APPENDIX 11: Synthetic data request assessment outcomes form

Request and Assessment Outcomes Form

Project name:	
Project description:	
Who is the Data Requestor organisation?	
Who is the responsible data user / lead at the Data Requestor?	
Who is the Data Provider organisation?	
Who is the accountable decision-maker at the Data Provider who will review / approve the synthetic data request?	
Any other key personnel involved in gathering information and / or conducting the assessments required under this framework:	
Who is responsible? *DR = Data Requestor, DP = Data Provider*	
Step 1: Use Case Assessment	
DR	1. Describe the use case
DR / DP to confirm	2. Is this use case for a clear 'public benefit' purpose related to providing health services, and where the expected benefits from the use case are related to consumer health or health system outcomes?

DR / DP to confirm	3. Do you anticipate a synthetic dataset will be suitable for this use case? *With a synthetic dataset, there must only be a very low risk that the dataset can identify or disclose information about individuals.*
DP	4. Has the Data Provider communicated publicly and broadly to their health consumers that they will use synthetic data about consumers for public benefit projects, such as those related to improving health outcomes for consumers and for the health system?
DP	5. Is the proposed use case acceptable under this framework? *Data Provider must complete the **Use Case Assessment** (Appendix 4) to assist with answering this question.*
DP	6. Are there other impacts or ethical reasons that mean the request should not proceed? *Data Provider must complete the **Impact Assessment** (Appendix 5) to assist with answering this question.*
Step 2: Assess and prepare source data	
DP / with assistance from the DR	7. What data is being requested and is it available? *Identify and describe the data elements or datasets being requested, including the type of data and any other parameters or characteristics (e.g. geography, date/time ranges, any important features or limitations). A data specification form may be used.*
DP / with assistance from the DR	8. Is the source data being requested relevant for the use case?
DP / with assistance from the DR	9. Does the Data Provider hold and control the source data? *If 'no', the request should be considered 'complex' and will require further assessment and action before the request can proceed under this framework. See Appendices 7 and 8 for further guidance.*

DP / with assistance from the DR	10. Does the source data need to be enriched or linked to datasets held by *other* organisations? *If 'yes', the request should be considered 'complex' and will require further assessment and action before the request can proceed under this framework. See Appendices 7 and 8 for further guidance.*
DP	11. Are there any other limitations or restrictions on using the source data to generate synthetic data?
DP	12. Have you identified the system and/or repository that the data will need to be extracted from?
DP	13. What format will be used for the synthetic data?
DP / with assistance from the DR	14. Are you satisfied that the data being requested is the minimum amount of information needed for the use case? *A subset of the source data may need to be prepared to only include what is needed to generate the synthetic dataset.* *All data and fields containing directly identifying information (such as names, addresses, phone numbers, date of birth, date of death, unique identifiers such as patient numbers, Medicare numbers or drivers licence numbers) must be removed or augmented to reduce the risk they will be 'leaked' via the synthetic dataset. If these fields cannot be removed or appropriately augmented, organisations must be aware of the risk of data leakage and the potential for heightened re-identification risk that must be assessed and managed prior to any use or sharing.*
DP	15. Have you created a data quality statement to be supplied to the Data Requestor that addresses the accuracy, completeness, reliability and currency of the source data which will be used to generate the synthetic data?

DP	16. Can you provide metadata and/or other material (such as a data dictionary) to help the Data Requestor to understand the nature of the source data and the resulting synthetic data?
DP / with assistance from the DR	17. Do the Data Requestor’s personnel possess the technical requirements and knowledge to effectively use the data for the identified purpose?
DP / with assistance from the DR	18. Is the source data ‘fit for purpose’ for the use case? *Data Provider must complete the* ***Technical Assessment*** *(Appendix 6) to assist with answering this question.*
Step 3: Generating the synthetic data	
DP / with assistance from the DR if needed	19. What model will be used to generate the synthetic data?
DP / with assistance from the DR if needed	20. Who will generate the synthetic data? *If third-party expertise is required, specify the third party and the arrangement (e.g. expertise provided via a contracting arrangement with the Data Provider).* *If the Data Provider will release the source data to another organisation (whether or not that is the Data Requestor) to generate the synthetic data, the request should be considered ‘complex’ and will require further assessment and action before it can proceed under this framework. See Appendices 7 and 8 for further guidance.*
DP	21. Have you documented the model and details of the parameters used to train the model?

