the disability data asset. The Australian National Data Integration Infrastructure Board (the Board) oversees the delivery and use of this system.

More information is on the [National Disability Data Asset website](#), including about [Privacy for the National Disability Data Asset](#).

What is a Privacy Impact Assessment?

This document is a response from the Commonwealth Partners to the recommendations from the 2023 Privacy Impact Assessment (PIA).

A PIA is a review of a project and how it might affect privacy. A PIA suggests ways to manage, reduce or remove privacy risks and impacts.

Privacy experts at Maddocks did a PIA for the disability data asset and its underlying system.

The Commonwealth Partners and Maddocks consulted with stakeholders for the PIA between March and July 2023. Maddocks wrote a detailed consultation report about the feedback.

Summaries of the PIA and consultation reports are on the National Disability Data Asset website at [Privacy for the National Disability Data Asset](#).

The Commonwealth Partners plan to update the PIA in 2025.

The assessment process

The 2023 PIA:

- checks the disability data asset and underlying system is in line with the [Privacy Act 1988](#), including the [Australian Privacy Principles](#) – these are the laws about how to manage personal information
- notes any privacy risks and ways we can reduce risk

- helps us to manage any privacy risks and impacts of the project
- checks how the disability data asset protects personal information. This includes from misuse, loss or unauthorised people accessing, changing or sharing information.

How we will respond to recommendations

Recommendation 1: Principles for adding datasets into the disability data asset in the future

Maddocks recommends that we develop a set of principles to guide how government adds new data to the disability data asset. We should publish these principles on the National Disability Data Asset website with a description of the data being added.

Our response

The Commonwealth Partners agree.

We will develop a set of principles. The principles will guide decisions about adding datasets into the disability data asset in the future. A dataset is a collection of information, records and facts.

When adding new datasets, the principles will consider:

- the public interest – in particular, whether it is in the interest of people with disability
- how useful the new data would be within the disability data asset
- any limits on using the data.

We will develop the principles with state and territory governments, the disability community and researchers. We will give the Council this set of principles to approve. We will publish these principles on the website with a description of the data being added.

We will complete this by December 2024.

Recommendation 2: Collection notices for data providers

A collection notice is a statement that an organisation gives to people when they ask for personal information. It explains why they need the information and how they'll use it. Maddocks recommends that data providers use standard words in their collection notices. For example, in forms and on websites. Data providers are government agencies that provide data to be included in the disability data asset.

The Council should support these standard words. The Board should approve them.

Over time, data providers should have to update their collection notices with the new standard words. For example, this could be included in data sharing agreements. Or they should be encouraged to do this. This would be a best practice way to tell people about how their information is being used.

Our response

The Commonwealth Partners agree.

We will ask Australian, state and territory government data providers to update their collection notices with standard words.

We will create a standard collection notice that data providers can use. We will base this on words from:

- the privacy statement on the National Disability Data Asset website
- collection notices or privacy statements from other assets – for example, the [Person Level Integrated Data Asset](#).

We will consult with relevant governance groups and data providers.

We will ask the Board to approve the standard words, with support from the Council.

We will complete this by July 2024.

Recommendation 3: Managing the risk of re-identifying data – review of processes

Maddocks recommends that the Council have regular processes to review how the risk of data being re-identified is being managed. For example, a review could be carried out every year.

The Council could also decide on situations that would trigger a review. For example, if there is a data breach or government advice about threats to cyber security. This is to make sure we can continue to use best practice when de-identifying data and managing re-identification risks. This would consider technology and risks as they change in the future.

Our response

The Commonwealth Partners agree.

We will ask the Board to commit to a re-identification review process. This review would check that we are still using the best methods to manage re-identification risks. The review could include checking:

- work plans of governance groups
- governance documentation
- security practices in place.

We will support the review process to be carried out at least once a year. And when any significant new or changed risks are identified.

We will document any:

- situations that trigger the review process
- actions that we take
- changes that we put in place.

This review will be reported to relevant governance groups. This includes the Board and the Council.

We will complete the first review by July 2025.

Recommendation 4: Managing the risk of re-identifying data – rules for what is shared

Maddocks recommends that any de-identification policy (now called the de-identification strategy) should be clear about:

- the risk of serious harm if someone is identified through use of the data in the disability data asset
- the need to consider and control this risk when using the data.

The strategy should also include the rules that apply to projects that use the data. We should consider if we need any extra processes, such as ones used in other data assets. For example, a process to check that results of data analysis are correctly de-identified before they leave the underlying system.

Our response

The Commonwealth Partners agree.

We will apply this recommendation in:

- the de-identification strategy
- the data access, use and release protocol.

We will complete this by June 2024.

Recommendation 5: Managing data breaches

Maddocks recommends that the Data Breach Response Plan (now called the Data Breach and Incident Response Framework) has one approach for dealing with data breaches across the government agencies working on the disability data asset. The Framework should clearly explain what each relevant governance group and organisation must do. This includes when the ABS stores the data.

The Framework should also specify who is responsible for writing notices about the breach for:

- the Office of the Australian Information Commissioner
- the Office of the National Data Commissioner
- any people affected by the breach.

Our response

The Commonwealth Partners agree.

We are putting strong security processes in place for the disability data asset and its underlying system. All systems will need to be approved as safe and secure to store and use data.

We will consider this recommendation when we develop the Framework. The Framework will have one approach for dealing with data breaches. This will clearly explain what each governance group and organisation involved in the data breach must do. It will cover who must oversee the breach, report on it and notify people about it.

All responsibilities will be in line with:

- data sharing arrangements

- the laws that apply, such as the data breach responsibilities in the [Data Availability and Transparency Act 2022](#) and the Notifiable Data Breaches scheme in the Privacy Act
- any other laws or policies that apply.

All organisations must be accredited to provide data services under the Data Availability and Transparency Act. Accredited organisations must have their own policies and processes in place for managing the risk of data breaches.

The Office of the National Data Commissioner could carry out independent checks of an accredited organisation. For example, they might check whether an organisation's activities are in line with the Data Availability and Transparency Act Scheme.

We will complete the Framework by June 2024.

Recommendation 6: Developing a compliance framework

Maddocks recommends that the Board develop a compliance framework to check that everyone is following our data sharing agreements. This framework should cover the disability data asset and the underlying system. For example, people who use the disability data asset and approved systems could report every year to:

- the Australian National Data Integration Infrastructure Guardian
- the National Disability Data Asset Guardian

These 2 guardians are ABS officers. They are responsible for managing the disability data asset and its underlying structure in a safe, legal and ethical way. They will also approve who can access and use the systems.

These reports could include checks around:

- collection notices
- security
- other matters such as independent reviews of systems and processes.

Our response

The Commonwealth Partners agree.

We will develop a compliance framework for the disability data asset and its underlying system. This framework will help assess and report that people and organisations are following the agreements and security obligations. This includes the Head Agreement and Bilateral Schedules and Multilateral Data Sharing Agreement.

The framework will also build on:

- other assurance documents – for example, the Legal Authorisation Framework and Data Governance Framework
- existing requirements – for example, under the Data Availability and Transparency Act Scheme.

We will complete this by October 2024.