Summary of 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 how people use 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?

A Privacy Impact Assessment (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.

Maddocks wrote a detailed PIA report. This document is a summary of that report. It includes the process and a summary of findings and recommendations.

More information is 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 Australia's *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.

The Commonwealth Partners and Maddocks consulted with stakeholders for the PIA between March and July 2023. Over 150 people came to the sessions. Deafblind Australia helped to run 2 sessions with people with disability. Inclusion Australia, with help from Down Syndrome Australia, ran a session for people with intellectual disability.

Maddocks wrote a detailed consultation report about the feedback. A summary of the report is on the Privacy for the National Disability Data Asset webpage.

Summary of findings

In the consultation sessions, people told us they strongly supported developing the disability data asset. Some people pointed out the serious problems for people if information about their health or disability is shared without authority.

The Australian community expects that sensitive information should be protected even more than other personal information. Sensitive information might include information about your health, racial or ethnic origin and religious beliefs. You can find more information and examples in section 6 of the Privacy Act and on the Office of the Australian Information Commissioner website.

Maddocks noted that the Commonwealth Partners have a focus on privacy in the design of the disability data asset. In particular, the governance arrangements will be strong and detailed. These are the rules about who makes decisions about the project and how. The rules and processes have been well designed to manage the data and privacy risks of the project. This includes to find risks in the future.

The Commonwealth Partners will put processes in place to protect people's personal information. When linking different data together, this includes:

- using detailed data sharing agreements
- following laws about how data is shared, including the *Data Availability and Transparency Act 2022*
- having set rules on what is shared from the linked data. For example, checks before releasing research findings.

We will de-identify all data in the disability data asset to make sure no one can find out who people are. But stakeholders noted in the consultation sessions that there may be a risk of being able to re-identify people when linking the data. This re-identification risk may increase as more data is added to the disability data asset.

Maddocks recommends ways to address this risk and improve how we protect people's privacy.

Recommendations

The PIA recommendations are on the following topics:

1. Principles for adding datasets into the disability data asset in the future
2. Collection notices for data providers
3. Managing the risk of re-identifying data – review of processes
4. Managing the risk of re-identifying data – rules for what is shared
5. Managing data breaches
6. Developing a compliance framework

There is more information in the Appendix – Detailed recommendations.

Appendix – Detailed recommendations

There are 13 Australian Privacy Principles (APPs). They are the rules in the Privacy Act about managing personal information. After each recommendation is a list of the APPs it relates to. You can find more about APPs on the Office of the Australian Information Commissioner Australian Privacy Principles webpage.

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

Background

The National Disability Data Asset Charter (the Charter) has strong principles and rules for how the disability data asset can be used. The disability community wrote the Charter. The Council and disability ministers will approve the Charter.

It is also important to have clear rules for when we add datasets into the disability data asset. A dataset is a collection of information, records and facts.

Proposed Approach

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.

Maddocks suggests that the principles should at least take into account:

- the public interest for adding new datasets – there could be guidelines on how to assess this, such as asking if it benefits the disability community
- how useful the new data would be within the disability data asset – it should only be added to the disability data asset if an approved research project is likely to use it
- the types of information in the new dataset and any limits on using it – for example, if it has information that is sensitive, even if the Privacy Act doesn't define it as sensitive information
- if the data includes information about First Nations people or other vulnerable people.

Related APPs

- APP 1 – Open and transparent management of personal information
- APP 3 – Collection of personal information
- APP 6 – Use or disclosure of personal information
- APP 11 – Security of personal information

Recommendation 2: Collection notices for data providers

Background

We will add data into the disability data asset through different legal ways. This will depend on how the data provider collected the data. Data providers are government agencies that provide data to be included in the disability data asset. Some data can be legally shared into the disability data asset without a person's consent.

An important privacy principle is making sure people know how their personal information will be used and shared.

Proposed Approach

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.

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

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.

Related APPs

- APP 1 – Open and transparent management of personal information
- APP 3 – Collection of personal information
- APP 5 – Notification of the collection of information

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

Background

One of the principles of the draft Charter is to make sure data is kept private and secure. The disability data asset will only contain de-identified information. But some people note that there is a risk the data could be re-identified. And that the risk will increase over time.

Proposed Approach

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.

Related APPs

- APP 6 – Use or disclosure of personal information
- APP 11 – Security of personal information

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

Background

If information from the disability data asset is re-identified, there is a chance of greater harm to the affected people. This is because of the type of information that makes up the disability data asset. And that the disability data asset includes information about vulnerable people.

Under the Data Governance Framework, we will develop a policy about de-identifying data. The Framework is a set of rules to make sure people share, manage and use the data in safe, secure, ethical and legal way.

Proposed Approach

Maddocks recommends that any de-identification policy 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 policy 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.

Related APPs

- APP 6 – Use or disclosure of personal information
- APP 11 – Security of personal information

Recommendation 5: Managing data breaches

Background

Government agencies work together to manage the disability data asset and its underlying system. This means there may be increased risk of a data breach. There may also be an increased risk that they won't be able to quickly handle these breaches.

Under the Data Governance Framework, we will create a Data Breach Response Plan. This will include a record about any data and privacy breaches and incidents. The plan would include a review every year.

Proposed Approach

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

The Plan 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.

Related APPs

- APP 11 – Security of personal information

Recommendation 6: Developing a compliance framework

Background

There will be a range of rules and processes in place to manage the disability data asset. This includes data sharing agreements. Under the Data Governance Framework, there is a plan to carry out audits and reviews of the underlying system.

Proposed Approach

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 system in a safe, legal and ethical way. They will also approve who can access and use the systems.

The reports could include checks around:

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

Related APPs

- APP 1 – Open and transparent management of personal information
- APP 6 – Use or disclosure of personal information
- APP 11 – Security of personal information

Learn more

Commonwealth Partners have responded to each of the 6 recommendations from the 2023 Privacy Impact Assessment (PIA). You can read the Response to the 2023 PIA on the National Disability Data Asset website at Privacy for the National Disability Data Asset.