Defining 'trusted entities' for the purposes of national data sharing

FINAL REPORT

Authors

Strategic Data Initiatives, Data and Digital Government, Queensland Department of Customer Service, Open Data and Small and Family Business

Data Strategy and Governance, Data and Analytics, Services Australia

Executive Summary

This project seeks to define the attributes of a 'trusted entity' to support safe, secure, and ethical data sharing across Commonwealth, state, and territory governments. Rather than creating a new accreditation scheme, the intent is to provide a consistent framework and practical guidance that complements existing data sharing frameworks, such as the *Data Availability and Transparency Act 2022* (Cth) (DAT Act) accreditations managed by the Office of the National Data Commissioner. By focusing on a common recognition of attributes related to trustworthiness, this work aims to reduce burden by streamlining data sharing processes, enhancing collaboration, and building confidence in the national data sharing environment.

A trusted entity is defined as an agency capable of safely, securely, and ethically managing shared data. Attributes have been developed under the five themes below which provide a common recognition on how agencies should assess trustworthiness, ensuring data custodians can make informed decisions about sharing data. The five themes the attributes sit under are:

1. **Transparency** which ensures clarity in data use and decision-making
2. **Accountability** which establishes clear roles, responsibilities, and compliance mechanisms
3. **Data management and governance** which focuses on maintaining data quality, metadata practices, and risk management
4. **Security** which safeguards data through robust technical controls and secure environments
5. **Privacy** which protects personal information through minimisation, de-identification, and incident reporting.

Outcomes

- Guidance material outlining the trusted entity attributes under the five themes of transparency, accountability, data management and governance, security and privacy.
- Alignment of the trusted entity attributes with the Office of the National Data Commissioner's accreditations.
- Use cases showcasing how the guidance material can be implemented or could have been used to streamline national data sharing.

DAT Act Review Alignment

The findings from this project have been shared with the DAT Act Review team. The project team acknowledges the collaborative approach taken by the DAT Act Review team in relation to the intersections of this project and the Review outcomes. The project team recognises the

close alignment between the findings and recommendations of this project and the DAT Act Review, particularly in relation to:

- the agreement that Office of the National Data Commissioner (ONDC) accreditation is generally robust and valuable
- the need for the recalibration of ONDC accreditation
- the adoption of 'accreditation categories' to enable more flexibility for specific data sharing use cases.

The future opportunities outlined in this report align closely with the adoption of accreditation categories and the ongoing work required to ensure consistency, collaboration and uplift of the national data sharing ecosystem.

Recommendations

The project team note that these opportunities could be impacted by existing and future national data sharing initiatives including recommendations from the Data Availability and Transparency Act Review. The project team, in consultation with workshop participants and with input from the Data Availability and Transparency Act Review team, recommend the following as future opportunities:

- The project team note accreditation by the ONDC aligns closely with the trusted entity attributes and there are 39 entities accredited. There is value in 'accredit once, use many times' in the national data sharing ecosystem. The project team acknowledges that accreditation by the ONDC is a robust assessment of trust and should be leveraged to support national data sharing.
- Trust metrics are difficult to measure, and further development is required to understand how the developed attributes can be incorporated into the national data sharing ecosystem given that not all data sharing activities require assessment against every attribute.
- Additional resources are required to support agency capability uplift to increase and demonstrate their trust reputation. The project team note that this aligns closely with the ongoing nature of data maturity uplift within an agency.
- Transparency around both trusted entity status and data sharing request outcomes was a strong theme emerging from the project. Further research is needed to understand the requirements for documenting data sharing activities, and how public transparency mechanisms could be embedded.

Introduction

The Fourth National Work Program and project rationale

National Cabinet's Intergovernmental Agreement on Data Sharing (IGA) sets out First Ministers commitment to more effective public sector data sharing. As part of embedding the IGA into data sharing practice, the National Data Sharing Work Program (Work Program) seeks to uplift the national data sharing system by focusing on priority policy areas to deliver collaborative, inter-jurisdictional projects and drive broader data sharing system reforms.

A key enabler of data sharing between Commonwealth, state and territory agencies, is trust. This requires mutual recognition and agreement of what characteristics define a trusted entity. Currently, there is no clear understanding of the best way to determine who is a 'trusted entity' when it comes to data sharing, impeding the effective and efficient exchange of information both within and across jurisdictions. While the ONDC Accreditation Framework is recognised nationally, there are challenges with its adoption and application to cross-jurisdictional data sharing initiatives.

This project under the Fourth Work Program aims to explore the general characteristics that define a 'trusted entity' for the purposes of national data sharing, and their application within existing frameworks, including the DAT Act. This project intends to highlight key opportunities for improvement with the current accreditation processes and offer an alternate approach. For example, one challenge with the current DAT Act accreditation process is that accreditation is tied to a department or agency. This means when teams who rely on that accreditation are moved into a different agency, their accreditation does not move with them, and they must pursue a new accreditation with their new agency. Additionally, a challenge faced by Accredited Users is that custodians often request information over and above what is required under the DAT Act accreditation process.

Target audience

While the guidance material and common attributes were developed by Commonwealth, state and territory governments and is suitable for their use, the guidance material can be used to aid in assessing any agency's trustworthiness in relation to data sharing.

What defines a 'trusted entity' and why do we need a definition?

For the purposes of data sharing, a trusted entity can be defined as an agency which can demonstrate that it has the attributes required to safely, securely and ethically manage another agency's data. A trusted entity is not limited to government agencies, but for the purpose of this project, data sharing is discussed within the context of the public sector national data sharing environment. All stakeholders involved in the creation and review of the project material were from government agencies.

Defining the attributes of a trusted entity will support improved data sharing by ensuring that there are common and agreed criteria which data custodians can use to assess if another agency will utilise shared data safely and securely. The guidance material will provide clear criteria for undertaking this assessment and demonstrate how criteria complement existing frameworks and resources.

Methodology

This project was co-led by the Queensland Government Department of Customer Services, Open Data and Small and Family Business with Services Australia and supported by a cross jurisdictional working group. The working group, comprised of representatives from selected Commonwealth, state and territory agencies (see Appendix 1), provided valuable information to the project team which contextualised and enhanced the guidance material.

The working group attended two workshops for the following activities:

- core features of a trusted entity
- advantages and disadvantages of current frameworks to assess trustworthiness
- potential ways to address limitations of existing frameworks
- pre-developed attributes of a trusted entity
- the level of assurance required to implement an attribute
- the importance of attributes based on different sensitivities of data
- preferred use cases.

Next steps

1. The guidance material is endorsed by Data and Digital Ministers, expected late 2025.
2. The guidance material is synthesised and published by the Department of Finance.
3. The guidance material is shared with the Data Availability and Transparency Act review team.
4. The lessons learnt will be documented and shared with the DDMM Data and Analytics Working Group to be leveraged by future Work Programs.

Guidance Material for Trusted Entities

How to use

The following guidance material documents attributes, which together define a trusted entity in the context of national data sharing.

An attribute is a specific, tangible and observable practice. An attribute aims to objectify trustworthiness and create a common recognition of practices which are evidence of trustworthiness. Please see the *Glossary* section for further definitions found in this report.

A trusted entity, for the purposes of national data sharing, would display or easily evidence the following attributes applicable to the data being shared. Trusted entities would be able to demonstrate the procedures and protocols which make up their data management and data governance environment. Not all attributes are relevant to all data sharing scenarios; however, a trusted entity is generally considered an 'expert' with high level data management practices, as demonstrated by the implementation of all attributes. The clear and consistent application of these attributes builds agency trust and confidence in safe and appropriate data sharing.

Alt text - This circular diagram titled 'Trusted Entity' illustrates the key components of a trusted entity. It is divided into five labelled segments: Transparency, Accountability, Data Management and Governance, Privacy, and Security. Each domain lists specific practices showing how these combined elements contribute to establishing a trusted entity.

