Adopters guidance

# Data access and re-identification risk intervention



## This is required guidance

It is legally required and it is an essential activity.

## From:

- Health Research Authority (HRA)

## This Guide covers:

- England

**Reviewed by:** Health and Care IG Panel

If you share, or provide access to, health and care data with the developers of a digital technology, you will need to consider the identifiability of the data. Adopters should not provide personal data unless strictly necessary to achieve a particular lawful purpose (with a lawful basis).

Any arrangement should be covered by a data sharing agreement, or a controller-processor contract, which will need to be prepared and signed by you and the developer.

If you are proposing to share confidential patient or service-user information outside your health or care setting, you should first make sure you have a lawful basis in place to share such information under the common law duty of confidentiality. Unauthorised access would constitute a breach.

# How to process anonymous data

Data rendered anonymous data is no longer considered personal data. See ICO's guidance on what is personal data?

Usually, you do not need consent or approval to process data that has been rendered anonymous before you have received it. This is because, when a person cannot be identified from data, its use is not subject to the common law duty of confidentiality or data protection legislation.

**Important note**: Determining whether the data you wish to use is personal data or not is your responsibility and you should carry out your assessment helped by the latest guidance on ICO's website. You should check ICO's website from time to time as new guidance becomes available.

In this process of anonymising personal data, an organisation must modify data in order to share it with a third-party organisation, while also putting in place additional processes and other appropriate safeguards to prevent the third-party using means (reasonably likely available to them) to re-identify the individual, and thus to make sure it meets effective anonymisation requirements. A key benefit of this is that is reduces risk of a data breach of personal data, which could cause harm to patients and service users.

A lawful basis is required to anonymise personal data (see step 4 of complying with the UK GDPR). A lawful basis under the common law duty of confidentiality is required to disclose confidential patient or service-user information with someone who would then apply anonymisation processes to the data. Where the anonymisation is to be

 

performed by someone who does not have a legitimate relationship, there will be a disclosure, albeit solely for the purposes of anonymising it, and a legal basis to lift the common law duty of confidentiality is required. This would likely apply to the technology developer. In such circumstances, you must obtain the prior explicit consent from the individual, unless there is another legal basis available to you, as described further below.

**Important note**: this type of consent (explicit consent from an individual to permit confidential information to be shared outside the team directly caring for them) is separate from UK GDPR consent. However, the rules on consent do not conflict. This is because they are about consent for different things under 2 different sets of regulations that were created to work together without tension. For more on this distinction, see the NHS Transformation Directorate's guidance on consent and confidential patient information and the HRA's guidance on consent in research.

**Important note**: if you are reliant on using anonymous data to fall outside the law, you must make sure the data you want to use has been rendered anonymous, and you have evidence to demonstrate that it is no longer personal data, before using or disclosing it. Any onward transfer of (or remote access to) the data may change its status to be personal data again, depending on any additional information and means available to the onward recipient. Therefore, the effectiveness of your anonymisation strategy must be determined on a case-by-case basis, using the latest guidance provided on ICO's website.

# A note on pseudonymisation

Pseudonymisation is a technique applied in circumstances when the link between individuals and the data that relates to them needs to be reduced but not removed entirely. It involves replacing information in a data set that directly identifies an individual. For example, it could involve replacing an NHS number, a name, or an address, with a unique number or code (a pseudonym). This has the effect that those receiving it cannot identify an individual directly from that data without access to additional information held separately and securely elsewhere (for example, the 'key' that would enable matching the pseudonym to the removed direct identifiers).

UK GDPR legislation applies to personal data. The UK GDPR considers that pseudonymisation is not an anonymisation technique but a type of safeguard. This is because, by itself, applying the technique does not render personal data anonymous in the hands of those receiving the information. More is required, such as putting in place a data-sharing or processing contract and other appropriate safeguards to prevent re-identification by the recipient. The determining factor is whether the recipient can use the modified data (on its own, or in conjunction with other available data using

 

reasonable means) to identify an individual. You need to consider the processes necessary to make sure data is rendered anonymous or effectively anonymous. See ICO's guidance on anonymisation, pseudonymisation and privacy enhancing technologies

If you are using pseudonymised data, make sure you understand your legal obligations described in how to process health and care data.

 