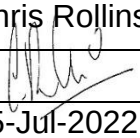
Plymouth Research and Development

NHS University Hospitals Plymouth NHS Trust

Standard Operating Procedure

Please refer to https://www.plymouthhospitals.nhs.uk/research-sops to ensure the latest version of this document is in use. Printed copies are uncontrolled.

Title:	Data protection		
Approver		Document No:	S2
Name:	Chris Rollinson	Version No:	8.0
Signature:		Effective Date:	Jul 2022
Date:	05-Jul-2022	Review Date:	Jul 2025

1. Purpose

To outline procedures for compliance with data protection for research conducted within the Trust.

The UK General Data Protection Regulation (GDPR) in conjunction with the UK Data Protection Act (DPA) 2018 sets out the statutory requirements for the processing of personal data (for further details see the Trust's Data Protection SOP - TRW.IGT.SOP.1210 1.2.). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully and transparently. Data protection laws protect personal privacy, requiring fair and lawful processing of personal information and restricting what can be done with it and to whom it may be disclosed.

All research organisations must specify a lawful basis for data processing and researchers should know this basis because approval bodies, like HRA and NHS Digital, will ask you to specify it.

UHP's lawful basis for undertaking research is '*task in the public interest* ', contained in Article 6.1(e) of GDPR. This assures research participants that the organisation is credible and using their personal data for public good.

When processing special categories of data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (known as *Special category data*). The Trust will typically rely on Article 9.2(j) of GDPR in addition to 6.1(e) i.e. *Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89 (1)*

Article 89 (1) sets out the technical and organisational safeguards that must be put in place before special category data can be used for scientific and historical research purposes. These are:

1. That we only gather the minimum amount of personal data necessary for the specified research purpose (e.g., if we do not need to collect information about ethnicity, we don't ask for it).
2. That data is anonymised wherever possible, either at point of capture or once collated.

3. Where data cannot be anonymised, it is, wherever possible, pseudonymised i.e., separated from the raw personally identifiable data and linked via a unique identifier.

In addition, at all times, you must ensure:

1. Appropriate technical and organisational measures are in place to protect personal data (see security section below).
2. The research is in the public interest (this will best be determined by the researcher in conjunction with the relevant ethics committee).

Under the GDPR, the Trust will not rely on consent as the legal basis for undertaking research. However, in line with best ethical practice and to demonstrate compliance with the common law duty of confidentiality, the Trust will, always obtain consent from data subjects to participate in research.

Where it is envisaged consent cannot be obtained from the data subject, this should be addressed during the ethics approval process.

UHP researchers may also undertake research projects requested and funded directly by an organisation(s), for this contract research the lawful basis for processing personal data will be *'the performance of a contract'*.

To comply with the Data Protection legislation information must be collected and used fairly, stored safely and not disclosed to any unauthorised person. This applies to both manual and electronically held data.

The new GDPR principles have strengthened data protection legislation. These principles set out obligations for businesses and organisations that collect, process and store individuals' personal data.

The GDPR outlines six data protection principles you must comply with when processing personal data. These principles relate to:

- **Lawfulness, fairness and transparency** - you must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** - you must only collect personal data for a specific, explicit and legitimate purpose. You must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.
- **Data minimisation** - you must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.
- **Accuracy** - you must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.
- **Storage limitation** - You must delete personal data when you no longer need it. The timescales in most cases aren't set. They will depend on your business' circumstances and the reasons why you collect this data.
- **Integrity and confidentiality** - You must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK Policy Framework for Health and Social Care Research (2017) incorporates the stipulations of the DPA and requires that in the research setting, the appropriate use and protection of participant data is paramount. All those involved in research must be aware of their legal and ethical duties in this respect. Particular attention must be given to systems for ensuring confidentiality of personal information and to the security of these systems.