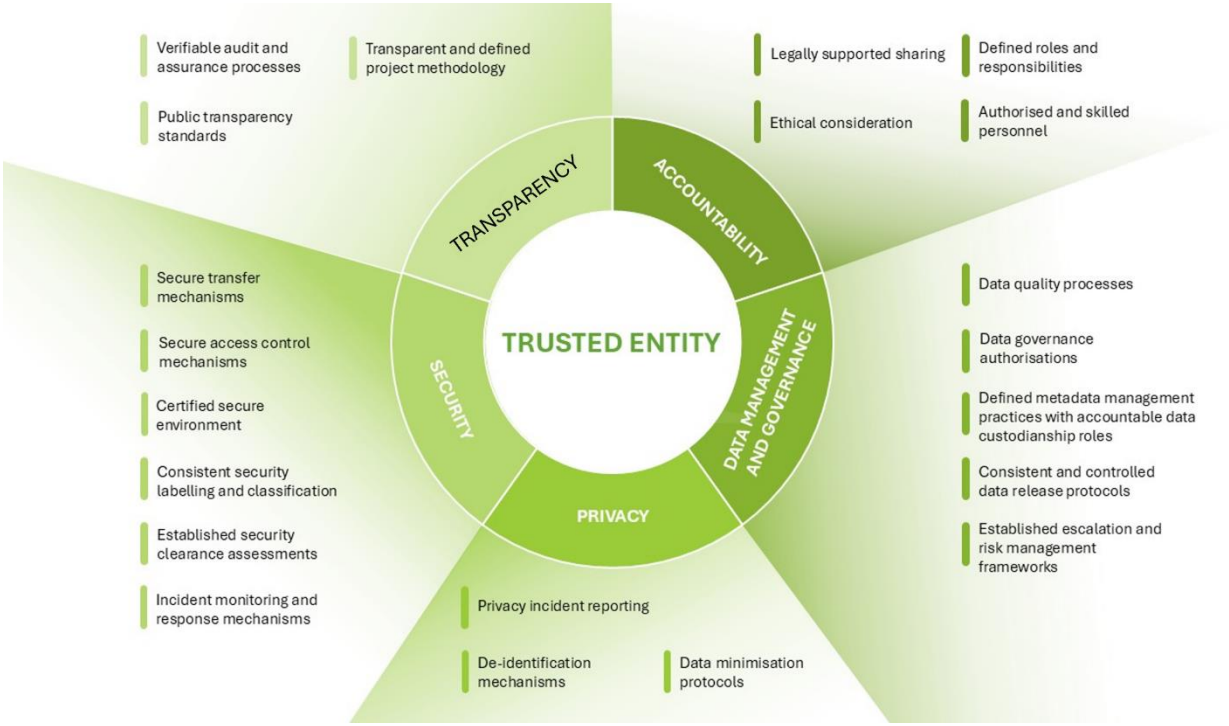

Image 1 – Summary of all trusted entity attributes.

The guidance material can be utilised in the following ways:

1. **Decision-making:** This guidance material has been developed to include questions related to each attribute to help data custodians assess trustworthiness and provide examples of relevant required information that should be gathered from a data requester to assess trustworthiness. There are many factors to consider when sharing data with another agency. The guidance material provides a simple format to consider what information is required to increase data sharing confidence. Data custodians should note that existing frameworks address many of these attributes and may find the matrix aligned with the ONDC accreditations (Appendix 2) helpful in determining if a data requester's accreditation or implemented framework addresses the required attributes.
2. **Policy development and implementation:** Data requesters can be proactive when requesting access to data by providing evidence of the required attributes when approaching a data custodian.
3. **Information resource:** This guidance material is complementary to many other useful and informative artefacts that exist in the national data sharing environment. The guidance material has a list of related resources (Appendix 3) to support the reasoning behind attributes and identify where further information is available.
4. **Capability uplift:** Data requesters can use this guidance material to proactively assess their internal practices and identify opportunities for improvement. The attributes provide common standards which data requesters can use to assess their own data management, security and governance environments.

Implementation

This material is for guidance only and it is up to an agency to determine whether an attribute and/or relevant guiding question is appropriate for specific data sharing activities based on the type of data being shared and the level of 'trustworthiness' required. Data sharing use-cases have been identified to help outline how this guidance material can be implemented or aligns with current approaches (Appendix 4-7). Data sharing should only occur when it is ethical and legal to do so, and the evidence of these attributes does not override any legal requirements for data sharing.

This guidance material only relates to the national data sharing environment, which primarily involves data sharing between and among Commonwealth, state and territory government agencies. This guidance material has been developed for implementation across the public sector but may also be useful or relevant to other data sharing scenarios.

The attributes can be applied on a situational basis based on the specific data sharing context. The degree to which an attribute is applied, if at all, will depend on the nature, volume, detail and sensitivity of the data requested. For example, data users requesting access to highly

sensitive data may be expected to provide evidence for most or all of the attributes. Requests for low sensitivity data may require evidence for fewer attributes. Depending on the data request, evidence of some attributes may not be required. For example, ethical requirements may not be necessary when shared data does not involve people.

Trusted entity attributes

Transparency

All government bodies have an ethical and often legal responsibility to be transparent. Transparency in the context of trusted entities relates to the ability of a data requester to provide clarity on relevant aspects of their data environment including how decisions are made and what shared data will be used for (for security-specific transparency approaches see *Security*). Transparency must be balanced with security, however the more information a data requester shares about their trusted entity attributes, the easier it is for a data custodian to assess their data sharing request. The transparency attributes below go beyond basic transparency achieved through appropriate documentation and explainability. They aim to outline a proactive practice which justifies ongoing data sharing.

The following attributes may be requested from a data requester to demonstrate transparency:

1. **Verifiable audit and assurance processes:** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.
2. **Public transparency standards:** The agency will have public-facing processes and/or standards for data release and publication.
3. **Transparent and defined project methodology:** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.

Attribute	Guiding questions
Verifiable audit and assurance processes	What audit processes does your agency undertake? What was the recent outcome of an audit? What assurance processes does your agency undertake? How do you ensure compliance to legal and ethical standards? Does your agency have a strategy or improvement plan for uplifting the data maturity of your agency? How does this align with your recent audit results? What data environment specific audit processes does your agency undertake? How frequently does this data environment get audited? Which aspects of the data environment were audited and at what security level are they operating? For example, only a single instance of a database operates at an Essential 8 level 3.

Public transparency standards	Does your agency have a public transparency statement? What documentation does your agency publish regarding its data processes and procedures? What documentation is available to staff to understand standards for data release? Does your agency have a public register of data sharing projects?
Transparent and defined project methodology	What documentation does this project have to detail the project methodology? Is there a risk register or a similar process in place to identify and mitigate risks within the project? What output vetting mechanisms are in place to ensure that only approved data is being released?

Accountability

Accountability in national data sharing ensures that agencies and stakeholders are held responsible for the ethical and lawful use of shared data. It promotes trust by demonstrating a commitment to fairness and compliance with established standards. Clear accountability mechanisms help mitigate risks such as data misuse or data breaches.

The following attributes may be requested from a data requester to demonstrate accountability:

1. **Legally supported sharing:** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.
2. **Ethical consideration:** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.
3. **Defined roles and responsibilities:** Agencies will have clear data roles and responsibilities to ensure accountability.
4. **Authorised and skilled personnel:** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.

Attribute	**Guiding questions**
Legally supported sharing	How does your agency manage data sharing agreements? Does it operate a data sharing register? What support does your agency have to understand the legal requirements of data sharing or the impact of legislation on the data your agency holds and hosts? How does your agency ensure legal compliance in data sharing? Has your agency considered the legal basis for requesting data? Does your agency undertake conformance assessments to ensure the shared data remains aligned with the specified purpose and legal authorisation for data sharing?
Ethical consideration	What ethics approval processes does your agency have? How does your agency ensure its ethics processes align with standards?

	Does this project/request require an ethics approval?
Defined roles and responsibilities	What data roles are evident within your agency? Does your agency have governance committees with responsibility for data management and issue resolution? What specific data governance processes within your agency ensure accountability and responsibility for data?
Authorised and skilled personnel	Is there agency specific training provided to data roles? What training is provided about data breach and risk management reporting? What training is provided about specific technical aspects of working with the data? Is training provided about the legal and non-legal consequences of data misuse?

Data Management and Governance

Data management and governance refers to the "exercise of authority and control (planning, implementation, monitoring and enforcement) over the management of data assets"[1]. The *Data Management and Governance* section refers to less technical data controls and focuses on the overall management of the agency's data ecosystem including roles, responsibilities and escalation pathways, and what procedures exist to prevent data disclosure incidents. The *Security* and *Privacy* sections outline attributes that implement actionable practices and mechanisms related to data security and privacy.

The following attributes may be requested from a data requester to demonstrate data management and governance:

1. **Data quality processes:** Data quality management plans will be implemented to ensure data integrity and compliance.
2. **Data governance authorisations:** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies' data governance priorities, dispute resolution processes and accountable data custodianship roles.
3. **Defined metadata management practices:** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.
4. **Consistent and controlled data release protocols:** Agencies will have clear operating models for data release, including for review, verification, and approval for release.
   Established escalation and risk management frameworks: Agencies will have established escalation pathways for managing risks and incidents. Projects will have

[1] DAMA International, *The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK)*, Technics Publications, 2015, p 69.

comprehensive risk management plans which consider privacy by design and security risk assessments.

