

APPENDIX 8: Decision tree for complex synthetic health data scenarios

The five-step approach for generating and using synthetic health data outlined in this Framework should be sufficient for managing privacy risks where a [synthetic health data request](#) involves a fairly straightforward workflow.

A sample scenario of a straightforward workflow would be as follows:

1. A SynD organisation (e.g. the University of Sydney as the [Data Requestor](#)) requests another SynD organisation (e.g. NT Health as the [Data Provider](#)) to generate a synthetic health dataset using [source data](#) already held by that [Data Provider](#), for an acceptable use case.
2. The [source data](#) is fit for purpose, and the resulting synthetic health dataset is considered robustly and effectively [de-identified](#) with only a [very low risk](#) of re-identification. The data [utility](#) is appropriate for the use case.
3. The [Data Provider](#) provides the [Data Requestor](#) with access to the synthetic health dataset in a secure manner and continues to have an appropriate level of oversight of the handling of the dataset.

However, for scenarios that involve more complex workflows, *or* where any of the steps in this Framework cannot be successfully completed, material privacy and legal compliance risks may emerge. In these cases, additional steps are needed to manage these risks.

The decision tree below anticipates some of these more complex scenarios where additional steps and assessments are required, to ensure the [synthetic health data request](#) can proceed lawfully.