If data collected for research purposes is anonymised prior to being shared it does not fall within the scope of Data Protection legislation. Notification of this must be included in the Integrated Research Application System (IRAS) form, however, UHP would expect that all those using anonymised data also adhere to the GDPR/DPA principles. In particular, that there is no attempt made to re-identify anonymised data.

- Special provisions for research (Research Exemption):
- Data must be used exclusively for research purposes
- Data must not be used to support measures or decisions relating to any identifiable living individual
- Data must not be used in a way that will cause, or be likely to cause, substantial damage or distress to any data subject
- The results of research or resulting statistics must not be made available in a form that identifies any data subject.

2. Definitions

Personal data is data that relates to living people from which they can be directly or indirectly identified - direct identifiability being from the data itself, or indirect identifiability being from the combination of the data with other available data.

Pseudonymisation a procedure by which the identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. “Pseudonymisation” – is a process that renders data neither anonymous nor directly identifying. Pseudonymisation is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. Pseudonymisation, therefore, may significantly reduce the risks associated with data processing, while also maintaining the data’s utility.

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. Anonymised data falls outside the DPA.

3. Scope

This SOP relates to all research hosted by, and/or sponsored by UHP

4. Responsibilities

The data protection of research participants is the responsibility of all members of the research team. The Investigator may delegate certain duties associated with data protection to members of the team, these should be recorded in the Delegation of Duties Log, which should be filed in the Investigator Site File.

Issues relating to the data protection of study participants should be addressed at all stages of the study process. This SOP applies to any staff involved in the setting up and conducting research e.g., *Chief Investigators (CI), *Principal Investigators (PI), Research Nurses & Midwives, Health Care Assistants (HCA), R&D Managers and Clinical Trial Administrative staff.

** CI's and PIs see appendix 1 & 2 for data protection responsibilities.*

5. Associated documents

- Trust policies regarding all aspects of data protection are located on the Trust's servers at: G:\DocumentLibrary\UHPT Trust Documents\Information Governance.
- TRW.IGT.SOP.1210 1.2 Data Protection SOP located as above.

6. Further references

- For more information about research and about general use of patient information go to https://www.hra.nhs.uk/information-about-patients/
- The UK regulator for Data Protection Legislation can be contacted as follows:
  Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, SK9 5AF. Web: https://ico.org.uk/