Attribute	Guiding questions
Data quality processes	Does your agency have a data quality management plan? How is this governed? What guidance material is available to support personnel in understanding data quality controls specific to your agencies data? What data validation protocols are utilised in your agency? Does your agency track the quality of data over time?
Data governance authorisations	Does your agency have a data governance policy? How does your agency implement the data governance policy? How does your agency delineate between data governance and platform governance/security? What decision making bodies exist to manage data governance? Who in your agency has approval to release data? Does your agency have a data maturity up-lift plan or data governance forward work plan? What dispute resolution processes does your agency have regarding data governance and data requests?
Defined metadata management practices with accountable data custodianship roles	What frameworks inform your agency's metadata management functions? How does your agency maintain consistency across metadata collection? Do all data assets within your agency have an accountable officer? How does your agency capture data lineage information?
Consistent and controlled data release protocols	Describe your agency's data release operating model. What output vetting procedures does your agency implement? What mechanisms does your agency have in place to ensure custodian release requirements have been met?
Established escalation and risk management frameworks	What are your agency's data incident reporting and escalation procedures? Who are your agency's accountable officers related to risk management? Does the project have a risk management plan?

Security

Security is critical to protecting shared information from unauthorised access, breaches, and misuse. Robust security measures ensure that the integrity and confidentiality of data is maintained. Security attributes relate to the technical data operating environment and how technical controls are monitored and controlled in both cyber and information security contexts.

The following attributes may be requested from a data requester to demonstrate appropriate security controls:

1. **Secure transfer mechanisms:** Agencies have secure mechanisms for sensitive data transfer to prevent breaches.

2. **Secure access control mechanisms:** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.
3. **Certified secure environment:** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.
4. **Consistent security labelling and classification:** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.
5. **Established security clearance assessments:** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.
6. **Incident monitoring and response mechanisms:** Mechanisms for incident monitoring, identification, and response are in place.

Attribute	Guiding questions
Secure transfer mechanisms	What secure transfer mechanisms does your agency operate? How does your agency determine when to use secure transfer mechanisms? Does your secure transfer mechanism change depending on the type and/or size of the data being transferred?
Secure access control mechanisms	How does your agency monitor and control data access? How does your agency maintain up-to-date information about data users authorised to access data? How does your agency determine what safeguards to implement for a data asset or specific project/data request? Are any of these safeguards automated? Do access controls differ if a data requester accesses data physically or digitally?
Certified secure environment	Does your agency have a certified secure data environment? What certification does this environment have? When was it last audited or verified? How does your agency determine if a certified secure data environment is required for a data asset or data project? Will this data request require a certified secure data environment?
Consistent security labelling and classification	How consistent is the application of security labelling and classification within your agency? What security labelling and classification system does your agency use? How does your agency determine when it is appropriate to use this security labelling and classification system, e.g. state, territory or Commonwealth labels?
Established security clearance assessments	What security and clearance vetting procedures does your agency use?
Incident monitoring and response mechanisms	What incident monitoring procedures does your agency have? Does your agency implement automated incident monitoring and response controls? Has your agency responded to a reportable breach in the last 12 months? If not, how has your agency responded to a simulated breach?

Privacy

Privacy controls in the national data sharing ecosystem are essential to protecting individuals' personal information and maintaining public trust. Adhering to strict privacy standards when sharing personal information ensures that data is handled responsibly and used only for its intended purposes. Safeguarding personal information minimises the risk of harm, while upholding ethical and legal obligations. Where de-identification procedures are required, these attributes should be considered.

The following attributes may be requested from a data requester to demonstrate appropriate privacy controls:

1. **Data minimisation protocols:** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.
2. **De-identification mechanisms:** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.
3. **Privacy incident reporting:** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.

Attribute	Guiding questions
Data minimisation protocols	Does your agency have a data minimisation policy? Does your agency have formal retention and disposal policies? How does your agency implement the privacy by design principle? Is the scope of the data requested appropriate to achieve the specified purpose?
De-identification mechanisms	Does your agency have a data de-identification policy? How does your agency implement the separation principle? What processes does your agency implement to adhere with privacy legislation?
Privacy incident reporting	What data disclosure compliance does your agency implement? How does your agency ensure outputs are compliant with project agreements and legislation? How does your agency manage and respond to privacy complaints?

Glossary

Accountable officer: Officers are responsible for managing data assets to support secure, high-quality and accurate data. Officers operationalise relevant data governance and management policies by undertaking data management activities across the data lifecycle. Agencies may use different terms for accountable officers including data stewards.

Attribute: A specific, tangible and observable practice.

Data custodian: The custodian is the agency who has the control of the data asset and has the authority for sharing and disclosure.

Data sharing register: A centralised record that tracks and documents data sharing arrangements between agencies. An example is ONDC's Data Sharing Agreement Register.

Data requester: An agency seeking authorisation to access and use data they do not have authority over and/or do not have access to for a specific purpose

Data sharing request: A request from an agency to access and use data held by another agency, which is assessed by the agency's data custodian.

Appendix 1: Working group representation

Commonwealth

- Australian Bureau of Statistics (ABS)
- Australian Institute of Health and Wellbeing (AIHW)
- Australian Taxation Office (ATO)
- Department of Social Services
- Department of Education
- Department of Finance
- Services Australia
- Office of the National Data Commissioner (ONDC)^
- Department of Health and Aged Care^

States and Territories

- Australian Capital Territory (ACT)
- Victoria (Vic)
- New South Wales (NSW)
- Western Australia (WA)^
- Northern Territory (NT)
- South Australia (SA)*^
- Tasmania (Tas)*^
- Queensland (Qld)

* Jurisdictional representatives were not able to attend workshop 1.

^ Jurisdictional representatives were not able to attend workshop 2.

Appendix 2: ONDC alignment with trusted entity attributes

The Office of the National Data Commissioner (ONDC) has established a robust national accreditation framework to ensure that only those who can safely handle public data are able to participate in data sharing. To be accredited as a data users, entities must meet the following criteria:

- the entity has appropriate data management and governance policies and practices and an appropriately qualified individual in a position that has responsibility for data management and data governance for the entity
- the entities are able to minimise the risk of unauthorised access, sharing or loss of data
- the entity has the necessary skills and capability to ensure the privacy, protection and appropriate use of data, including the ability to manage risks in relation to those matters.

In addition to the above, accredited data service providers (ADSP) must also have the necessary policies, practices, skills and capability to perform one or more of the following data services: de-identification of data, secure access data and/or complex data integration.

Findings

Analysis of the trusted entity attributes compared to the ONDC accreditation framework shows that:

- ADSP accreditation aligns with all the attributes.
- User accreditation aligns with nearly all the attributes. Whilst most attributes are covered, there are three attributes which are mostly/partially aligned and two which are not expressly covered in the ONDC framework. The primary reason for non/partial alignment is that the attributes in question relate to data projects, which are generally covered in the ONDC's data sharing agreements and not in the accreditation framework. Information about the two attributes not covered may also be collected throughout the assessment process in adjacent questions, however, they are not expressly part of the original questionnaire set for user accreditation.

More information on the accreditation framework can be found on the ONDC website:

Expected characteristics for user accreditation | Office of the National Data Commissioner; and

Expected characteristics for data service provider accreditation | Office of the National Data Commissioner

Theme	Attribute	User Strong	User Partial	ADSP Strong	ADSP Partial
Transparency	**Verifiable audit and assurance processes:** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.	✓		✓	
Transparency	**Public transparency standards:** The agency will have public-facing processes and/or standards for data release and publication.	✓		✓	
Transparency	**Transparent and defined project methodology**: Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.		✓	✓	
Accountability	**Legally supported sharing:** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓		✓	
Accountability	**Ethical consideration:** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards. Agencies will have clear data roles and responsibilities to ensure accountability.	✓		✓	
Accountability	**Defined roles and responsibilities**: Agencies will have clear data roles and responsibilities to ensure accountability.	✓		✓	
Accountability	**Authorised and skilled personnel:** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.	✓		✓	
Data Management and Governance	**Data quality processes:** Data quality management plans will be implemented to ensure data integrity and compliance.	✓		✓	
Data Management and Governance	**Data governance authorisations:** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities, dispute resolution processes and accountable data custodianship roles.	✓		✓	
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles**: Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.	✓		✓	
Data Management and Governance	**Consistent and controlled data release protocols:** Agencies will have clear operating models for data release, including for review, verification, and approval for release.		✓	✓	
Data Management and Governance	**Established escalation and risk management frameworks**: Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.	✓		✓	
Security	**Secure transfer mechanisms**: Agencies have secure mechanisms for data transfer to prevent breaches.		✓	✓	

