NDIS Public Data Sharing Policy

August 2020

Contents

1. Definitions

Term	Abbreviations	Definition
Application Program Interface	API; APIs	An Application Program Interface (API) is a communication protocol which allows for two applications to talk to each other.
Data Custodian		An organisation responsible and in the custody of data. The custodian is responsible for the safe transfer and storage of data.
Data Sharing Agreement or Memorandum of Understanding	DSA MoU	When entering into tailored data sharing agreements the NDIA will establish a Data Sharing Agreement (DSA), which is sometimes referred to as a Memorandum of Understanding (MoU) where the agreement is with another government entity. DSAs can be legally binding and set the guidelines and use of NDIS data.
De-identification		The removal of direct personal identifiers, such as name and address, or any information that can be defined as personal information under the *Privacy Act (Cth) 1988.*
Five Safes Framework		An approach to assessing and controlling the risks associated with data sharing and release. Use on the '*Five Safes Framework'* was published as the Australian Government approach by the Australian Bureau of Statistics. It has since been included in the *Data Sharing and Release Act (proposed).*
National Disability Insurance Agency	NDIA; 'the Agency'	The National Disability Insurance Agency administers the National Disability Insurance Scheme as per the *NDIS Act 2013.*
National Disability Insurance Scheme	NDIS; 'the Scheme'	The National Disability Insurance Scheme, as legislated in the *NDIS Act 2013.*
Obfuscate		To make data unclear and intentionally confused to ensure it cannot be re-engineered to identify participants.
Participant		A person with disability who has a plan under the *NDIS Act 2013*

Term	Abbreviations	Definition
Public Interest Certificate or Authorisation	PIC	A Public Interest Certificate (PIC) is an authorisation for the disclosure of protected Agency information if it meets the purposes set out in the *NDIS Act 2013*. A PIC thoroughly outlines the intended purpose of disclosure so a delegate of the CEO can make an informed decision whether to disclose or not.
Privacy Impact Assessment	PIA	A Privacy Impact Assessment (PIA) considers the legal and reputational risk of a project, with reference to the *Privacy Act (Cth) 1988* . It assesses the compliance of a potential project, or data request and identifies risks and makes recommendations on how they can be mitigated.

2. Executive summary

The *NDIS Public Data Sharing Policy* outlines on what data NDIA will share, and how NDIA makes decisions on releasing that data. The policy covers most data sharing and release arrangements with:

- The general public, including participants and commercial entities through open data,
- Governments, and
- Academics / researchers.

Data sharing is an important ingredient in ensuring the success of the NDIS and in enabling participants to exercise choice and control in reaching their life goals and outcomes. Greater access to data encourages competitive, innovative markets, informs policy development and creates a transparent and accountable public service. Further, increased access to data helps participants, their families and carers and the community recognise opportunities. This all serves to bolster community confidence in the NDIS and assist the Scheme to meet its aims as a world first social and economic reform.

Data-sharing decisions made by the NDIA are underpinned by a set of principles. These are:

- **The participant is at the centre of everything we do**: This principle states that all decisions must be made with NDIS participants' collective interests in mind, as well as be respectful to the rights of individuals.
- **NDIA is the custodian of NDIS 'protected' data[1]:** This principle reinforces the role of NDIA to act with integrity in the collection, use and disclosure of NDIS data.
- **Ethical use:** This principle states that decisions to share data should align with community expectations and standards.
- **Responsible release:** This principle addresses the need to consider ways to mitigate the risk of data misuse or misinterpretation once released.
- **Lawful release:** This principle reinforces that all decisions to share data must meet the legal requirements of relevant legislation, including *NDIS Act 2013* and *Privacy Act (Cth) 1988*.

Development of the *NDIS Public Data Sharing Policy* has been heavily informed, and is aligned to, the draft Commonwealth *Data Sharing and Release Act* (*proposed*). Risks

---

[1] All NDIS data is protected under *NDIS Act 2013* s60(1)

associated with data sharing are assessed using the Australian Government's *Five Safes Framework*. The five domains considered in the *Framework* are:

- **Projects –** data is shared for an appropriate purpose;
- **People –** The user has the appropriate skills and authority to access data;
- **Settings –** The way data is shared minimises risks of unauthorised use or disclosure;
- **Data –** Appropriate and proportionate protections are applied to the data; and
- **Outputs –** Reports and analyses have appropriate safeguards prior to release.

Risks identified against the five domains in the *Five Safes Framework* interact with each other. For example, a 'high' risk project may involve 'low' risk data and therefore data sharing would be considered 'safe for sharing'. The *NDIS Public Data Sharing Policy* details how NDIA will assess the interaction between domain risks.

The *NDIS Public Data Sharing Policy* also states how the NDIA will consider releasing data.

- **Open data release** refers to data that is released to the general public without any access restrictions. For data to be openly released, the data <u>must</u> be graded as low risk against the 'Data' domain of the *Five Safes Framework*. Open data includes data cubes, interactive visualisations, synthesised reports, access to data via Application Programming Interfaces (APIs) and NDIS performance publications.
- **Tailored data release** refers to data that is released to individuals or organisations to support a specific purpose. Tailored data releases are documented using a Data Sharing Agreement (DSA). The DSA includes the conditions that NDIA require the recipient comply with in order to mitigate specific risks. Non-compliance of the conditions in a DSA will result in the recipient being considered an unacceptable risk in future assessments.