7. Acronyms

CI: Chief Investigator

CRF: Case Report Form

CTIMP: Clinical Trial of an Investigational Medicinal Product

DPA: Data Protection Act 2018

EU: European Union

GCP: Good Clinical Practice

GDPR: General Data Protection Regulation

HCA: Health Care Assistants

HRA: Health Research Authority

ICO: Information Commissioner's Office

IRAS: Integrated Research Application System

LoA: Letter of Access

MHRA: Medicines and Healthcare products Regulatory Agency

PI: Principal Investigator

PIS: Participant Information Sheet

R&D: Research, Development & Innovation

REC: Research Ethics Committee

RGM: Research Governance Manager

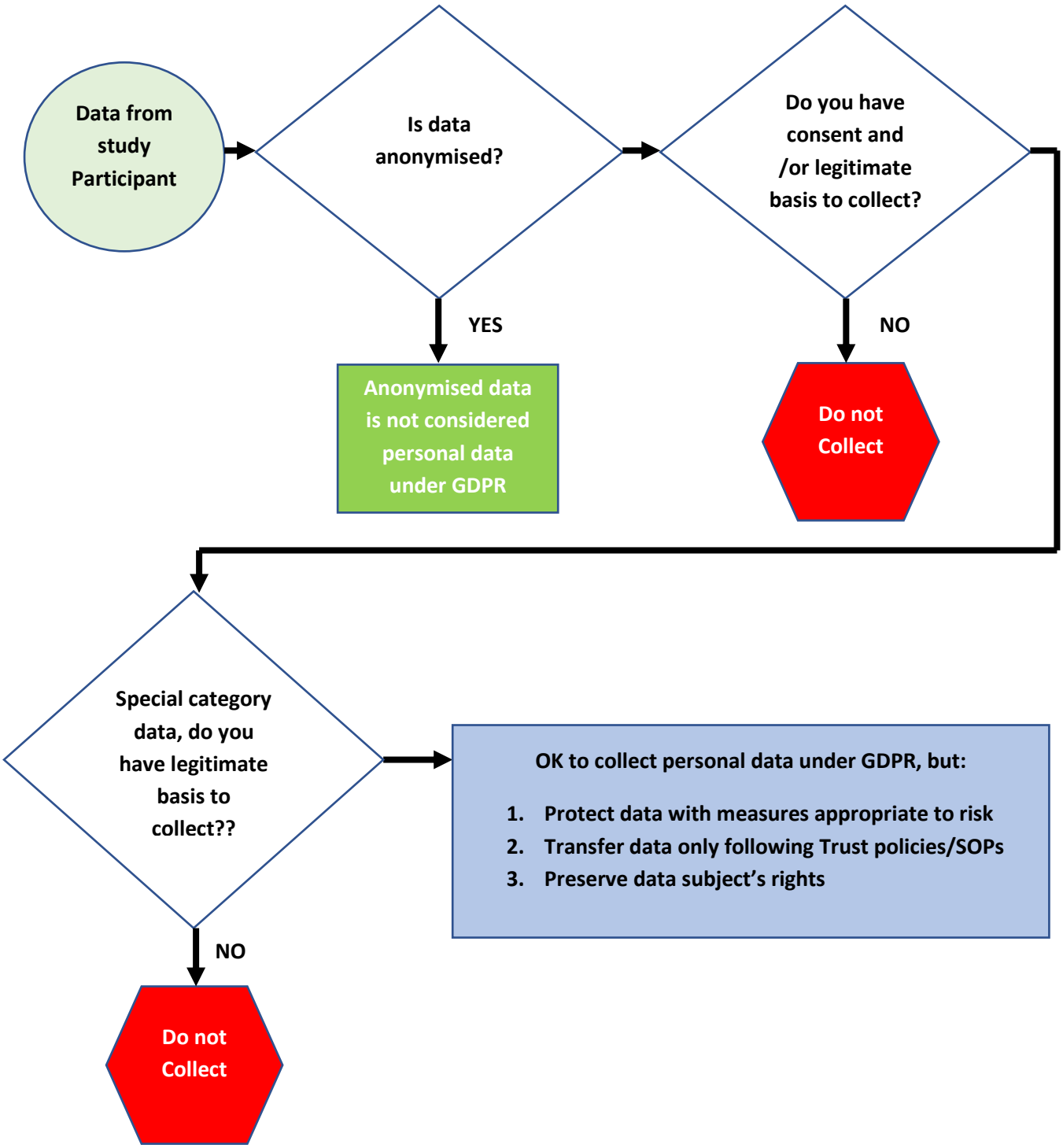
RO: Research Office

SOP: Standard Operating Procedure

UHP: University Hospitals Plymouth NHS Trust

UK: United Kingdom

8. Process map(s)/ flow chart(s)



9. Procedure

Step	Action	Responsibility
1	**General considerations** The management of data protection must be explicit within a study protocol and confidentiality and reference to a privacy notice must be made in the Participant Information Sheet (PIS) provided to potential study participants; the Research Governance Team will review UHP sponsored projects prior to R&D approval being given to ensure they will comply with the requirements of Data Protection legislation. The Trust Information Governance Team Trust and or the Caldicott Guardian may also be utilised if further advice or opinion is required. When UHP hosts a research project, responsibility for data protection issues rest with the study Sponsor.	RGM & Deputy RGM
2	It is standard practice to inform a participant's GP that they have been recruited into: (a) a study that involves an Investigational Medicinal Product, or (b) any other interventional study, which may affect a patient's care. This may only be done with the consent of the participant; hence a clause asking for permission to inform their GP of their participation in a study must be included on the informed consent form. Lists of participants randomised to trials must not be kept in places where people other than the research team can see the information. Case Record Forms (CRFs) and other paper records should be kept in a locked room. If possible, they should be kept in a locked filing cabinet in a locked room. If visitors regularly pass through the office where the data are kept or if the office is frequently unoccupied, personal data should not be left in a visible place (e.g., on desktops, notice boards, computer screens etc.).	Research Team
3	All researchers working on a study from outside of NHS employment must have a Letter of Access (LoA) or Honorary Contract with UHP to work on that study before they are allowed access to data, samples, or patients. This is in addition to any other Data Protection requirements.	Research Team and R&D Operations Team
4	Once the study is completed it is the responsibility of the Investigator to ensure the safe and secure storage of the data from the study into the Trust archive facility.	Research Investigator

Step	Action	Responsibility
5	**Recruitment** Approaching potential volunteers for research is described in the Trust SOP T2 Approach and Identification of participants for research. If a specific study advertisement is to be used (e.g., posted notice, newspaper, or magazine advert) a copy of the advertisement must be submitted with the Ethics and R&D application. The advertisement should contain the following: • Name and address of the investigator • The purpose of the research and in summary form, the eligibility criteria for the study. • A straightforward and truthful description of the incentives to the participant for participation (e.g., payments, free treatment). • The location of the research and the person to contact for further information. Generic adverts for research (without specifically naming studies) must be approved by one of the R&D Management team prior to use.	Sponsor & Research Team