Theme	Attribute	User Strong	User Partial	ADSP Strong	ADSP Partial
Security	**Secure access control mechanisms:** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.	✓		✓	
Security	**Certified secure environment:** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.	✓		✓	
Security	**Consistent security labelling and classification:** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.	✓		✓	
Security	**Established security clearance assessments**: Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	✓		✓	
Security	**Incident monitoring and response mechanisms:** Mechanisms for incident monitoring, identification, and response are in place.	✓		✓	
Privacy	**Data minimisation protocols:** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.	✓		✓	
Privacy	**De-identification mechanisms**: Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.	✓		✓	
Privacy	**Privacy incident reporting:** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	✓		✓	

Appendix 3: Table of trusted entity attributes and guiding questions

Theme	Attribute	Guiding questions	Useful resources
Transparency	**Verifiable audit and assurance processes** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.	• What audit processes does your agency undertake? • What was the recent outcome of an audit? • What assurance processes does your agency undertake? • How do you ensure compliance to legal and ethical standards? • Does your agency have a strategy or improvement plan for uplifting the data maturity of your agency? How does this align with your recent audit results? • What data environment specific audit processes does your agency undertake? • How frequently does this data environment get audited? • Which aspects of the data environment were audited and at what security level are they operating? For example, only a single instance of a database operates at an Essential 8 level 3.	
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.	• Does your agency have a public transparency statement? • What documentation does your agency publish regarding your agency's its data processes and procedures? • What documentation is available to staff to understand standards for data release? • Does your agency have a public register of data sharing projects?	• Guidelines on data matching in Australian Government administration | OAIC
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk	• What documentation does this project have to detail the project methodology? • Is there a risk register or a similar process in place to identify and mitigate risks within the project?	

Theme	Attribute	Guiding questions	Useful resources
	management procedures, will be documented and shared with the relevant data custodian.	• What output vetting mechanisms are in place to ensure that only approved data is being released?	
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	• How does your agency manage data sharing agreements? Does it operate a data sharing register? • What support does your agency have to understand the legal requirements of data sharing or the impact of legislation on the data your agency holds and hosts? • How does your agency ensure legal compliance in data sharing? • Has your agency considered the legal basis for requesting data? • Does your agency undertake conformance assessments to ensure the shared data remains aligned with the specified purpose and legal authorisation for data sharing?	• Data Sharing Agreements | ONDC
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.	• What ethics approval processes does your agency have? • How does your agency ensure its ethics processes align with standards? • Does this project/request require an ethics approval?	• APS Data Ethics Framework | Department of Finance • APS Data Ethics Use Cases | Department of Finance • Australia's Artificial Intelligence Ethics Principles | Department of Industry Science and Resources • Interim guidance on government use of public generative AI tools | Digital Transformation Agency • Adoption of Artificial Intelligence in the Public Sector | Digital Transformation Agency

Theme	Attribute	Guiding questions	Useful resources
			• OECD Good Practice Principles for Data Ethics in the Public Sector | OECD
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	• What data roles are evident within your agency? • Does your agency have governance committees with responsibility for data management and issue resolution? • What specific data governance processes within your agency ensure accountability and responsibility for data?	• Data job role personas | Australian Public Service Commission • SES Accountabilities for Data | Department of Finance • Chief Data Officer Information Pack | Department of Finance • Best Practice Guide to Applying Data Sharing Principles | DPM&C • Protective Security Policy Framework - Section 2 | Department of Home Affairs • APS Data Ethics Framework | Department of Finance
Accountability	**Authorised and skilled personnel** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.	• Is there agency specific training provided to data roles? • What training is provided about data breach and risk management reporting? • What training is provided about specific technical aspects of working with the data? • Is training provided about the legal and non-legal consequences of data misuse?	• APS Data Capability Framework | Australian Public Service Commission • Protective Security Policy Framework - Section 16, 18 & 19 | Department of Home Affairs
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.	• Does your agency have a data quality management plan? How is this governed? • What guidance material is available to support personnel in understanding data quality controls specific to your agencies data? • What data validation protocols are utilised in your agency? • Does your agency track the quality of data over time?	• Australian Privacy Principle 10: Quality of personal information | OAIC

Theme	Attribute	Guiding questions	Useful resources
Data Management and Governance	**Data governance authorisations** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies' data governance priorities, dispute resolution processes and accountable data custodianship roles.	• Does your agency have a data governance policy? • How does your agency implement the data governance policy? • How does your agency delineate between data governance and platform governance/security? • What decision making bodies exist to manage data governance? • Who in your agency has approval to release data? • Does your agency have a data maturity up-lift plan or data governance forward work plan? • What dispute resolution processes does your agency have regarding data governance and data requests?	• Data Custodians | Data.gov.au • Establishing an information governance framework | National Archives of Australia • Data Integration Projects - Data Custodians | National Statistical Service
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.	• What frameworks inform your agency's metadata management functions? • How does your agency maintain consistency across metadata collection? • Do all data assets within your agency have an accountable officer? • How does your agency capture data lineage information?	• Australian Government Recordkeeping Metadata Standard | National Archives of Australia • Guide on Metadata Attributes | ONDC
Data Management and Governance	**Consistent and controlled data release protocols** Agencies will have clear operating models for data release, including for review, verification, and approval for release.	• Describe your agency's data release operating model. • What output vetting procedures does your agency implement? • What mechanisms does your agency have in place to ensure custodian release requirements have been met?	
Data Management and Governance	**Established escalation and risk management frameworks** Agencies will have established escalation pathways for managing risks and incidents. Projects will	• What are your agency's data incident reporting and escalation procedures? • Who are your agency's accountable officers related to risk management? • Does the project have a risk management plan?	• Commonwealth Risk Management Framework | Department of Finance

Theme	Attribute	Guiding questions	Useful resources
	have comprehensive risk management plans which consider privacy by design and security risk assessments.		• Establishing Risk Management Framework | Department of Finance • Risk Management Toolkit | Department of Finance • Five Safes framework | Australian Bureau of Statistics
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.	• What secure transfer mechanisms does your agency operate? • How does your agency determine when to use secure transfer mechanisms? • Does your secure transfer mechanism change depending on the type and/or size of the data being transferred?	
Security	**Secure access control mechanisms** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.	• How does your agency monitor and control data access? • How does your agency maintain up-to-date information about data users authorised to access data? • How does your agency determine what safeguards to implement for a data asset or specific project/data request? Are any of these safeguards automated? • Do access controls differ if a data requester accesses data physically or digitally?	
Security	**Certified secure environment** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.	• Does your agency have a certified secure data environment? • What certification does this environment have? When was it last audited or verified? • How does your agency determine if a certified secure data environment is required for a data asset or data project? • Will this data request require a certified secure data environment?	• Protective Security Policy Framework | Department of Home Affairs

Theme	Attribute	Guiding questions	Useful resources
Security	**Consistent security labelling and classification** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.	• How consistent is the application of security labelling and classification within your agency? • What security labelling and classification system does your agency use? How does your agency determine when it is appropriate to use this security labelling and classification system, e.g. state, territory or Commonwealth labels?	
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	• What security and clearance vetting procedures does your agency use?	
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.	• What incident monitoring procedures does your agency have? • Does your agency implement automated incident monitoring and response controls? • Has your agency responded to a reportable breach in the last 12 months? If not, how has your agency responded to a simulated breach?	
Privacy	**Data minimisation protocols** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.	• Does your agency have a data minimisation policy? • Does your agency have formal retention and disposal policies? • How does your agency implement the privacy by design principle? • Is the scope of the data requested appropriate to achieve the specified purpose?	• Australian Privacy Principle 11 Security of personal information | OAIC • Protective Security Policy Framework - Section 11 Information disposal | Department of Home Affairs • Guide to undertaking privacy impact assessments | OAIC • Privacy by design | OAIC • 10 steps to undertaking a privacy impact assessment | OAIC

Theme	Attribute	Guiding questions	Useful resources
			• Privacy impact assessment tool | OAIC • Assessing privacy risks in changed working environments: privacy impact assessments | OAIC
Privacy	**De-identification mechanisms** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.	• Does your agency have a data de-identification policy? • How does your agency implement the separation principle? • What processes does your agency implement to adhere with privacy legislation?	• Australian Privacy Principles guidelines | OAIC Australian Privacy Principle 11 Security of personal information | OAIC • De-identification and the Privacy Act | OAIC • De-Identification Decision-Making Framework | OAIC • Data confidentiality guide: Understanding re-identification | ABS • The separation principle | ABS
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	• What data disclosure compliance does your agency implement? • How does your agency ensure outputs are compliant with project agreements and legislation? • How does your agency manage and respond to privacy complaints?	• Notifiable data breaches | OAIC • Preventing, preparing for and responding to data breaches | OAIC • Handling privacy complaints | OAIC • Information privacy officers | Office of the Information Commissioner Queensland

Appendix 4: Use case - Victorian Department of Health and Department of Families, Fairness and Housing