In assessing risks against the *Five Safes Framework*, the NDIA CEO or their delegate may consider advice from the NDIA's Data Management Committee[2]. In some instances, explicit consent may be required from participants prior to data being released. The NDIA will publish on its website a register of tailored data releases.

---

[2] The Data Management Committee (DMC) oversees NDIA's governance and management of data. The DMC membership and responsibilities span all functions of the NDIA.

3. Introduction

3.1 Key points

- The *NDIS Public Data Sharing Policy* covers data the NDIA shares and releases to external entities via two release methods - open data and tailored data requests.

- Data sharing is critical to the success of the NDIS and allowing participants to exercise choice and control in reaching their life goals and outcomes.

- Data sharing encourages competitive, innovative markets while also informing policy development.

- Open data sharing creates a more transparent and accountable public service, bolstering community confidence in the NDIS.

- The NDIA has developed its data sharing policy in line with Australian government frameworks for the sharing and release of public sector data, including consideration for whole of government data policies and initiatives

- The *NDIS Public Data Sharing Policy* is underpinned by principles that put the participant at the centre of Agency decision making and releases data in line with relevant ethical and legal considerations.

- The *NDIS Public Data Sharing Policy* supports adoption of digital channels and technology to share and exchange data (APIs).

3.2 What does the NDIS Public Data Sharing document cover?

The *NDIS Public Data Sharing Policy* regards data the NDIA is considering to share and release with external entities. External parties include government, academic researchers and the general public.

The NDIA will release this data via two release methods:

- Open Data, and
- Tailored data release.

This policy also covers the NDIA's decision-making process in releasing de-identified, aggregated data for open data releases and identifiable data for tailored requests.

Decision-drivers and risk assessments are considered in this policy, and seek to give guidance on how data requests are handled.

The policy also seeks to explain how risks are mitigated and decisions are made regarding the release of large public data sets, and smaller tailored requests for academics researchers and organisations.

3.3   Why is data sharing important for the NDIS?

The National Disability Insurance Scheme (NDIS) is a world-first social and economic reform agenda, supporting people with disability to live an ordinary life in an inclusive community. Data sharing is a critical success factor in enabling people with disability to exercise choice and control in how they live their lives, supporting conversations regarding social and economic participation.

By publicly sharing data, the National Disability Insurance Agency (NDIA) enables participants, their families and carers to become better informed consumers on support options. Further, sharing data allows service providers to make informed business decisions on market entry, in turn creating more vibrant, competitive markets.

Open data and its availability allows key stakeholders to better understand the problems they face, and how they can overcome them. Data integration across vast and different data sets generates new insights not considered before. Making data available to researchers and across governments will drive innovation in disability support models and policy development.

3.3.1   Data sharing empowers people with disability

At the centre of the NDIS are participants who are informed consumers, exercising choice and control about the supports and services they access. Information availability becomes a deciding factor in how participants make their choices.

With access to information, participants will drive markets to become more responsive to their needs. By improving the availability of data evaluating the effectiveness of support models and the availability of support alternatives, participants can be selective in finding the support, and providers, that best suit them.

Over time, data will allow participants to see the goals and outcomes being achieved by other NDIS participants. These insights result in increased awareness of opportunities and inform future goals and aspirations. The pursuit and achievement of goals benefits individual participants, and also results in a diverse and healthy market.

3.3.2 Data sharing creates competitive, innovative markets

Access to data can assist providers in streamlining their services, and find geographies and niches with unmet demand.

By enabling data-driven insights, providers will be able to investigate potential areas of operation and/or offer their supports in regions they were not aware required disability support. By exposing existing and potential demand data, providers can better understand opportunities and develop strategies to attract the business of people with disability.

In an increasingly digital world, data access also has the potential to develop ground-breaking new products and services to transform the way individuals live with a disability. Through open data, digital innovators can create new innovative methods of meeting market demands (including the introduction of new digital service delivery models). Releasing NDIS data gives the market the opportunity to react and grow as a result of an abundance of new information.

3.3.3 Data sharing informs policy development

With greater access to information governments can develop better informed policy. It allows the wider community including governments, academics and stakeholders in key communities to offer insights to the NDIA so it can make evidence-based policy decisions.

Data access gives researchers the ability to provide insights that inform markets and policy-makers on real-world behavior, resulting in more effective policy. Research and the availability of NDIA data assists in developing support models that are most likely to result in a positive outcome. Once beneficial outcomes are identified the market and policy-makers react to provide more informed options to those who live with a disability.

Further, like all Australians, people with disability interface with a range of government services across local, state and federal jurisdictions. By enabling data sharing agreements with government agencies, the NDIA is supporting policy areas in other areas of government. This provides for greater visibility on how citizens interface with government services, which improves the transfer of service provision across jurisdictions and reduces duplication.

3.3.4 Data sharing builds community confidence in the NDIA

Data sharing and transparency is crucial in delivering an effective NDIS and building public confidence in the NDIA to deliver the Scheme.

Transparency around NDIS activity makes the NDIA more accountable. It promotes visibility of government activity and expenditure while motivating the NDIA to continue meeting community expectations. Transparency of NDIS activity allows for collaboration with the wider community and industry partners, fostering a deeper involvement with the public. Most importantly, transparency assists in facilitating a dialogue between the NDIA and participants.

