

# RESEARCH DATA SHARING KEY PRINCIPLES

## PERSONAL DATA

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

### DATA MINIMISATION

Personal data must only be collected where necessary/legally justifiable, and hence each required data-point should have a justifiable purpose.

### OPT-OUT

Where possible, individuals that have chosen to opt-out of any data processing for research must have their data removed. This will not be possible (or necessary) where truly anonymous datasets are sourced.

### ANONYMOUS / PSEUDONYMOUS

Wherever possible, data should be anonymised or pseudonymised. Pseudonymised data can fall within the scope of GDPR depending on how difficult it is to attribute the pseudonym (eg. Incident number) to a particular individual.

### ENCRYPTION

Datasets containing personal data must be sent securely and encrypted to reduce (though does not eliminate) the likelihood of loss or interception. The GDPR takes a 'risk' based approach to data security, and encryption reduces the likelihood of data loss where used appropriately.

## ANONYMOUS?

### NAMES

Remove entirely unless necessary, and strongly consider alternatives

### ADDRESSES

Remove entirely unless necessary, and consider scope of location required. The trust considers the first half and one digit of the second half of the post code (eg. SO21 2??) acceptable, unless where combined with other information in the dataset this could reasonably reveal the patient.

### PHONE NUMBERS

Remove entirely. Incomplete phone numbers can be useful, and numbers can identify a specific location

### INCIDENT DETAILS

Remove unless necessary—the incident number consists of the data of the incident and an identifier.

### TIMESTAMPS

Consider whether these could be combined with other details to reasonably reveal the particular individual

## MEDICAL INFORMATION

Certain treatment or medical history combined with a small amount of data could reasonably reveal an individual, especially with rare conditions.