Use case information

Identifying Characteristic	Details
Use case name	Integrated Data Resource (IDR)
Date	Ongoing
Data Requester	Victoria Department of Health (DH) Victoria Department of Families, Fairness and Housing (DFFH) Universities/External Researchers
Data Custodian	Victoria Department of Health (DH) Victoria Department of Families, Fairness and Housing (DFFH)
Data Characteristics	Personal Sensitive Information Health Records Unique Identifiers Health Services Data Social Services Data Education Data
Approved purpose	The IDR is used for research, policy development and service delivery.
Approved timeframe	Since 2017 with ongoing annual refreshes.
Legal basis for sharing	Relevant legislation that applies on a case-by-case basis includes: • *Children, Youth and Families Act 2005* (Vic) • *Disability Act 2006* (Vic) • *Drugs, Poisons and Controlled Substances Act 1981*(Vic) • *Health Services Act 1988* (Vic) • *Housing Act 1983* (Vic) • *Inquiries Act 2014* (Vic) • *Mental Health and Wellbeing Act 2022* (Vic) • *Public Health and Wellbeing Act 2008* (Vic) • *Royal Commissions Act 1902* (Cth) • *Victorian Data Sharing Act 2017* (Vic).
Additional Notes	The IDR is a data asset/sharing system that follows the 'share-once, use-often' principle and delivers many to many sharing. The IDR is managed by the Centre for Victorian Data Linkage (CVDL) in DH/DFFH. The IDR may only be accessed within the Victorian Data Access Linkage

Identifying Characteristic	Details
	Trust (VALT) which is a secure access environment. VALT is a certified Accredited Data Service Provider by the Office of the National Data Commissioner. The CVDL was established in 2009 as Victoria's specialist linkage unit and has extensive experience in undertaking data linkage and integration services for government and researchers over the past 15 years. The CVDL undertakes around 100 new linkage projects each year, and many ongoing projects with regular or periodic linkage. The CVDL has extensive experience in linking data sets across health, human services, justice, police and education. This includes linkage of some Commonwealth datasets, including MBS, PBS and the Australian Immunisation Register. The CVDL primarily undertakes linkage using identifiers, but also has experience with Privacy Preserving Record linkage, such as Bloom Filters. At any time, CVDL's total project workload averages around 170 projects, including new and ongoing projects, and a small number of project amendments. Researchers and Victorian departments can place an application to CVDL to access data in the IDR.

Alignment with attributes

The below table displays the alignment of the use case with the trusted entity attributes.

- **Strong alignment:** The data custodian required the data requester to provide significant evidence of the attribute to assess trustworthiness.
- **Partial alignment:** The data custodian required the data requester to provide some evidence of the attribute to assess trustworthiness.
- **Not assessed:** The data custodian did not assess the attribute, or it was not applicable.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Transparency	**Verifiable audit and assurance processes** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.			✓	Not applicable as the data is accessed in a secure access environment managed by the CVDL.
Transparency	**Public transparency standards**			✓	Not assessed as data custodians that provide data to the CVDL for linking are responsible for maintaining their own public transparency information.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	The agency will have public-facing processes and/or standards for data release and publication.				
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.	✓			Data requesters must submit a linkage request application, which includes a detailed project specification that specifies research/policy objectives and the requested data. The CVDL reviews the project specification and determines whether the project is feasible from both a technical and governance perspective. The CVDL team and the researcher work together to discuss potential issues in achieving the research objectives. This process enables the CVDL team to develop familiarity with different research methods and current research topics, while the researchers are provided with a better understanding of issues or limitations with the data requested. Output vetting is conducted jointly by the CVDL and data custodians.
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓			Requesters are required to sign data sharing agreements and/or confidentiality agreements.
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.		✓		Depending on the legislative enabler to access the IDR an ethics assessment may be required.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	✓			Requesters are asked to exhaustively list who will have access to the data and their roles and contact information.
Accountability	**Authorised and skilled personnel** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.			✓	While project applicants manage the authorisation and skill level of their personnel accessing the data, CVDL staff have strong alignment with this attribute. The CVDL and relevant data custodians review the project application and outputs from a technical and governance perspective to ensure data will be used appropriately.
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.			✓	Not applicable as the data quality of the IDR is managed by the CVDL.
Data Management and Governance	**Data governance authorisations** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities, dispute resolution processes and accountable data custodianship roles.	✓			
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.			✓	Not applicable as the metadata of the IDR is managed by the CVDL.
Data Management and Governance	**Consistent and controlled data release protocols**			✓	Not applicable as the CVDL has identified a standard list of variables that require confidentiality in consultation with data custodians. The CVDL reviews

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Agencies will have clear operating models for data release, including for review, verification, and approval for release.				the outputs from the VALT and only releases the outputs such as tables, PowerPoint slides and reports if they meet confidentiality requirements. Unit record data is not released from VALT.
Data Management and Governance	**Established escalation and risk management frameworks** Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.		✓		As data is accessed in the VALT, many of the risks associated with data access and data breaches are mitigated or managed by the CVDL team. Requesters and their agencies are required to comply with any mandated privacy breach reporting procedures. Data requesters and users are required to implement safeguards to minimise confidentiality risks by assessing the project risk against the ABS's Five Safe principles.
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.			✓	Not applicable as data is only accessible in VALT.
Security	**Secure access control mechanisms** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.			✓	Not applicable as data is only accessible in VALT.
Security	**Certified secure environment** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.			✓	Not applicable as data is only accessible in VALT.
Security	**Consistent security labelling and classification**			✓	Not applicable as security labelling and classification is managed by CVDL.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.				
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	✓			Where appropriate security clearance assessments are required to access data in CVDL.
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.			✓	Not applicable as incident monitoring is managed by CVDL.
Privacy	**Data minimisation protocols** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.	✓			The CVDL team will ask requesters to fill out a technical specifications document which includes the research question and the specific data items required from the IDR. This is reviewed and assessed by the CVDL team to ensure that only the data items necessary for the specific research questions are provided.
Privacy	**De-identification mechanisms** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.	✓			Requesters must meet confidentiality requirements to receive outputs from the VALT project specific virtual machine such as tables, PowerPoint slides and reports.
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	✓			Requesters and their agencies are required to comply with any mandated privacy breach reporting procedures.

Appendix 5: Use case - Western Australian Government and the Department of Health, Disability and Aged Care

Use case information

Identifying Characteristic	Details
Use case name	PeopleWA
Date	09/2025
Data Requester	Various – government, researchers, not-for-profits, Aboriginal Community-Controlled Organisations
Data Custodian	Multiple
Data Characteristics	<20gb unit record de-identified data in a secure environment
Approved purpose	Research, policy development, service delivery/improvement, Closing the Gap
Approved timeframe	Various – a couple of months to ongoing requests
Legal basis for sharing	PeopleWA Memorandum of Understanding (MOU) *Privacy and Responsible Information Sharing Act 2024* (WA)
Additional Notes	This is general information on PeopleWA, rather than being related to a specific applicant seeking PeopleWA data. Requested data can only be accessed within PeopleWA's secure access environment. The PeopleWA team undertake all relevant output vetting in line with the terms and conditions of PeopleWA and data custodians' requirements. As the asset is de-identified, the legal basis for sharing is not critical. If the data request meets the project requirements of access, then the data can be shared.

Alignment with attributes

The below table displays the alignment of the use case with the trusted entity attributes.

