Developers guidance

Understanding types of health and care data

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 20 January 2023

Reviewed by: Health and Care IG Panel

Two types of health and care data can be distinguished to help you determine when the relevant legal and regulatory frameworks apply:

1. Data that relates to identified or identifiable individuals. **Confidential patient and service-user information** includes information that identifies or could be used to identify the individual (such as name and address), relating to, or in connection with, an identified or identifiable individual's past or present use of services (NHS or adult social care). This broad definition is in recognition of the importance of maintaining trust in health and care services, so that all individuals can be reassured in fully engaging with these services that their confidential information will only be used in ways that they reasonably expect.
2. Data that does not or no longer relates to identified or identifiable individuals **(anonymous data)**, such that the process of rendering the data anonymous means that the laws that apply to the modified data no longer apply to those receiving it.

Important note: data can be rendered anonymous in different ways. One way is by applying a machine-learning model to a real-world dataset. For example, real-world derived synthetic data can be generated by creating average results from a large set of data. This type of synthetic data can be distinguished from synthetic data that is totally made up with no relationship to anyone living or dead (hereafter called 'artificial data').

When data is generated to statistically mimic real-world data that it replaces, an assessment should be carried out regarding the likelihood of individuals being re-identified from the synthesised data. If necessary, additional safeguards may be needed to make sure that any re-identification risks (or other privacy risks) are sufficiently remote so that it may be considered anonymous.

Get more information:

ICO guidance on anonymisation, pseudonymisation, and privacy enhancing technology