Releasing data related to the administration of the NDIS creates a source of truth regarding the NDIA's performance. Accurate and available information reduces anecdotal debate and encourages relevant discussions around the NDIS.

3.4   How does the NDIA approach to data sharing align to broader Commonwealth government frameworks?

The Australian Government is committed to increasing transparency and availability of government data.

The Australian government has established an interim National Data Commissioner to develop new legislation to support these reforms including the ability to share public sector data for specific purposes with appropriate safeguards.

The National Data Commissioner will work with government agencies and regulators to improve guidance on using existing legislative mechanisms to release open data prior to the reform legislation being introduced.

The NDIA has developed this policy in anticipation of the new legislative framework for the sharing and releasing of public sector data. In particular, the NDIA has adopted the draft data safeguards proposed by the National Data Commissioner and the Data Sharing Principles, which includes modernising risk assessments related to sharing and releasing data.

3.5   What principles underpin NDIA's decision-making?

Decisions regarding what data NDIA shares, and how NDIA releases data, are anchored by a set of important principles that seek to put the interest of participants first. The principles below act as a guiding mechanism for how the NDIA shares its data, ensuring NDIA acts as a responsible custodian and owner of NDIS data.

3.5.1 The participant is at the centre of everything we do

Any decision to share data must be made with participants best interests in mind, and respects the origin of NDIS data. Participants have a right to data that respects the individual and collective interests of those who live with a disability, and data that empowers sustainable choice and control over disability supports.

The NDIA holds NDIS information consistent with the general principles guiding all actions under the *NDIS Act*. Such principles include the rights of people with a disability to have the same right as other members of Australian society, and to respect their worth and dignity to live free from abuse, neglect and exploitation. Additionally, they must have their privacy and dignity respected[3].

The NDIA takes its role in safeguarding the rights of participants extremely seriously, and handles all personal data in accordance with the expectations of those individuals. The NDIA also manages its data in line with the expectations of the greater community, in accordance with the NDIS privacy policy and all privacy legislation.

3.5.2 NDIA is the custodian of NDIS data

As custodians of NDIS data, it is critical the NDIA maintain trust of all persons about whom it holds and owns data, including participants and providers.

The NDIA is responsible for data collection and, in accordance with legislation, policies, guidelines and any specific conditions, for use applicable to that data. The way custodians deal with data must be legal, with consent and align with reasonable expectations of the data owner.

As custodians, the NDIA seeks to use NDIS data to advance participant disability support and afford them choice and control. The NDIA will take steps to facilitate data sharing and release by controlling and mitigating risks.

The NDIA will take steps to ensure it is informed when making decisions to share NDIS data for research. When appropriate, researchers will be required to obtain prior legal and ethical approval from a certified Human Research Ethics Committee must be obtained in accordance with the *National Statement on Ethical Conduct in Human Research 2007* (2018).[4]

---

[3] Section 4(6), 4(10) *NDIS Act* 2013
[4] Unless the NDIA is required or authorised under law.

Where data being shared is not openly released, but is de-identified, the details of these arrangements will be publicly listed. The guidelines informing a NDIS decision to share such data are documented later in this policy.

3.5.3 Ethical use

The use and disclosure of NDIS data must align with community and participant expectations and must be lawful.

As a public entity, the community expects data sharing to be in the public interest and equitable. When considering the release of data the NDIA must be satisfied that it will be of benefit to NDIS participants and that it will not result in harm to participants.

On the flipside, the community expect that the maximum value is realised from publicly-funded NDIS data. To this end, NDIA must approach data sharing requests from an 'enabling' starting point.

Academic and other research organisations will be required to demonstrate to the NDIA that they have obtained approval from a certified Human Research Ethics Committee (HREC) dependent on the nature of the request[5].

When required by the NDIA CEO or their delegate, a panel of diverse stakeholders, including people with disability, will advise decision-makers on the potential risks of data release. The process where decisions are made will be controlled, documented, and auditable.

3.5.4 Responsible release

The responsible release of data considers ways to mitigate or control for risks related to data being misused or misinterpreted. A thorough and consistent risk assessment should be conducted to understand potential risks and their likelihood.

Data must be of an assured quality and protect the identity of participants. A conservative risk appetite must be applied when considering quality and privacy. The maturity of both the data and the process by which it was generated will be a consideration in the release.

---

[5] 'A consumer guide to the principles for accessing and using publicly funded data for health research' NHMRC, 2016.

In order to reduce the risk of misinterpretation, and being mindful of potential social impact, the NDIA will release accompanying metadata guides and supporting information on data subjects as released.

3.5.5 Lawful release

The NDIA's database contains personal identifying data, protected and sensitive information. All disclosures of NDIS data must be compliant with relevant legal obligations and be compliant with the [NDIA's privacy policy](#) and the [NDIA's operational guidelines covering the handling of protected Agency information.](#)

4. Sharing NDIS data

4.1 Key points

- NDIA will share data with the general population, governments and academic researchers where there is a clear purpose supporting data sharing.
- The NDIA uses the *Five Safes Framework* to identify risks related to data sharing and release.
- The NDIA will use a standard approach to evaluating risks and for developing controls.
- Data Sharing Agreements may contain conditions that data recipients must comply with, in order to control data sharing and release risks.

4.2 What data will NDIS share?

The data that the NDIA will consider for release is outlined in the table below and expanded upon in Appendix A: Data available for release.

