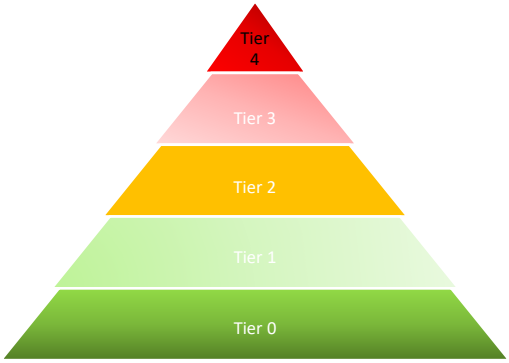
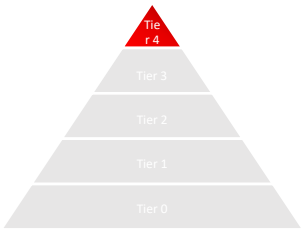
Sensitivity Tiers and Assessment

Turing Data Safe haven tiers and flow diagram



Our model goes from Tier 0 – publicly available, open information – to Tier 4 – personal data where disclosure poses a substantial risk to safety.

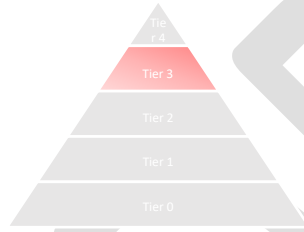
This guidance below should give you an idea of how to classify your data for the Data Study Group. It should be referenced in conjunction with the classification flowchart.



Tier 4 environments are for:

- Personal data where disclosure poses a substantial threat to safety, security or health
- Commercial or governmental data which could be subject to attack by sophisticated, well-resourced and determined actors such as nation states

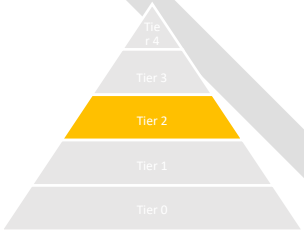
Tier 4 data is **not** appropriate for Data Study Group use.



Tier 3 environments are for:

- Pseudonymized or synthetic data where confidence in the quality of anonymization is weak
- Commercial data which is sensitive
- Commercial or governmental data which could be subject to attack by attackers with bounded capabilities such as hackers

---



Tier 2 environments are for:

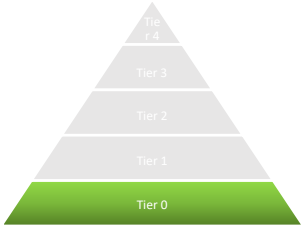
- Pseudonymized or synthetic data where confidence in the quality of anonymization is strong
- Commercial data where risks from disclosure are low

Tier 2 data should be very unlikely to be subject to targeted attack.

Tier 1 environments are for:

- Data intended for eventual but not immediate publication
- Datasets where the only risks of disclosure are to the researchers' competitive advantage
- Pseudonymized or synthetic data where confidence in the quality of anonymization is absolute
- Commercial information where the consequences of disclosure are so low as to be trivial

---



Tier 0 environments are for:

- Publicly available, openly published information
- Data which is intended for immediate publication

How to assess project Tiers: