Northern Ireland Ambulance Service
Health and Social Care Trust

Staff Guidance - Anonymisation: Managing Data Protection: Information Commission Office Risk code of Practice Summary

---

What is anonymisation?

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information. The Data Protection Act controls how the Northern Ireland Ambulance Servie HSC Trust (NIAS) uses 'personal data' – that is, information which allows individuals to be identified.

NIAS is increasingly reliant on anonymisation techniques to enable wider use of personal data. NIAS is therefore adopting the use of the Information Commissioner Code of Practice: Managing Data Protection Risk Code of Practice. The code of practice explains the issues surrounding the anonymisation of personal data, and the disclosure of data once it has been anonymised. The code describes the steps NIAS can take to ensure that anonymisation is conducted effectively, while retaining useful data. These relates to all datasets across the Trust that contain levels of personal and sensitive information held in for example, Command and Control records, Human Resource records, Clinical Audit records etc.

The full code is available on the Trust's intranet site.

- The code shows that anonymisation of personal data is possible and desirable. Anonymisation ensures the availability of rich data resources while protecting individuals' personal data.

- Anonymisation is of particular relevance now, given the increased amount of information being made publicly available through Open Data initiatives and through individuals posting their own personal data online. An Open Data initiative currently operates within Northern Ireland which NIAS will be required to provide anonymised datasets to.

- The code explains the data protection implications of anonymising personal data. It contains, in full, the Information Commissioner's recommendations about anonymising personal data and assessing the risks associated with producing – and particularly publishing – anonymised data.

- The Data Protection Act 1998 should not prevent the anonymisation of personal data, given that it safeguards individual's privacy and is a practical example of the 'privacy by design' principles that data protection law promotes. But effective anonymisation does depend on a sound understanding of what constitutes personal data.

- Adopting the good practice recommendations in the code will help you to anonymise personal data so that individuals' privacy is not compromised by an inappropriate disclosure of personal data through re-identification.

- Advantages of using anonymising data where appropriate over person data include:

  - ✓ It protects against inappropriate disclosure of personal data; few legal restrictions apply;
  - ✓ It can be easier to use anonymised data in new and different ways because of the DPAs purpose limitation rules do not apply;
  - ✓ It allows NIAS to make information public while still complying with data protection obligations, and;
  - ✓ The disclosure of anonymised data is not disclosure of personal data – even when the Data Controller holds the key to re-identification to take place.

- NIAS will ensure that we have in place an effective governance structure in relation to their anonymisation processes. It will help you if the ICO receives a complaint about processing of personal data, including its anonymisation, or if we carry out an audit.

- In the event of the Information Commissioner investigating an issue arising from the anonymisation of personal data, he will take the good practice advice in this code into account.

- It is essential to carry out a thorough risk analysis on the likelihood and potential consequences of re-identification at the initial stage of producing and disclosing anonymised data.

- The risk of re-identification will differ according to the way the anonymised information is disclosed, shared or published:

  - ✓ Publication to the world at large is more risky than limited access;
  - ✓ Limited access allows the disclosure of 'richer data', but relies on robust governance arrangements.

- In cases where the consequences of re-identification of anonymised data could be significant – for example, because it would leave an individual open to damage, distress or financial loss - organisations should:

  - ✓ Seek the data subject's consent for the disclosure of the data explaining its possible consequences;
  - ✓ Adopt a more rigorous form of risk analysis and anonymisation; or
  - ✓ In some scenarios, only disclose within a properly constituted closed community and with specific safeguards in place.

- The Information Commissioner will generally take the view that where an organisation collects personal data through a re-identification process without individuals' knowledge or consent, it will be collecting personal data unlawful and could be subject to enforcement action.

- You don't always have to seek consent to anonymise personal data– it is likely one of the other conditions will provide a viable alternative. Provided that there is no likelihood of the anonymisation causing unwarranted damage or distress to individuals, and you can satisfy another condition – there will be no need to obtain consent as a means of legitimising the processing.

- Spatial information includes post-codes, GPS data and map references and will sometimes constitute personal data. There is no simple rule for handling this kind of data under the DPA. The approach you take to handling spatial information will be dependent on available related information and the size of the dataset you are dealing with.

- To avoid disclosure of personal data, and to reduce re-identification risk, for some types of spatial information, you should consider removing or blurring certain elements – for example, using partial post-codes rather than full post-codes.

- Small numbers in small geographical areas present increased risk – but this does not mean that small numbers should be removed automatically. For example, removing numbers relating to five or ten individuals or fewer may be a reasonable rule of thumb for minimising risk of identification in a proactive disclosure scenario.

- While the DPA will not prevent organisations from disclosing anonymised information, there may be some other reasons for withholding such data. When disclosing anonymised data, you may wish to consider the whether disclosures are compatible with the rights provided under the European Convention on Human Rights, or other relevant statutory prohibitions.

- Section 33 of the DPA is useful for NIAS which process personal data for research as it provides an exemption from compliance with certain parts of the DPA. The exemption is only relevant where personal data (rather than anonymised data) is used for research. Notwithstanding the provisions in section 33, it is good practice to plan for the publication of anonymised data as early as is practicable, which will help minimise or negate the risk to individuals.

For further information about Anonymisation: Managing Data Protection Risk Code of Practice Visit www.nias.hscni.net or www.ico.gov.uk