Data to be released	Definition
Population demographics	Information on numbers of participants currently in the NDIS, and projected participant numbers at full scheme. Types of analysis variables that may be included would be geography, age group, and disability.
Plans, support types and budgets	Information on the number of participant plans, access requests, access met decisions, and need for support through the NDIA. Demographics that can be analysed include geographic region, age group, disability, and type of support.
NDIS plan budgets	Information on the value of current participant plan budgets, historical participant plans and plan management approaches. Demographics that can be analysed include geographic region, age group, disability, and type of support.
Market supply	Information on active providers and their market share. Demographics that can be analysed include geographic region, participant characteristics and type of support.
Goals & outcomes	Information on the current participant plans, historical participant plans, goals in progress and key outcomes indicators. Demographics that can be analysed include geographic content, age group, disability, and type of goal.
NDIA performance	Data on operational performance of the NDIA, including processing volumes, wait-times and backlogs.

4.3   Who will NDIS share data with?

The NDIA will share data with:

- General public, including people with disability, commercial organisations and media,
- Australian government departments and agencies (both Commonwealth and State/Territory), and
- Academic researchers.

4.4   For what purpose will NDIA share data?

The NDIA will consider sharing data, if the purpose of any release is:

- To inform participants of the availability and effectiveness of support models.
- To inform disability and related policy development.
- To support disability related academic research into disability support models and outcomes, and to enable academic research in the public interest.
- To inform the development of robust disability services.
- Any other reasonable purpose related to the objectives of the NDIS.

Under the *NDIS Public Data Sharing* Policy, data will not be shared with individual entities for commercial purposes.

4.5 In what circumstances does this policy not apply?

There are some data arrangements not covered in the *NDIS Public Data Sharing Policy.* These include:

- Data sharing or release required for the purposes of NDIA carrying out its legislated purpose and operations.
- Data sharing or release to an organisation as part of contracted NDIA work.
- Data sharing in response to concerns for participant safety or due to suspected abuse, neglect, natural disaster.[6]
- Requests made under Freedom of Information legislation.[7]
- Data sharing or release to an organisation governed under the NDIS Digital Partnership Program.

4.6 How does NDIA make decisions regarding data sharing?

In making decisions around sharing data externally, the NDIA CEO, or their delegate, consider –

1. Whether the data can be shared, and if so
2. How should it be released in order to minimise risks.

To support decision-makers, an assessment is conducted against each of the *Five Safes Framework* elements. The combined assessments provide direction on the conditions and format of any data to be released. The *Framework* considers risks across the following domains:

- **Projects:** Data is shared for an appropriate purpose

---

[6] The NDIA has current agreements in place to share data where participant safety is concerned.
[7] This is managed through the Freedom of Information policy <https://www.ndis.gov.au/about-us/policies/freedom-information>

- **People:** The user has the appropriate authority and skills to access the data
- **Settings:** The environment in which the data is shared minimises the risk of unauthorised use or disclosure
- **Data:** Appropriate and proportionate protections are applied to the data
- **Output:** The output from the data sharing arrangement is appropriately safeguarded before any further sharing or release

4.6.1 Using the *Five Safes Framework* risk assessment

Risks against the *Five Safes Framework* interact with each other. For example, a 'high risk' project using 'low risk' data will ultimately find the data release to be 'safe' Conversely, a 'medium risk' user accessing data on a 'high risk' setting may be considered 'unsafe'.

Figure 1 is the decision tree that NDIA will use to determine the outcomes of the *Five Safes Framework* risk assessment, and in determining whether DSAs need any specific conditions to control for risks.
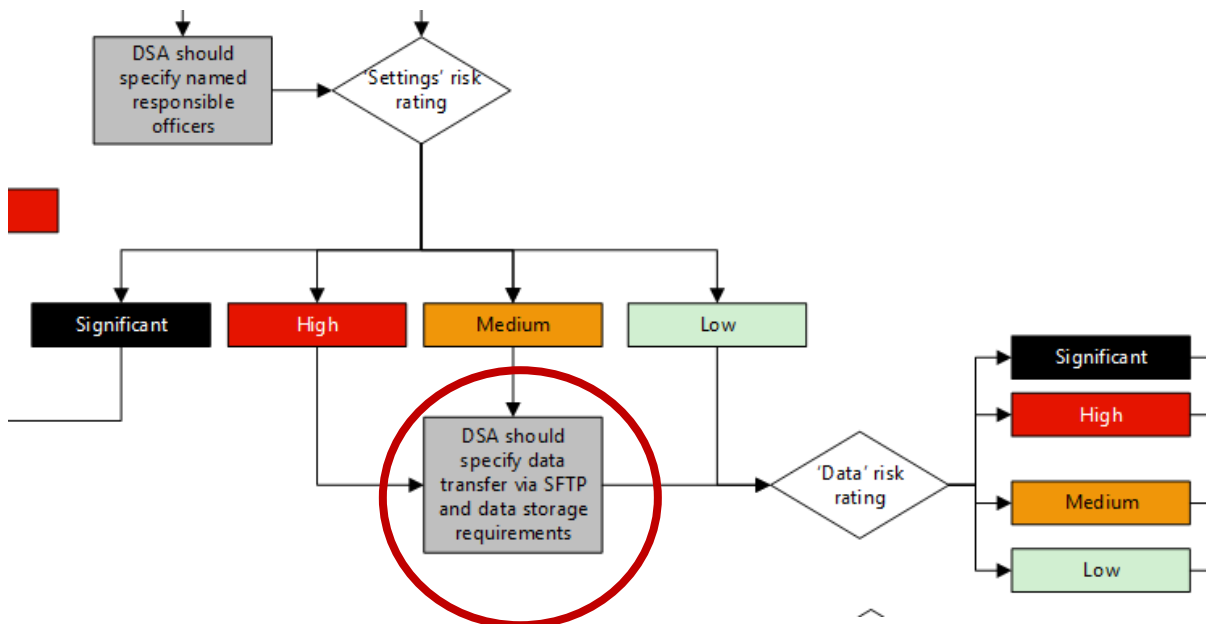
DSA should specify data transfer via SFTP / secure access via APIs and data storage requirements