6	**Anonymisation** For the purposes of studies involving Investigational Medicinal Products (IMPs) it is not possible to completely anonymise data, as participant safety and source data verification are important part of the study safety and monitoring procedures. It may also be necessary to review the source data in order to answer data queries therefore data must be pseudonymised. In order to pseudonymise data, study participants are to be given an identifier (a pseudonym) by which they are known in a system (e.g., Case Record Form, computer database), this is typically a number, but can be an identifier of the researcher's choice. In order to link the patient to their data, one master list with the identifier and patients' details will be kept separately and should be kept in a locked cabinet/office/password protected file; no copies of this list should be made. Pseudonymised data qualifies as personal data under Data Protection legislation and arrangements must be made to comply with requirements. For some studies it is possible to completely anonymise data for example radiographic images and histology slides. This data can only be classed as anonymous if it is impossible to identify the participant from the information	Research Team

Step	Action	Responsibility
	or any other information, which is to be held (the link between the data and patient is broken). In these exceptional cases only, data protection legislation does not apply, as anonymised data is not considered to be personal data.	
7	**Transferring of data outside of the UK.** The UK has recognised all EU member states as providing an adequate level of data protection for the purposes of the UK GDPR. The following countries or territories have also been deemed adequate: Andorra and Argentina. Personally identifiable data must not be transferred to any country that lies outside these areas without adequate protection (e.g., anonymous, encrypted) and agreements in place. This means that personally identifiable data cannot be transferred electronically to the greater part of the world, including Russia and Eastern Europe, USA, Canada, most of South America, Africa, Middle East, Asia, China, Australia, or New Zealand without the express consent of the participant. Consent to transfer data outside of the UK should be sought during the initial consent process (for more detail see R&D SOP A&C4_Research Data Sharing Agreement)	Sponsor and Research Governance team
8	**Use of computer equipment** Personally identifiable data should be stored on a network not a 'C' drive or personal pen drives and CDs etc. Passwords should never be shared, even with team members or line managers, as this is a breach of the Computer Misuse Act (1990). If a laptop is to be used to store participant data it should be a Trust owned laptop, which will have encryption installed to protect data should the laptop be stolen or lost. Personal laptops can be used for general work; however, no confidential or identifiable data should be stored on them. If Trust laptops are used by staff in their homes or home computers are used (in accordance with UHP guidelines (Remote Access Policy) for trial related work, confidential information regarding trial participants must be kept confidential and not be seen by other people. For IMP studies, if participant data to be used in the analysis of the product is stored electronically it must be possible for regulatory authorities to inspect the database and have a clear audit trail of corrections, i.e. if data is	All research staff