- **Strong alignment:** The data custodian required the data requester to provide significant evidence of the attribute to assess trustworthiness.
- **Partial alignment:** The data custodian required the data requester to provide some evidence of the attribute to assess trustworthiness.
- **Not assessed:** The data custodian did not assess the attribute, or it was not applicable.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Transparency	**Verifiable audit and assurance processes** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.			✓	Not applicable as data can only be accessed in PeopleWA's secure access environment.
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.			✓	Not assessed as data custodians that provide data to the CVDL for linking are responsible for maintaining their own public transparency information.
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.	✓			Data requesters are required to complete an application form that requests evidence of project methodologies. PeopleWA does complete some output vetting and risk management processes on behalf of the requester.
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓			PeopleWA want to understand how a requesting agency ensures staff understand and adhere to PeopleWA's terms, including MOUs and data use agreements.
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.	✓			Data requesters need to advise ethics processes in place, including who they apply to, compliance and repercussions for non-compliance. Requesters should be able to demonstrate a track record of ethical data use, both at the individual and sector level, and should reflect a commitment to responsible data stewardship over time.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	✓			Data requesters are required to have clearly defined roles for each project as covered by PeopleWA's terms and conditions.
Accountability	**Authorised and skilled personnel** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.	✓			
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.			✓	Not applicable as PeopleWA manage the quality of the asset and its outputs.
Data Management and Governance	**Data governance authorisations** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities, dispute resolution processes and accountable data custodianship roles.		✓		PeopleWA are particularly focused on how the data is restricted to only staff approved to work on the project.
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.			✓	Not applicable as PeopleWA manage the metadata of the asset.
Data Management and Governance	**Consistent and controlled data release protocols**			✓	Not applicable as PeopleWA manage data release procedures.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Agencies will have clear operating models for data release, including for review, verification, and approval for release.				
Data Management and Governance	**Established escalation and risk management frameworks** Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.	✓			PeopleWA requires agencies to have risk management procedures.
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.			✓	Not applicable as data is only accessible via PeopleWA's secure environment.
Security	**Secure access control mechanisms** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.	✓			PeopleWA want to ensure that an agency's controls and safeguards align with theirs especially in scenarios involving remote work, geographic restrictions, and dual roles**.**
Security	**Certified secure environment** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.			✓	Not applicable as data is only accessible via PeopleWA's secure environment.
Security	**Consistent security labelling and classification** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.		✓		Data requesters must provide information on how they track and enforce labelling and classification procedures where they have received a sensitive approved export.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.			✓	Not applicable as PeopleWA conduct vetting processes instead of requesting agency.
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.	✓			
Privacy	**Data minimisation protocols** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.			✓	Not applicable as the PeopleWA team undertake any data minimisation and de-identification procedures. Terms and conditions of use state that requesters cannot re-identify or link the data to other sources.
Privacy	**De-identification mechanisms** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.			✓	Not applicable as the PeopleWA team undertake any data minimisation and de-identification procedures. Terms and conditions of use state that requesters cannot re-identify or link the data to other sources.
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	✓			PeopleWA require evidence of an agency's processes to handle data breaches.

Appendix 6: Use case - New South Wales Department of Communities and Justice

Use case information

Identifying Characteristic	Details
Use case name	NSW Human Services Dataset
Date	09/2025
Data Requester	Multiple
Data Custodian	NSW Department of Communities and Justice with the following data partners: • NSW Bureau of Crime Statistics and Research and Youth Justice NSW • NSW Registry of Births Deaths and Marriages • Legal Aid NSW • NSW Police Force • NSW Ministry of Health • NSW Department of Education • NSW Education Standards Authority • Revenue NSW.
Data Characteristics	The Human Services Dataset (HSDS) contains de-identified data collected through the administration of different NSW Government services and some Commonwealth Government supports (i.e. welfare and medical benefits). Data is de-identified and contains information from all NSW residents born on or after 1 January 1990 and their relatives. The current version of the asset is the 2023 HSDS which includes data up to and including 30 June 2023. The list of datasets available within the 2023 HSDS can be found on the HSDS website.
Approved purpose	Approved purposes are contained in the Public Interest Direction and Health Public Interest Direction (PIDs) made by the NSW Privacy Commissioner for the Human Services Dataset Project. Two threshold criteria inform considerations of whether a proposal meets the Approved Purposes: 1. Conformance to two guiding principles: a) the proposed activity must facilitate or enable the Project Objectives, which is to ensure that effort and funding across government is focussed on interventions that will improve long-term outcomes for Vulnerable Children or Young Persons and their families at the earliest opportunity b) the data will be used to design and deliver better government services for Vulnerable Children or Young Persons and their families. 2. Under the overarching rubric of these guiding principles, the data that is collected and used will:

Identifying Characteristic	Details
	a) provide specific identifications of trends and gaps in government service usage and delivery; b) facilitate services that are better tailored to the needs of Vulnerable Children or Young Persons and their families both now and in the future; c) deliver clear evidence on service, support and program effectiveness and a detailed view of resource allocation and gaps; d) provide valuable information for research and planning of government supports and services; and e) enable Participating Agencies and other government agencies to meet the Project Objectives by implementing new policy and program development directed to improving outcomes for Vulnerable Children or Young Persons and their families.
Approved timeframe	Ongoing request with annual refresh.
Legal basis for sharing	The creation and use of the Human Services Data set (HSDS) is enabled by the PIDs made for the Human Services Dataset Project by the NSW Privacy Commissioner under s41(1) of the *Privacy and Personal Information Protection Act 1998* and s62(1) of the *Health Records and Information Privacy Act 2002* in New South Wales, Australia. This direction was made on 20 December 2024 and will expire on 13 January 2026. The PIDs govern the extent to which the NSW Department of Communities and Justice and participating agencies may depart from the Information Privacy Principles and Health Privacy Principles for the purposes of the Project. This allows government agencies to collect, use and disclose data in ways that would otherwise be precluded by privacy legislation. In the case of the HSDS, the PIDs permit the collection and linkage of administrative datasets across government agencies, so that the data can be re-used to design and deliver better government services for vulnerable children or young persons and their families.
Additional Notes	Access and use of the HSDS is governed by the Department of Communities and Justice according to the following guidelines: • The Guidelines for access to and use of the Human Services Dataset (HSDS) • Application forms for accessing the Human Services Dataset (HSDS) • Human Services Dataset application process flow chart The data linkage for this project is performed by the Centre for Health Record Linkage (CheReL) and the dataset is hosted by the NSW Data Analytics Centre within the NSW Department of Customer Service. To protect privacy of individuals, the HSDS can only be accessed by authorised personnel in secure environments for approved projects. The secure environments are available within the NSW Data Analytics Centre (DAC) and ABS DataLab (for data linked with Commonwealth assets).

Alignment with attributes

The below table displays the alignment of the use case with the trusted entity attributes.

- **Strong alignment:** The data custodian required the data requester to provide significant evidence of the attribute to assess trustworthiness.
- **Partial alignment:** The data custodian required the data requester to provide some evidence of the attribute to assess trustworthiness.

- **Not assessed:** The data custodian did not assess the attribute, or it was not applicable.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
Transparency	**Verifiable audit and assurance processes** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.			✓	Data can only be accessed in the NSW DAC and ABS secure environments. These environments along with governance and privacy procedures are annually audited to ensure compliance with the PIDs made by the NSW Privacy Commissioner. The DAC secure environment is accredited by the ONDC.
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.			✓	Approved Analysts are not required to publish processes. NSW DCJ provides publicly available resources on their website about data collection and use.
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.	✓			Analysts requesting access to data for analytics purposes are required to complete a project proposal which includes provide research methods.
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓			The project must comply with the PIDs from the NSW Information and Privacy Commissioner and the *Data Sharing (Government Sector) Act 2015* (NSW) and the public interest directions from the NSW Information and Privacy Commissioner. There are two public interest directions related to this project for the: *1) Privacy and Personal Information Protection Act 1998* 2) *Health Records and Information Privacy Act 2002* Approved Analysts are legally obliged to use the information only for Approved Purposes, adopt best privacy, security and de-

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
					identification practices, and keep the information confidential, secure and protected from loss, unauthorised use or disclosure. Approved Analysts are required to sign a legally binding data privacy and confidentiality agreement.
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.	✓			Projects are required to obtain ethics approvals if undertaking these specific activities: • Aboriginal Health and Medical Research Council for those disaggregating or using Aboriginal data in analysis (other than describing the sample) • NSW Population Health Services Research Ethics Committee for projects accessing the NSW Health data or when they want to link additional datasets to the HSDS • DCJ Artificial Intelligence (AI) Ethical Review Board if the project is using AI techniques
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.		✓		The Human Services Data Partnership provides governance over the HSDS in accordance with legislative and the requirements of the PIDs.
Accountability	**Authorised and skilled personnel** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.	✓			To be eligible for approval to access the HSDS, an analyst must: • demonstrate evidence of technical ability in data or statistical analysis • sign a legally binding data privacy and confidentiality agreement • confirm that they have read and understood DCJ's data breach policy • have a current Working with Children Check • have a current National Police Check (Criminal Records Check) • be willing and available to undertake training on appropriate use of data, and privacy, confidentiality and security obligations

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
					Approved Analysts must undertake training before accessing data and undertake privacy verification checks.
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.			✓	Data providers are required to check and validate their own data prior to supply. Data providers update their notes each year and are required to supply a data quality statement with each annual refresh of data.
Data Management and Governance	**Data governance authorisations** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities, dispute resolution processes and accountable data custodianship roles.			✓	Family and Community Services Insights, Analysis and Research and its contracted entities are required to comply with NSW Government policies and frameworks.
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.			✓	Data providers maintain the metadata of their assets and the DAC manages metadata for the HSDS.
Data Management and Governance	**Consistent and controlled data release protocols** Agencies will have clear operating models for data release, including for review, verification, and approval for release.		✓		Output checking processes are a combination of data requester and data custodian actions. Analytic output checkpoints must be passed prior to external release (including any release to the requesting agency or party) from the secure analytical platform: a) All analytical outputs must be aggregated, and where necessary, confidentialised, before it can be taken out of the DAC's Advanced Secure Analytics Lab (ASAL) or ABS DataLab analytic environment. As part of this process, the Approved Analyst must check the outputs to ensure