FIGURE 1: DECISION TREE FOR ASSESSING THE FIVE SAFE FRAMEWORK
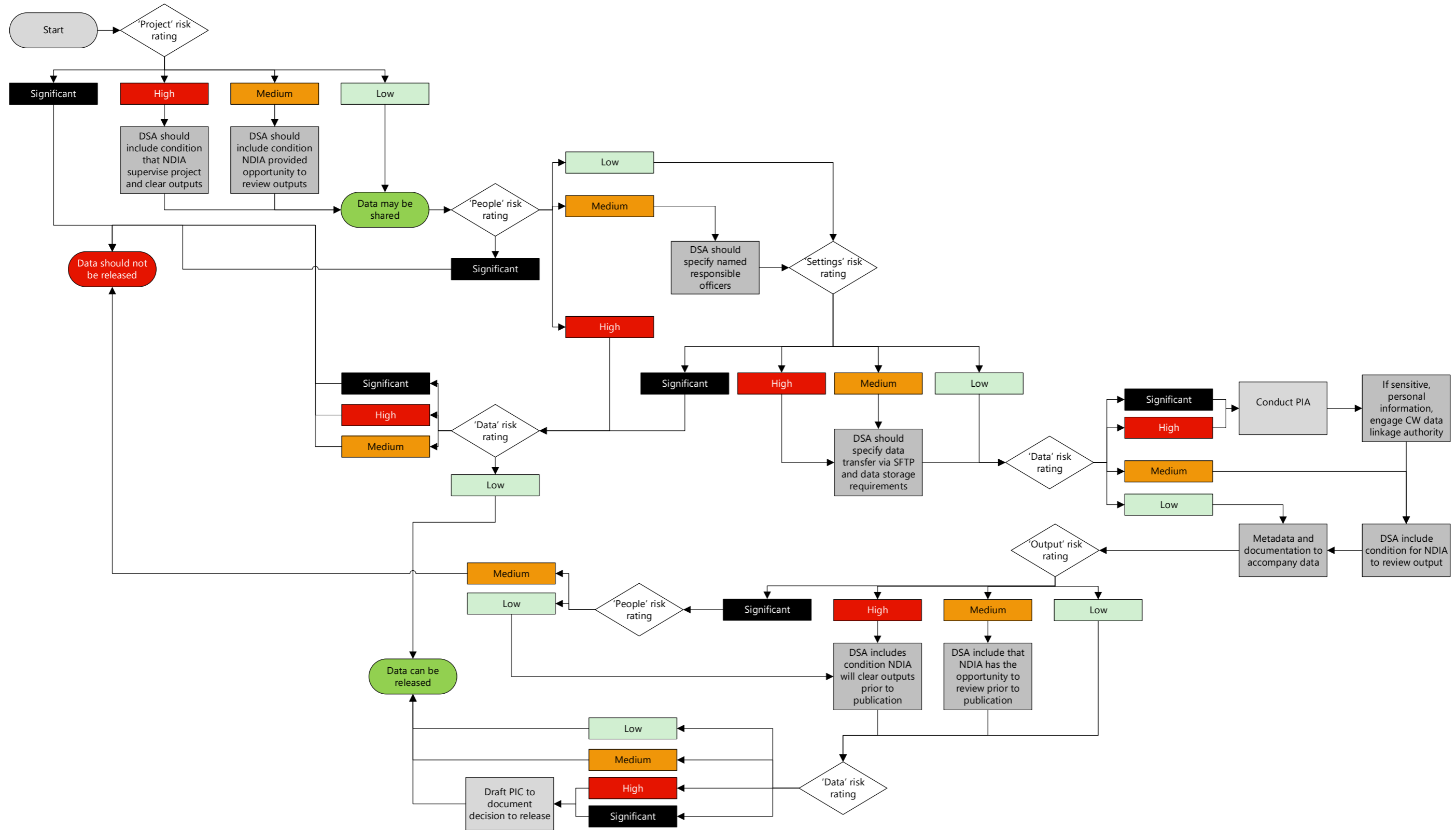
Guidance is provided in the following sections on how risks against the *Five Safe Framework's* domains are graded.

4.6.2 Assessing 'Project risks'

The NDIA data request process requires all researchers or organisations to explain the purpose of their project and the need to access NDIS data.

Research-based projects are initially considered by the NDIA Research and Evaluation Office (**REO**). The REO ensures that research is ethical and is in the public interest. The Research and Evaluation Office will ensure that research conforms to the applicable National Health and Medical Research Council guidelines and regulatory requirements. Projects being considered for data sharing are assumed to have met the REO's thresholds.

