APPENDIX 7: De-identification techniques

De-identification aims to break the link between a dataset and an individual in the real world, so that the disclosure of a fact (such as that a patient is being treated at this hospital for HIV) cannot be linked back to an identified individual (the patient is Sally Citizen).

The harm being prevented here is known as 'identity disclosure'. Identity disclosure - which occurs when data is re-identified - can arise in one of two ways: by either matching a person to data, or matching data to a person. Checking the robustness of de-identification techniques should involve testing your dataset for both these types of re-identification risk.[48]

> "De-identification is not a single technique, but a collection of approaches, algorithms, and tools that can be applied to different kinds of data with differing levels of effectiveness. In general, privacy protection improves as more aggressive de-identification techniques are employed, but less utility remains in the resulting dataset."[49]

There is no single 'correct' way to de-identify data. It is an exercise in risk management. Re-identification risks will differ according to the type of data, its context, and other factors. Trade-offs need to be made between minimising the risk of re-identification, and maximising the value of the data. The wrong de-identification method can fail to reduce privacy risk, and/or decrease data utility.

Examples of de-identification techniques include:

- aggregation
- suppression (remove identifiers or other overtly identifying data fields)
- generalisation (e.g. replace exact date of birth with a date range like '35-44 year olds')
- pseudonymisation (replace direct identifiers with statistical linkage keys (SLKs), or encrypt or hash identifiers), and
- perturbation (adding noise, micro-aggregation or data-swapping).

There are multiple ways to ~~two main~~ measure de-identification, including:

- K-anonymity
- Differential Privacy, and

[48] When considering re-identification risks, the GDPR makes clear that the identifiability of data should not be considered in a vacuum. Instead, "account should be taken of all the means reasonably likely to be used … to identify the natural person directly or indirectly", including "objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments"; see GDPR Recital 26.

[49] Simson L. Garfinkel, NISTIR 8053: De-Identification of Personal Information, National Institute of Standards and Technology, US Department of Commerce, 2015, p.1; available at http://dx.doi.org/10.6028/NIST.IR.8053.

- Measuring the likelihood of successful inference attacks

K-anonymity is a framework that provides a measure for testing the likelihood that an individual can be distinguished from others in a dataset. It does so by measuring uniqueness within a dataset.

Under the k-anonymity approach to de-identification, data fields are categorised as direct identifiers, indirect or quasi-identifiers, or attributes. K-anonymity involves manipulating the direct and indirect identifiers until the desired level of re-identification risk is reached.

> "A dataset is said to be k-anonymous if, for every combination of quasi-identifiers, there are at least k matching records".[50]

This means that within a given dataset, the smallest number of people who share the same identifiers (whether direct or indirect) is 'k'. So k=6 means that six people within that dataset share the same identifiers, and you can't distinguish between those six people any further. Another way of phrasing this is that if k=6, every individual in the dataset is indistinguishable from at least five other people.

The higher you set 'k', the lower the risk of re-identification (based on their identifiers, at least), because there are more people in the 'crowd' who share the same characteristics.

The more multi-dimensional the data is, the more difficult it is to achieve k-anonymity. For example, within a group, gender alone may not enable any individual to be singled out from a particular at dataset. However, gender + age + postcode might make some individuals unique in that dataset.

In particular, k-anonymity assumes that unit level data is presented in such a way that each 'unit' of data relates to one individual, and that no individual is represented more than once in the dataset.

Differential Privacy is a mathematical concept, the definition of which is

> "that the result of an analysis of a dataset should be roughly the same before and after the addition or removal of a single data record."[51]

In other words, differential privacy means that adding or removing one particular person's record from a dataset makes so little difference to the database's statistical properties, such as query results, that it is not feasible to tell whether any particular person's record is included or not. The aim of differential privacy is to "[allow] researchers to draw lessons and

[50] Simson L. Garfinkel, NISTIR 8053: De-Identification of Personal Information, National Institute of Standards and Technology, US Department of Commerce, 2015, pp.20-21; available at http://dx.doi.org/10.6028/NIST.IR.8053.
[51] Simson L. Garfinkel, NISTIR 8053: De-Identification of Personal Information, National Institute of Standards and Technology, US Department of Commerce, 2015, p.7; available at http://dx.doi.org/10.6028/NIST.IR.8053.

derive valuable conclusions from a data set without being able to determine whether or not such conclusions are based on the personal data of any given individual”.[52]

Differential privacy is therefore defined as having been achieved if the result of an analysis of a dataset is indistinguishable before and after the addition or removal of a single data record. Differential privacy works best on large datasets, where data can be perturbed (by adding noise) without impacting too greatly on the validity of the analysis of the whole.

Data perturbation may suit open data projects involving the release of large datasets, where the identifiers have already been controlled for (either because the dataset never included identifiers by design; or because there is confidence that each individual is represented by only one unit record and k-anonymity techniques have already been applied), but where the attributes might expose patterns of behaviour that could potentially reveal identity.

Measuring the likelihood of successful inference attacks includes both assessing the likelihood of both membership inference attacks and attribute inference attacks. ***[SynD members: do you have some wording that can be added here to flesh out how these risks are measured and how they evaluate de-identification efforts?]***

The effectiveness of these different approaches to de-identification will depend on the . These different approaches to de-identification suggest, but don’t dictate, which methods are best to achieve ‘de-identified’ data. For example, k-anonymity will focus on techniques such as suppression or generalisation of identifiers from a dataset, while differential privacy might involve data perturbation techniques such as adding noise.

Further Resources

HealthStats NSW: Privacy issues and the reporting of small numbers

Any other relevant resources and / or organisational policies can be set out / linked to here

CSIRO & OAIC, *The De-Identification Decision-Making Framework*. Available at: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-decision-making-framework (the OAIC notes that, as this guide was produced in 2017, certain information it contains may now be out of date)

Office of the Victorian Information Commissioner (OVIC), *The Limitations of De-Identification – Protecting Unit-Record Level Personal Information*, available at: https://ovic.vic.gov.au/privacy/resources-for-organisations/the-limitations-of-de-identification-protecting-unit-record-level-personal-information/

[52] Omer Tene and Jules Polonetsky, “Judged by the Tin Man: Individual Rights in the Age of Big Data”, 15 August 2013, p.11, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311040

Office of the Information Commissioner Queensland, *Report on Privacy and Public Data: Managing re-identification risk*, available at: https://www.oic.qld.gov.au/__data/assets/pdf_file/0016/43045/Privacy-and-public-data-managing-re-identification-risk.pdf

ISO/IEC 27559:2022
Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework
https://www.iso.org/standard/71677.html

ISO/IEC 27554:2024
Information security, cybersecurity and privacy protection — Application of ISO 31000 for assessment of identity-related risk
https://www.iso.org/standard/71672.html

ISO/TS 14265:2024
Health informatics — Classification of purposes for processing personal health information
https://www.iso.org/standard/83447.html

ISO 25237:2017
Health informatics — Pseudonymization
https://www.iso.org/standard/63553.html