Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust

GDPR and Data Protection Act 2018

Guidance for Researchers

1. Definitions

'Personal data'
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.

'Directly'
Information allows direct identification. Such information includes name, picture, phone number, address.

'Indirectly'
Information allows indirect identification. Such information includes a username or IP Address.
Note that personal data that has been pseudonymised – e.g. key-coded –may still be personal data depending on how difficult it is to attribute the pseudonym to a particular individual.

'Processing personal data'
Any activity with personal data i.e. storage, retention, transfer, deletion, editing, anonymising.

'Controller'
Determines the purposes and means of processing the personal data. It is the sponsor who determines what data is collected for the research study through the protocol, case report form and/or structured data fields in a database. The sponsor therefore acts as the controller in relation to the research data.

'**Processor'**
Responsible for processing personal data on behalf of a controller. A Processor must act in accordance with data controller instructions.

'Safeguards'
The measures that are taken to ensure that data is processed securely, accurately and in accordance with data protection principles. These may be technical (access controls, software design) or organisational (policy).

2. What the Law says

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. In the UK, the Data Protection Act 2018 came in force on the 23 May 2018.

Data Protection Act 2018 requires each activity of processing data to have a legal basis under this legislation. Where information is imparted to another individual or organisation, the Common Law Duty of Confidentiality must also be considered.

For health and social care research undertaken within the UK Policy Framework for Health and Social Care Research, by universities and NHS organisations**, the legal basis is 'task in the public interest'.**

In considering the Common Law Duty of Confidentiality, confidential information can only be imparted to another where there is:

1. Consent - explicit or implied
2. Statutory obligation e.g. Court order, requirement of legislation.
3. Overriding public interest

3. Data Minimisation

There is a strong emphasis on implementing safeguards for personal data. This means that all Trust employees should give consideration to the arrangements for security and storage of data. Consideration should be given in determining whether personal data is necessary or whether it can be pseudonymised or anonymised. Any personal data used should be kept to a minimum.

Example 1: An electronic recruitment record

The below example is clearly anonymous. It can be re-identified through information within the Trial Master File or Investigator Site File. Access to the means to identify the individual is limited to appropriate Trust employees. This arrangement is also compliant with Good Clinical Practice.

	A	B	C	D	E
1	**Study ID Number**	**RIO Number (or equivalent)**	**Initials**	**Date of Consent**	
2	NTW001	123456	JB	01/01/2018	
3	NTW002	567890	WH	03/01/2018	
4					

Example 2: Recording consent to hear about further studies

The participant should be asked for consent to be contacted. The mechanism for the participant to withdraw their consent should be communicated.

The below example is clearly anonymous. It can be re-identified through information within the Trial Master File or Investigator Site File. This arrangement is also compliant with Good Clinical Practice.

	A	B	C	D	E
1	**Study ID Number**	**RIO Number (or equivalent)**	**Initials**	**Date of Consent**	**Consent for Further Studies**
2	NTW001	123456	JB	01/01/2018	Yes
3	NTW002	567890	WH	03/01/2018	No
4					

If a separate database is to be kept, explicit consent should be gained for their personal information to be held on a database.

Example 3: Participant Case Report Form

Add the study ID on top of every page, not identifiable data.

Participant Randomisation Code								
Date of Assessment	D	D	M	M	Y	Y	Y	Y
Name of Assessor								
Signature of Assessor								

4. Safeguards

CNTW policies relating to confidentiality, security, and handling of personal data should be followed at all times. Any member of staff not adhering to Trust policy may be subject to disciplinary procedure.

Appropriate safeguards need to be put in place to protect the confidentiality, integrity and availability of information.

An assessment of the impact of processing on the rights and freedoms of data subjects needs to be assessed. This is through a Data Protection Impact Assessment. HRA assessment replaces the need for a DPIA as the elements of such are covered.

5. Transparency Information

The participant is entitled to request the following information from the sponsor (this is a general summary and not an exhaustive list):

- The name and contact details of the data protection officer (DPO)
- Why the data is being processed (the purpose) and the legal basis for doing so
- How long the data will be stored
- The list of all recipients to whom the personal data will be disclosed
- That the data subject has a right to make a complaint to the ICO and to be provided the contact details to do so
- How appropriate or suitable safeguards are achieved if the data is to be transferred out of Europe

This information is contained within the Fair Processing Notice for the Trust which is available via the Trust website, intranet and hard copy (on request). There are other accessible versions of this Fair Processing Notice in the form of a leaflet, and an easy read leaflet. These are available through the Patient Information department.

Where possible the participant information sheet should set out the above in relation to the particular research activities at sites that involve processing of personal data, as well as any processing by the sponsor, including the act of anonymising (relevant to them).

The requirements relate to personal data and not to data that is no longer identifiable. However, to meet ethical expectations, you should still provide clarity to participants about what is happening to their data even when it is no longer personal data.

When communicating this information, it should be clear, intelligible and accessible. You can do this by providing layered information that allows people to obtain information at the level of detail they are interested in. For example, simple basic information provided directly to participants can be supplemented by more detailed information on a study website. If you have participants at different stages of your study (e.g. some being recruited and some in long-term follow-up) you should tailor the provision of information appropriately. You should consider the route for providing transparency information, for example, would information be more accessible and available if provided and/or published by the site(s) on behalf of the sponsor as well as by the sponsor.

6. Further Guidance

The HRA has drafted guidance and a series of templates to help us meet data protection legislation requirements.

The Information Commissioner's Office (ICO) Website also has a wealth of guidance available.

7. Monitoring Compliance

CNTW will audit your compliance with the GDPR, so we recommend that you keep records in investigator site files and trial master files of your decisions about how your study complies with the GDPR. As sponsor, CNTW will work with you and support you to ensure your study complies with the GDPR and trust requirements.