Project risks are graded as per Figure 1 using the highest applicable rating (for example, if a project is related to assessing a new support model [risk rating = low], however is likely to cause distress to participants [risk rating = significant], then project will be rated as a 'significant risk project'.

TABLE 1: INDICATORS OF 'PROJECT' RISKS

Risk rating	Example indicators of risks
Significant	- Is for commercial purposes - Is not ethical - Likely to result in harm or distress for participants or interfere with the privacy of participants
High	- Requires sensitive and personal identifying information - Likely to result in negative perceptions surrounding the performance of the NDIA and NDIS
Medium	- Requires specific yet de-identified information on participants - Data may be used for multiple purposes or on-disclosed to third parties - May result in negative findings about the NDIS or may result in negative attitudes from the wider community
Low	- Strongly linked to purposes documented in Section 4.4

4.6.3 Assessing 'People' risks

In assessing people risks, the NDIA considers the data handling and interpretation skills of individuals and organisations accessing released data.

If data is to be used for research purposes, the REO will grant approval based on the Human Research Ethics Committees (**HREC**) process, which assesses whether the methods correctly address the research question, that they have the appropriate skills and experience to undertake the project. The NDIA may require organisations or researchers to enter into legally binding agreements which set the appropriate boundaries for data use.

People risks are graded as per Figure 1 using the highest applicable rating.

TABLE 2: INDICATORS OF 'PEOPLE' RISKS

Risk rating	Example indicators of risks
Significant	- Requestor is an individual not affiliated with research, academia, government etc. - Individual or organisation requesting data has previously not complied with the terms of a Data Sharing Agreement
High	- Responsible officer receiving data has not demonstrated experience in dealing with sensitive data, or has had a reportable data breach within the last 5 years - Data is being released openly to the general public
Medium	- Academic researchers with Human Research Ethics Committees - Organisation has provided evidence of experience, qualification, policies and processes with regards to data handling and interpretation
Low	- Government departments

4.6.4 Assessing 'Setting' risks

In assessing 'setting' risks, the NDIA evaluates the technologies proposed to transfer, store and analyse any data being released.

Setting risks are graded as per Figure 1 using the highest applicable rating.

TABLE 3: INDICATORS OF 'SETTING' RISKS

Risk rating	Example indicators of risks
Significant	- No information provided to enable assessment of data handling approach - Off-shore databases (including cloud storage) where compliance with Australian Privacy Principle 8 might be difficult.
High	- Unsecured email transfer

Risk rating	Example indicators of risks
	- Public databases (including cloud storage) located in Australia. - Unclear ICT system and/or data handling evidence. - Access via Public / Open APIs
Medium	- Private, secure databases (including cloud storage) located in Australia. - Auditable, user system logs. - Access restricted to named individuals with password protected system accounts - Strong evidence of appropriate level of ICT system security provided - Access via OPEN NDIS APIs
Low	- Use of a secure File Transfer Protocol - Access via secured NDIS API - Australian Government ICT networks

4.6.5 Assessing 'Data' risks

In assessing 'data' risk, NDIA evaluates the sensitivity, quality and interpretability of the data to be shared. This includes, but isn't limited to, data that is personally identifying, of reputational risk, is immature or poorly understood. Data-specific risks are evaluated by NDIA's Data Management Committee (**DMC**), informed by subject-matter and technical experts.

Data risks are graded as per Figure 1 using the highest applicable rating.

TABLE 4: INDICATORS OF 'DATA' RISKS

Risk rating	Example indicators of risks
Significant	- Identifiable data (containing name, date of birth, address) - Data that is commercial in confidence - High risk of identifying individuals
High	- Data is sensitive - Data that concerns a relatively small number of participants - Data requires specific knowledge to interrogate and interpret - Data to be openly released - Data with known quality issues, or generated from immature systems and/or business processes

Risk rating	Example indicators of risks
	- Data with indirect identifiers (age, gender, post code)
Medium	- Data that represents complex or not generally understood concepts - Data requires supporting information to interpret correctly - Aggregated data to a specific demographic area - Data that potentially could be reverse-engineered to be identifiable.
Low	- Highly aggregated data - No possibility of identifying individuals through reverse engineering or complex analytics - Data that represents simple concepts - Data that is simple to interpret and requires no or limited supporting information – e.g. simple participant counts

4.6.6 Assessing 'Output' risks

In assessing 'output' risks, the NDIA considers potential on-disclosure and publication impacts after data has been released.

Output risks are graded as per Figure 1 using the highest applicable rating.

TABLE 5: INDICATORS OF 'OUTPUT' RISKS

Risk rating	Example indicators of risks
Significant	- Intention to on-disclose personal identifying information to a third party - Intention is to contact participants, their family and/or carers. - Request is ambiguous in its intention to on-disclose to a third party
High	- Request has stated intention to on-disclose to a third party - Data carries a significant reputational risk - Releasing reports with minimal oversight, not peer reviewed - NDIA is provided an opportunity to review reports and findings prior to any public release
Medium	- Analysis will be used as an input into peer-reviewed publication - NDIA is provided an opportunity to review reports and findings prior to any public release - Reports for internal use only

Risk rating	Example indicators of risks
Low	- Reports for public with extensive government oversight.
	- Reports will not be publicly released

5. Data release

5.1 Key points

- The NDIA will release data utilising different methods dependent on whether it is an open data or tailored data release.