DP	22. After the synthetic data has been generated, will the model be stored separately in a secure manner or otherwise destroyed?
Step 4: Assess and manage re-identification risks	
DP	23. Has the dataset been reviewed and treated for re-identification risks? *See Appendix 7 for further guidance on de-identification techniques.*
DP / with assistance from the DR if needed	24. Has a Re-Identification Risk Assessment been completed? What was the resulting level of re-identification risk? *Where the risk level is more than very low, the request should be considered ‘complex’ and will require further assessment and action before the request can proceed under this framework. The project must be paused until a lawful pathway to proceed has been determined. See Appendices 7 and 8 for further guidance.*
Step 5: Manage residual privacy risks	
DP & DR	25. Where and how will the data be stored? *For example:* • *In the Data Provider’s storage system (on-premises)* • *In the Data Requestor’s storage system (on-premises)* • *In a storage system provided by a third party (e.g. third-party cloud platform provider) (specify the third party, the storage system and which organisation is responsible for the system)*
DP & DR	26. Who is responsible for the security of the storage system (including access management)? Provide details.
DP or DR	27. Describe the data security measures that will be in place to protect the data (provide details) *Describe the security measures that will be put in place to protect the data during storage and access, including from misuse, interference and loss, as well as unauthorised access, modification or disclosure.*

	Measures can include technical and organisational controls. For example/if applicable: • *access is limited to those who have been approved by the Data Custodian at the organisation that will hold the synthetic data* • *periodic audits of who has access, and removal when access is no longer warranted* • *user login credentials and minimum password requirements* • *maintenance of access logs and audit trails* • *any additional authentication measures* • *data encryption* • *data to be handled in accordance with information security policies (name and link to (if possible) any key policies)* • *system restricts users from downloading or saving data to local drives (if applicable)* • *staff training*
DP or DR	28. In which state or territory will the data be stored? *If the data will be stored in a system held or controlled by a SA public sector agency, a WA public sector agency prior to 1 July 2026, or eld by a private sector entity with an annual turnover under $3 million, a legal risk assessment must first be carried out and appropriate contract clauses must be used in the Data Sharing Agreement to ensure compliance with applicable privacy principles (see Appendix 11, 'Privacy obligations regulating the use and disclosure of health information' for further information).*
DP	29. What mechanism will be used for sharing the data securely with the Data Requestor? *For example:* • *Secure online data transfer site (e.g. Secure file transfer protocol/SFTP)* • *Secure end-to-end transfer system with password protection (e.g. OneDrive)* • *Other (specify)*

DP and DR	30. Will any third parties (including contracted service providers) be permitted access to the data? If third parties will be permitted access, describe the controls in place to protect the data. *For example, vendor due diligence prior to onboarding, appropriate privacy and security contractual clauses (including data breach notification requirements), ongoing performance and relationship management*.
DR	31. What are the expected outputs from the analysis of the synthetic dataset? Will the outputs be shared outside of the Data Requestor organisation?
DP or DR	32. How long will the synthetic dataset be retained? Provide a rationale for the retention period. *Retention periods could include:* • *For the duration of the project* • *For a specified time after the end of the project* • *Indefinitely (include a justification/rationale for the retention period)* *Specify any legal obligations to retain data and the required timeframes*
DP or DR	33. What will happen with the data at the end of the retention period? *For example, data to be destroyed, returned, retained (or 'other') at the end of the retention period. Include any other details or requirements regarding destruction or return of data (e.g. such as disposal methods, transfer methods for return, evidence or attestation of destruction, or applicable policies or standards).*
DP or DR	34. What controls will be put in place to protect the data after sharing? *Examples include:* • *Data Sharing Agreement* • *Data Use Agreements*

	- *Assurance activities, e.g. audit of compliance with Data Sharing Agreement, compliance attestations, etc.*		
DP	35. Are you satisfied that the synthetic data can be safely shared in the circumstances? *Data Provider must complete the **Safety Assessment** (Appendix 10) to assist with answering this question.*		
DP and / DR	36. Any additional comments, conditions or recommendations regarding the synthetic data request:		
DP	37. Is the synthetic data request approved?		
To be completed by the accountable decision-maker at the Data Provider			
Signature:		Date:	
Name / title			