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
					these do not contain any personal information and that individuals cannot be re-identified. b) Aggregated outputs are checked by the DAC and FACSIAR (as the governance lead) to ensure that these outputs do not contain personal information and individuals cannot be re-identified. c) Members of the Human Services Dataset Governance Advisory Committee and Authorised Reviewers from relevant agencies review the aggregated outputs for disclosure and publication risks. d) The Data Custodian's approval may be sought for release of aggregated outputs that relate to significant projects or sensitive topics.
Data Management and Governance	**Established escalation and risk management frameworks** Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.			✓	The NSW Department of Communities and Justice operates a principal department and collaborative shared Audit and Risk Committee in line with the TPP20-08- Internal Audit and Risk Management Policy for the General Government Sector.
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.			✓	Data is only ever transferred between the Government data partners and CheReL for linkage using CheReL's secure file transfer and data handling processes. CheReL securely transfers this information to: • the DAC's ASAL – for linked NSW datasets; and • ABS DataLab – for data linked with the Commonwealth PLIDA data.
Security	**Secure access control mechanisms** Agencies will implement data safeguards, use secure access environments appropriate to			✓	The HSDS is accessed in a secure access environment, either in the DAC's ASAL or ABS DataLab.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
	the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.				
Security	**Certified secure environment** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.			✓	The HSDS is accessed in a secure access environment, either in the DAC's ASAL or ABS DataLab. Both these secure access environments are accredited by the ONDC.
Security	**Consistent security labelling and classification** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.			✓	The DAC ensures there is appropriate security labelling and classification of data.
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	✓			Approved analysts are required to have a current Working with Children Check and have a current National Police Check (Criminal Records Check).
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.	✓			Under the PIDs, the Chair is obliged to notify the NSW Privacy Commissioner "where any entity involved in the Project collects, uses or discloses Personal Information other than in accordance with this Direction". DCJ is also required under the Mandatory Notification of Data Breach Scheme to notify the Privacy Commissioner and affected individuals of eligible data breaches (unless a relevant exemption applies).
Privacy	**Data minimisation protocols** Agencies will implement the privacy by design principle, including minimising the			✓	The HSDS governance model enforces strict de-identification, access controls, and output vetting. CHeReL links data for approved analysts.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
	collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.				
Privacy	**De-identification mechanisms** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.	✓			Approved Analysts are required to adopt best practice privacy, security and de-identification practices to minimise disclosure risk, such as the Human Services De-Identification Decision Making Framework and the Five Safes Framework. Approved Analysts are required to apply privacy verification checks to the de-identified, linked unit-level data, including de-identification, aggregation and confidentialisation. Approved Analysts must conduct these checks prior to commencing data analytics, and before the external or public release of any statistical outputs.
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	✓			HSDS has a data breach policy which contains a copy of the data breach reporting form to be filled out if required.

Appendix 7: Use case – Commonwealth Department of Health, Disability and Ageing

Use case information

Identifying Characteristic	Details
Use case name	Supplying health data for the Person-Level Integrated Data Asset (PLIDA)
Date	Ongoing
Data Requester	The Australian Bureau of Statistics (ABS)
Data Custodian	The Department of Health, Disability and Ageing (DHDA)
Data Characteristics	Health data included: • Australian Immunisation Register (AIR) • Medicare Benefits Schedule (MBS) • Pharmaceutical Benefits Scheme (PBS)
Approved purpose	Analysis, research and statistical purposes
Approved timeframe	Data supplied to the ABS for period specified in the Public Interest Certificate (PIC).
Legal basis for sharing	Data sharing is authorised under the *National Health Act 1953*, *Health Insurance Act 1973* and *Australian Immunisation Register Act 2015*. DHDA issues PICs under these Acts. Data provided to the ABS is also protected by the *Census and Statistics Act 1905*.
Additional Notes	DHDA has data sharing arrangements with trusted data brokers to supply health data for approved purposes. An example is provision of data for the Person-Level Integrated Data Asset (PLIDA), a linked data asset that is managed by the ABS. The ABS provides access to PLIDA data to approved users in the ABS DataLab environment (or other ABS secure environments). Requests to conduct projects using PLIDA undergo an assessment and approval process, managed by the ABS. For a project to be approved, the ABS and the Data Custodians (the agencies responsible for the source data, in this case DHDA) must agree to the proposed use of the data. The ABS provides project proposals requesting PLIDA data to DHDA via a secure 'myData' Portal. The DHDA reviews and determines if the project proposal meets DHDA requirements, and if so, approves the proposal. The ABS then provides the researchers with access to PLIDA. The ABS is an Accredited Data Service Provider (ADSP) which means the National Data Commissioner has deemed the ABS capable of handling public sector data and minimising risk of unauthorised access or use. The ABS is authorised to undertake complex data integration, de-identification, and provide secure data access services to support data sharing. The DHDA leverages the ABS' accreditation (which is subject to ongoing monitoring by the Office of the National Data Commissioner) to be assured that the ABS consistently implements and performs appropriate data handling processes.

Alignment with attributes

The below table displays the alignment of the use case with the trusted entity attributes.

- **Strong alignment:** The data custodian required the data requester to provide significant evidence of the attribute to assess trustworthiness.
- **Partial alignment:** The data custodian required the data requester to provide some evidence of the attribute to assess trustworthiness.
- **Not assessed:** The data custodian did not assess the attribute, or it was not applicable.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Transparency	**Verifiable audit and assurance processes** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.		✓		DHDA knows the ABS is subject to multiple compliance and assurance processes to meet Australian Government requirements, such as adhering to the Protective Security Policy Framework, and Infosec Registered Assessors Program (IRAP) cyber-security reviews. This information is available on the ABS website. DHDA also relies on the ABS's ONDC accreditation to trust that appropriate audit and assurance processes are in place.
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.	✓			The ABS publishes information on its website about how PLIDA data can be accessed for research. DHDA leverages the many documents ABS publishes to have assurance of processes and standards.
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.	✓			The ABS uses the Five Safes Framework to facilitate safe data access and release. The ABS, in their role as data broker, provides DHDA with comprehensive research documentation for potential projects. This allows DHDA to make informed decisions about the appropriate use of their data.
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear	✓			Data is supplied to PLIDA through a PIC from DHDA. The ABS provides approved researchers with secure access to integrated data under the Census and Statistics Act. The ABS' clear legislative authority for making data available in ways

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	documentation such as agreements and data sharing registers.				that protect privacy and maintain confidentiality provides assurance to DHDA when utilising them as a data broker.
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.	✓			At the discretion of DHDA, Human Research Ethics Committee approvals are required for PLIDA projects that involve DHDA data. The ABS also conducts regular Privacy Impact Assessments of PLIDA.
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	✓			DHDA knows the ABS has processes in place to ensure only appropriate people can access data, such as application of the separation principle. ABS staff are also bound by the secrecy provisions in the Census and Statistics Act. DHDA also relies on ABS's ONDC accreditation to provide assurance that the ABS has appropriately trained staff.
Accountability	**Authorised and skilled personnel** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.	✓			The ABS is an Accredited Data Service Provider (ADSP) which means they have proven they have appropriately trained and experienced staff to manage data. The ABS provides technical training for personnel working with PLIDA data, and researchers requesting access to PLIDA must complete PLIDA training to be onboarded onto the PLIDA environment. This aligns with DHDA requirements.
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.	✓			The ABS applies data quality management plans which includes guidance and validation protocols for personnel accessing PLIDA.
Data Management and Governance	**Data governance authorisations** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities,	✓			Specific authorisation roles are defined in the PIC which authorises DHDA to share data with ABS.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	dispute resolution processes and accountable data custodianship roles.				
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.			✓	Not applicable as DHDA data custodians are responsible for data assets in PLIDA including the preparation of metadata and source data.
Data Management and Governance	**Consistent and controlled data release protocols** Agencies will have clear operating models for data release, including for review, verification, and approval for release.	✓			DHDA knows the ABS applies automated and manual data release controls to PLIDA outputs. Information about these controls is provided to Data Custodians and users.
Data Management and Governance	**Established escalation and risk management frameworks** Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.			✓	The ABS and DHDA as Commonwealth entities are bound by the *Privacy Act 1988* (Cth) and required to follow the same notifiable data breach reporting procedures as outlined by the Commonwealth Information Commissioner.
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.			✓	Not applicable as DHDA data is accessed in secure access environments by PLIDA researchers.
Security	**Secure access control mechanisms** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.	✓			The ABS manages access to PLIDA with access restricted to authorised users in secure environments (i.e. ABS DataLab). The ABS only permits access to the DataLab environment once requesters have completed the Responsible Officer and Individual Officer legal undertakings and appropriate training. The ABS review and update access controls with safeguards