- Openly released data is de-identified to mitigate the risks associated with identifying NDIS participants.

- Tailored data requests will be released to academics, research organisations and government departments/agencies.

- NDIS data for research purposes will be evaluated by the REO to assess the merits of the proposed research.

- The DMC assist the CEO or their delegate in evaluating the risk as low, medium, high or significant using the *Five Safes Framework*.

- A public register of tailored data sharing agreements utilising NDIS data will be available on www.ndis.gov.au

5.2 How will NDIA release data?

NDIA will use two general methods to release data -

1. *Open Data Release* – data that is released to the general public, without any access or use restrictions applied. Table 6 documents the types of open data that NDIA will release.

2. *Tailored Data Release* – data that is released to named individuals or organisations, with restrictions on the data's use and on-disclosure. Table 7 documents the types of tailored data arrangements that NDIA may consider.

TABLE 6: 'OPEN DATA' RELEASE METHODS

Release method	Description	How is released and accessed?
Downloadable data cubes and tables	Aggregated data will be available in downloadable formats for self-directed exploration and/or integrations into external parties' systems and analyses.	ndis.gov.au – Data & Insights page
Interactive visualisations	Data will be presented visually, either as maps, charts or infographics. These visualisations will be able to be filtered to display populations or characteristics of interest	ndis.gov.au – Data & Insights page
Synthesised Reports	These reports provide an alternative way to access the information without the need to access visualisations or data cubes.	ndis.gov.au – Data & Insights page
APIs	Data will be shared via APIs for currently available data sets such NDIS Price Guide, Registered Provider Data.	ndis.gov.au – Data & Insights page (ie. API Link under file links – possible access through API Catalogue DPP Developer portal, DTA site etc)
Quarterly Performance Reports	These reports provide insight into NDIS activity and NDIA operational performance	Ndis.gov.au

TABLE 7: 'TAILORED DATA' RELEASE METHODS

Release Method	Description	How is data released and accessed?
Tailored data release	Data tailored to the needs of academics to support research[8]. Exchange will occur directly between NDIA and the other party.	As per method prescribed by risk assessment.
Multi-organisational, linked data assets	Integrated data assets managed by third parties, where data from multiple organisations are combined for the purpose of supporting academic and policy research.	Via MOU / Public Disclosure Certificate, and transferred via Secure File Transfer Protocol or APIS.
Enduring authorised datasets	Sharing arrangements involving a periodic refresh of data (including real time). These arrangements typically are typically exchanges between government departments.	Via Memorandum of Understanding / Public Disclosure Certificate / Data Sharing Agreement and transferred via Secure File Transfer Protocol or APIS.

5.3   Open data

5.3.1   Purpose of releasing open data?

The NDIA is committed to promoting transparency and accountability in government. Utilising the knowledge and insight obtained by making data available to the public will bring with it new opportunities in how the NDIA manages the scheme. Greater access to information enables participants to become informed consumers and to exercise choice and control in how they reach their disability care goals.

---

[8] Research will be considered by the NDIA's REO prior to data being shared. Data that is identifiable will require explicit participant consent prior to sharing, and will only be disclosed if the research is in the interest of NDIS Participants.

The NDIA is releasing data that is freely available, easily discoverable, accessible and able to be re-used.

5.3.2 How will data be protected and risks managed?

Managing sensitive data risks:
All publicly released data is de-identified to protect the privacy of participants and NDIS stakeholders. The NDIA has removed all personal identifying information and direct identifiers from open data. The information is no longer considered personal information under the *Privacy Act* (*Cth*) 1988 if de-identified.

In response to identified risks, the NDIA employs de-identification methods to manipulate data. For security reasons, specific methods of de-identification cannot be disclosed in this policy – however, the NDIA applies cell-level manipulation in its de-identification process. Such manipulation is conducted by the Office of the Scheme Actuary to preserve the usefulness of the data, while manipulating the fields to prevent them from identifying participants.

To balance the exposure of aggregated demographic data and protection of participants, NDIS applies techniques to *obfuscate* data while keeping the data fit for purpose of trend analysis and general decision guidance. Some methods that have been applied include:

- Providing only aggregated values with broad categories
- Merging low count/value categories
- Range bands instead of exact values
- Add/subtract a random number to non-aggregate rows
- Multi layered treatment to rows with very low counts

Managing risks of misinterpretation:
Additional modes by which the NDIA protects the use of open data is by providing accompanying metadata 'how to use' guides and synthesises reports that offer deep-dives into various areas of the scheme.

5.4 Tailored releases of NDIA data

5.4.1 Who will NDIA enter into tailored data sharing agreements with?

The NDIA will enter into tailored data sharing arrangements with:

- Academics
- Research organisations

- Government departments and agencies

5.4.2 How will data be protected and risks mitigated?

As per outcome of the risk assessment and in line with the Data Sharing Agreement (**DSA**)

The DSA will document:

- Terms and use of data being released
- Expected conditions around on-disclosure
- Requirements for access, transfer and storage

5.4.3 What happens in the case of non-compliance with the conditions within a DSA?

Given each DSA varies dependent on the nature of the agreement, consequences for a breach can vary greatly. However, any breach of an agreement in the past will be considered as a significant factor in assessing any future data requests.