Step	Action	Responsibility
	changed on the database it must not be erased; the original entry must still be accessible. Identifiable information must not be stored on home computers, personal laptops, floppy disks, CDs, handheld devices, digital cameras or other imaging equipment. Identifiable information that is not encrypted must not be sent *via* email. To ensure all research projects within the Trust are conducted in accordance with the DPA. This SOP should be read in conjunction with the Trust formal documents relating to Data Protection and Information Governance.	
9	**Data breaches**: If you suspect a research data breach has occurred you must inform the CI /PI, the study sponsor and the R&D Governance team immediately (R&D Governance: plh-tr.rdgovernance@nhs.net or ext.'s. 31045 /32195). The breach must also be recorded on the Trusts DATIX system. The Research Governance team will notify the Information Governance team of any breaches as early as possible as there are time-limits governing how long we must undertake certain actions in response to a data breach.	Researchers and Research Governance team

10. Changes from last revision

Updated template, and add new text and flow diagram.

Appendix: Chief Investigator (CI) responsibilities — Appendix 1

The CI with support from the research team should ensure the following:

- The CI ensures that data is to be collected (prospectively or retrospectively) with consent given by the data subject.
- The CI documents in the protocol what data is to be collected and how it will be analysed.
- The CI ensures that data will not be used for anything additional to what is specified at the time of consent.
- The CI ensures appropriate security arrangements for both electronic (back up/ password protection) and paper (locked cupboard) files.
- The CI assesses if any data will be sent externally by post or electronically.
    - The CI assess the safety of the data transfer (ensures adequate data protection regulations).
- The CI assesses if the data is anonymised, if the data is not anonymised:
    - The CI obtains explicit consent from the data subject using a REC approved Informed Consent Form.
    - The CI contacts the Information Governance (IG) Team (informationgovernancepht@nhs.net) if explicit consent is not possible, to discuss the next step.
- The CI determines the method of data storage and takes appropriate action.
- The R&D Dept. ensures compliance with DPA is documented in the Clinical Trial Agreement (Contract) in the event of commercial involvement.
- In the event that a request is received for release of data under the Freedom of Information Act 2000, or a Subject Access Request under the Data Protection Act 2018 the CI must contact the IG Team & Caldicott Guardian within three working days to agree appropriate arrangements for possible data release.

Appendix: Principal Investigator (PI) responsibilities — Appendix 2

The PI with support from the research team should ensure the following:

- The PI ensures that data is to be collected (prospectively or retrospectively) with consent given by the data subject.
- The PI ensures the protocol clearly identifies what data is to be collected and how it will be analysed.
- The PI ensures that data will not be used for anything additional to what is specified at the time of consent.
- The PI ensures appropriate security arrangements for both electronic (back up/ password protection) and paper (locked cupboard) files.
- The PI assesses if any data will be sent externally by post or electronically.
    - The PI assess the safety of the data transfer (ensures adequate data protection regulations).
- The PI assesses if the data is anonymised, if the data is not anonymised:
    - The PI obtains explicit consent from the data subject, using a REC approved Informed Consent Form
    - The PI contacts the Information Governance (IG) Team (informationgovernancepht@nhs.net) if explicit consent is not possible, to discuss the next step.
- The PI determines the method of data storage and takes appropriate action.
- The R&D Dept. ensures compliance with Data Protection Regulations is documented in the Clinical Trial Agreement (Contract) in the event of commercial involvement.
- In the event that a request is received for release of data under the Freedom of Information Act 2000, or a Subject Access Request under the Data Protection Act 2018 the PI must contact the IG Team & Caldicott Guardian within three working days to agree appropriate arrangements for possible data release.