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
					tailored to data sensitivity. This information is available on the ABS website.
Security	**Certified secure environment** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.	✓			PLIDA data is only accessed in certified ABS secure environments.
Security	**Consistent security labelling and classification** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.			✓	The ABS and DHDA follow the same Commonwealth standards on security labelling and classification.
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	✓			The ABS has security clearance and vetting procedures in place, consistent with Australian Government Security Vetting Agency standards.
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.	✓			The ABS has incident monitoring and response procedures in place, including automated controls and breach response protocols. Real and simulated breaches are managed as part of ongoing risk management. The ABS and DHDA adhere to the same Commonwealth legislative requirements for data breach reporting.
Privacy	**Data minimisation protocols** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.		✓		The ABS publicly publishes the PLIDA Privacy Statement on how personal information is treated in PLIDA. The ABS and DHDA work together with researchers to ensure data minimisation protocols are in place.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Privacy	**De-identification mechanisms** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.	✓			The ABS applies deidentification techniques and implements functional separation (or roles) in all data integration projects. The ABS and DHDA adhere to portfolio and privacy legislation and manage re-identification risks. The ABS publishes information on these controls on their website.
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.			✓	The ABS and DHDA will manage and respond to data breaches in accordance with the Commonwealth notifiable data breach conditions from the Information Commissioner.

Appendix 8: Use case – Queensland Government Department of Health

Use case information

Use case name	Data sharing between Queensland Health and the Brisbane North Primary Health Network
Date	03/2024
Data Requester	Brisbane North Primary Health Network (BN PHN) (and other Queensland Primary Health Networks).
Data Custodian	Queensland Health (QH)
Data Characteristics	The Deed of Disclosure between QH and the BN PHN states that QH may disclose data considered confidential (including patient-level) data from a range of data collections if approved by the relevant custodians, including the Queensland Hospital Admitted Patient Data Collection (QHAPDC) and the Emergency Department Collection (EDC). Given the breadth of data held by QH, there is not a prescribed/exclusive list of data and characteristics listed in the Deed as the relevant data to be shared is negotiated on a project-by-project basis.
Approved purpose	The data may only be disclosed by QH to BN PHN for the sole purpose of evaluating, managing, monitoring or planning primary and population-based health services.
Approved timeframe	On-going
Legal basis for sharing	By establishing the BN PHN as a 'prescribed entity' under Queensland legislation, select QH confidential data may be disclosed to the BN PHN under the following Statutory Provision/s: • Section 150(b) of the Hospital and Health Boards Act 2011 • Section 225(b) of the Public Health Act 2005 • Section 147(4)(h)(ii) of the Private Health Facilities Act 1999 for the sole purpose of evaluating, managing, monitoring or planning of primary and population-based health services.
Additional Notes	Queensland Health has an ongoing partnership with the Primary Health Networks to develop and deliver sustainable primary health care and preventative health care programs for Queenslanders. Data sharing underpins development, implementation, monitoring and evaluation of these programs which may be department-led programmes (e.g. Health Needs Assessments, Local Area Needs Assessments) to Hospital and Health Services (HHS) aimed at local communities. Having the BN PHN listed as a 'prescribed entity' under the relevant statutory provisions allows for QH to enter into local data sharing agreements specific to individual programmes, without the administrative burden of having to obtain legal approval to disclose confidential data on each occasion (as this legal approval has been pre-obtained for specific purposes as identified above).

Alignment with attributes

The below table displays the alignment of the use case with the trusted entity attributes.

- **Strong alignment:** The data custodian required the data requester to provide significant evidence of the attribute to assess trustworthiness.
- **Partial alignment:** The data custodian required the data requester to provide some evidence of the attribute to assess trustworthiness.
- **Not assessed:** The data custodian did not assess the attribute, or it was not applicable.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Transparency	**Verifiable audit and assurance processes** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.	✓			The Deed of Disclosure between QH and BN PHN outlines the BN PHNs obligations regarding security and appropriate usage of data, including processes for security audits and protection of data.
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.			✓	Whilst not a requirement in the Deed, BN PHN does have a public facing privacy statement.
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared			✓	The Deed between QH and BN PHN outlines the responsibilities regarding confidentiality, privacy, security, unauthorised use and information privacy. Specific projects may outline additional requirements.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	with the relevant data custodian.				
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓			This project is supported under Section 150(b) of the Hospital and Health Boards Act 2011; Section 225(b) of the Public Health Act 2005 and Section 147(4)(h)(ii) of the Private Health Facilities Act 1999.
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.			✓	Data can only be used for evaluating, managing, monitoring or planning of primary and population-based health services. Data shared is often administrative in nature, with low-risk ethical considerations.
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	✓			The Deed outlines high level responsibilities of the BN PHN in receiving, handling, storing and using the data. Specific projects may outline additional requirements. PHNs adhere to national data governance frameworks, and the Primary Health Insights platform has common permission requirements for access, roles and responsibilities to consistently protect data.
Accountability	**Authorised and skilled personnel** Personnel will have the knowledge, skills, authorisation and training to use data appropriately,			✓	The agreement between QH and BN PHN does not identify individual personnel nor specific role types, however the BN PHN complies with Australian privacy legislation (including the Australian Privacy Principles) and with the terms and conditions of data sharing agreements. BN PHN also participates in the National Governance Framework (developed by the PHN Cooperatives

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	including training in data breach and risk management.				National Data Governance Committee) which includes procedures for data breaches and risk identification.
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.			✓	This would be the responsibility of the local QH area sharing data and BN PHN on a project-by-project basis.
Data Management and Governance	**Data governance authorisations** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities, dispute resolution processes and accountable data custodianship roles.		✓		The Deed of Disclosure between QH and BN PHN outlines high-level responsibilities for security, privacy, dispute resolution and information privacy. Further responsibilities can be established as required. BN PHN also participates in the National Governance Framework (developed by the PHN Cooperatives National Data Governance Committee).
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.			✓	QH retains authority over the metadata as the custodian of the data.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Data Management and Governance	**Consistent and controlled data release protocols** Agencies will have clear operating models for data release, including for review, verification, and approval for release.	✓			The Deed between QH and BN PHN outlines high-level responsibilities for security, privacy, destruction of data, data reproduction and information privacy. The Deed also outlines restrictions on secondary data provision. Further responsibilities can be established as required.
Data Management and Governance	**Established escalation and risk management frameworks** Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.	✓			The Deed of Disclosure identifies BN PHNs responsibilities regarding insurance, indemnity, dispute resolution, security and notification of disclosure. Further responsibilities can be established as required. BN PHN also participates in the National Governance Framework (developed by the PHN Cooperatives National Data Governance Committee) which includes procedures for data breaches (among others) and risk identification.
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.	✓			The Deed between QH and BN PHN outlines responsibilities regarding encryption of data transfer, data security, information privacy, insurance and indemnity.
Security	**Secure access control mechanisms** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with	✓			The Deed outlines the requirements of BN PHN to protect the security of data disclosed by QH. BN PHN stores and accesses data via their 'Primary Health Insights' (PHI) platform, which has a public security statement. The PHI platform utilises robust role-based access controls and multi factor authentication for all users.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	appropriate security clearances.				
Security	**Certified secure environment** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.	✓			BN PHN utilises PHI platform to safely store and analyse data. PHI is a Microsoft Azure platform which is accredited to ISO 27001 compliance and has met the requirements of the Australian Government for secure storage of both 'sensitive' and 'protected' information through the Infosec Registered Assessors Program (IRAP).
Security	**Consistent security labelling and classification** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.			✓	The PHI platform is accredited to ISO 27001 and has met requirements to store 'protected' and 'sensitive' information as per the IRAP program. The National Governance Framework for all PHNs which supports data asset handling and governance.
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.			✓	
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.	✓			The Deed outlines BN PHNs responsibilities regarding system monitoring, data security audits and disclosure breaches. Further requirements may be identified in local data sharing agreements.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Privacy	**Data minimisation protocols** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.			✓	BN PHN only receive data for a particular purpose, as agreed by both QH and the PHN.
Privacy	**De-identification mechanisms** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.		✓		The Deed states that the BN PHN cannot share, release and provide access to any data that could identify a person or health facility. Specific requirements can be outlined in data sharing agreements as appropriate. The BN PHN must ensure its processes related to safe handling of data adhere to the Office of the Australian Information Commissioner (OAIC) guidelines.
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	✓			The Deed between QH and BN PHN states the legislative responsibility regarding confidential information, and requirements relating to security and disclosure breaches. The BN PHN also is obligated to report data breaches to the OAIC.