Past behaviours and breaches are considered as part of the 'people' risk assessment when assessing a data request. Deliberate non-compliance will attract a risk rating of significant, which will result in the rejection of future requests. Further any breaches of will be reported to the Office of the Australian Information Commissioner.

In the event that a data recipient becomes aware of an act of non-compliance or a data breach, they should inform NDIA immediately.

5.4.4 How to request access to NDIS

Tailored data releases are initiated using the Tailored Data Release Request form.

This form is available from https://www.ndis.gov.au/about-us/data-and-insights/public-access-data

NDIA will typically assess applications within 28 days of receiving a complete form.

Figure 2 describes the tailored data release process, identifying the key steps in determining whether data can be shared and released.

5.5 Providing feedback to NDIA regarding data sharing agreements

5.5.1 Will there be a register of tailored data sharing agreements?

Yes. The NDIA will maintain and regularly update a public register of its data sharing arrangements. This applies to government data sharing agreements and to research.

The register will be available on www.ndis.gov.au

5.5.2 When does NDIA require explicit consent from individuals on the use and release of their data?

The NDIA will require explicit consent from participants where academic research requires their name or direct identifiers for their research.

Any research of this kind will attract the mandatory requirement of informed consent from all those involved.

5.5.3 How do I provide feedback?

If you would like to provide feedback on the NDIA Data Sharing procedure, you can do so at the website. ndis.gov.au

FIGURE 2: THE TAILORED DATA REQUEST ASSESSMENT PROCESS

Develop request
- Requesting organisation develops request.
- Reponsible officer describes nature of the request.
- A research request rests on the unqiue nature of the research. Before submitting a request of this kind please check the Research Project Public Register to check if research similar is already being assisted by the NDIA.

Research and Evaluation Office
- If a research request the proposal goes before the Research and Evaluation Office (**REO**).
- If the REO are satifisfied it is appropriate on the basis that it is unique and in the public interest it is forwarded to the Data Management Commitee (DMC).

Data Management Commitee
- DMC records details regarding the data request and monitors it until it has been completed. The request is assessed as being valid and will provide an estimate for the cost of fulfilling the data request.
- The request is distributed to all members of the committee.

Risk assessment
- The DMC assist the CEO, or their delegate, to complete the risk assessment documented in Section 2.5.1
- The delegate may request input from DMC members in determining risk, including input from the NDIA Legal Branch in evaluating any legal and privacy risks.
- Requests that indicate significant data sharing and release risk, but require escalated decision-making due to sensitivities around refusing the request may be referred by DMC to the NDIA CEO or the NDIS Board Risk Subcommittee.

Outcome of request
- The requesting organisation is notified.
- A data sharing agreement (DSA) is drafted for the organisation to consider.
- If the organisation does not accept the conditions of the DSA, a further request may be submitted which mitigates risks identified during the *Five Safes Framework* assessment.
- If unsuccessful, the requesting organisation will recieve a denial letter which details the reasoning behind the denial. Further requests will be consiered which reduce the risks identified during the assessment.

Appendix A: Data available for release

Subject area	Description of data to be provided
Participant demographics data	Administrative data at the participant level on age, gender, primary and secondary disability, functional information, CALD status and residential information.
Participant access data	Administrative data at the participant level on access decisions including decision status and reasons for eligible and ineligible participants.
Participant exits data	Administrative data on participant exits including the exit date
Participant transition data	Administrative data at the participant level on transition including transition cohort, NDIS regions, transition dates, and State/Commonwealth program of origin.
Participant plan data	Administrative data at the participant plan level on the history of plans approved, plan start and end dates, committed amounts, and self-managed plans, including scheduled and unscheduled reviews.
Supports committed data	Administrative data at the participant committed support category level on the history of supports committed and their committed amounts including support line item data, where available (e.g. specialist disability accommodation, supported independent living).
Supports received data	Administrative data at the participant support line item and provider registration group level on the history of supports received, support dates, provider claimed amounts, and provider claimed dates.
Supports paid data	Administrative data at the participant support line item and provider registration group level on the history of payments made for the supports received to the providers claiming, including payment amount, payment dates, providers, and flags for self-managed participants and participants with plan managers.
Supports in-kind data	Administrative/invoicing data at the participant support line item and provider registration group level on the history of in-kind supports received including 'payment' amount and support received dates.
Provider registration data	Administrative data at the provider level on provider registration details, registration groups and self-managed determinations.

Subject area	Description of data to be provided
Participant outcomes data	Administrative data at the participant level from the NDIS Outcomes Framework (short form) on participant outcomes excluding free-text fields.
Participant pathway data	Administrative dates at the participant level to track participant interfaces with the NDIS including date of contact, access, plan commencement, plan approval, support booking, support provision, provider claim, provider payment and exit.
Participant goals data	Administrative data at the participant plan level on participant goal domains at each plan review.
Participant satisfaction data	Survey data at the participant level from the NDIS satisfaction surveys on participant satisfaction with the NDIS planning, excluding free-text fields.
Carer demographics data	Administrative data at the carer level on the demographic and characteristic of family and formal carers.
Supports (mainstream interface) data	Administrative data at the participant support line item level flagging supports which interface with mainstream services.
ECEI program data	Administrative data at the participant, support and provider level including contact with the Early Childhood partner, connected supports, short-term interventions, referrals, plans and providers.