University Hospitals Plymouth NHS Trust

STANDARD OPERATING PROCEDURE

DO NOT USE THIS SOP IN PRINTED FORM WITHOUT FIRST CHECKING IT IS THE LATEST VERSION

The definitive versions of all UHPNT RD&I Dept SOPs appear online, not in printed form, to ensure that up to date versions are used. If you are reading this in printed form check that the version number and date below is the most recent one as shown on the Trust's website: https://www.plymouthhospitals.nhs.uk/researchers

Data Protection

SOP No: S2

Version No: 7.0

Effective Date: Jan 2019

Supersedes: Version 6.0, Aug 2017

Page: **1** of **11**

Last Review Date: Jan 2019 Next review date: Jan 2022

APPROVED BY

Name: Chris Rollinson

Job Title: Research Governance Manager

Signature: 

Date: 18th Dec 2018

1 Purpose and Scope

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

The EU General Data Protection Regulation (GDPR) in conjunction with the UK Data Protection Act 2018 sets out the statutory requirements for the processing of personal data. 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.

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.

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.

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 the IRAS application form however UHPNT would expect that all those using anonymised data also adhere to the GDPR/DPA principles.

- 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.

In scope: All research hosted by, and/or sponsored by UHPNT.

Definitions

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.
CI	Chief Investigator
CRF	Case Report Form
CTIMP	Clinical Trial of an Investigational Medicinal Product
DPA	Data Protection Act 2018
GCP	Good Clinical Practice
GDPR	General Data Protection Regulation
HRA	Health Research Authority
MHRA	Medicines and Healthcare products Regulatory Agency
PIS	Participant Information Sheet
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.
RD&I	Research, Development & Innovation
REC	Research Ethics Committee
RO	Research Office
SOP	Standard Operating Procedure
UHPNT	University Hospitals Plymouth NHS Trust

2 Who should read this document?

All staff involved in setting up and conducting research e.g. Chief Investigators (CI), Principal Investigators, Research Nurses & Midwives, Health Care Assistants (HCA), RD&I Managers and Clinical Trial Administrative staff

3 Procedure to Follow

3.1. Responsibility

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.

3.2 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 Manager and or the Trust Information Governance Team will review UHPNT sponsored projects prior to RD&I approval being given to ensure they will comply with the requirements of Data Protection legislation. . The Trust Caldicott Guardian may also be utilised if further advice or opinion is required. When UHPNT hosts a research project, responsibility for data protection issues rest with the study Sponsor.

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 desk tops, notice boards, computer screens etc.).

All researchers working on a study from outside of NHS employment must have a Letter of Access (LoA) or Honorary Contract with UHPNT 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.

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.

3.3 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 RD&I 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 RD&I Management team prior to use.

3.4 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 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.

3.5 Transferring of data outside of the European Economic Area.

A major requirement of the Data Protection Act 2018 is that personally identifiable data must not be transferred to any country that lies outside the European Economic Area (EEA) without adequate protection (e.g. anonymous, encrypted).

The EEA comprises the following countries:

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom with Switzerland[1].

This means that personally identifiable data cannot be transferred electronically to the greater part of the world, including Russia and Eastern Europe, USA, Canada, 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 EEA should be sought during the initial consent process.

3.6 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 UHPNT 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 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 hand held devices, digital cameras or other imaging equipment.

Identifiable information may 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.

4 Document Ratification Process

The review period for this document is set as ***default of three*** years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be approved by ***a senior RD&I manager or their Deputy***.

Non-significant amendments to this document may be made, under delegated authority from ***a senior RD&I manager***, by the nominated author. These must be ratified by ***a Senior RD&I manager***.

Significant reviews and revisions to this document will include a consultation with ***appropriately knowledgeable staff***. For non-significant amendments, informal consultation will be restricted to ***staff*** who are directly affected by the proposed changes.

Dissemination and implementation

4.1. Dissemination of this SOP

4.1.1. New SOPs and new versions of existing SOPs: The Research Governance Manager will be responsible for ensuring authorised SOPs are uploaded on the RD&I internet site. Internal Trust Staff are expected to use the RD&I internet site to access latest versions of SOPs and to check the website regularly for updates.

Notice of new or amended procedural documents that have undergone a major amendment will be given *via* the following routes:

- Inclusion in the Trust weekly e-bulletin Vital Signs
- Direct email to Trust Researchers and or teams

4.2. Training in this SOP

4.2.1. All staff whose activities are subject to this SOP should ensure that they read and understand the content of the SOP.

5 Reference material

1. For more information about research and about general use of patient information go to https://www.hra.nhs.uk/information-about-patients/

2. The UK regulator for Data Protection Legislation can be contacted as follows:

   Information Commissioner's Office (ICO)

   Information Commissioner's Office

   Wycliffe House Water Lane

   Wilmslow

   SK9 5AF

   Web: https://ico.org.uk/

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 RD&I 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 RD&I 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.

6 Amendment History

Version Number:	7.0
Date Of Amendment:	Nov 2018
Details Of Amendment:	SOP reviewed; format updated. Changed Trust and Dept. names. Updated references to the Data Protection Act 2018, General Data Protection Regulation (GDPR) and the UK Policy Framework for Health and Social Care Research (2017).
Version Number:	6.0
Date Of Amendment:	Jul 2017
Details Of Amendment:	Update SOP template and numbering system. Review and update of SOP.
Version Number:	5.0
Date Of Amendment:	Jan 2015
Details Of Amendment:	RD&IManagement team approval for generic research posters added
Version Number:	4.1 (minor amendment)
Date Of Amendment:	Mar 2012
Details Of Amendment:	Cover page - Change of SOP location address.
Version Number:	4.0
Date of Amendment:	Aug 2009
Details of Amendment:	Change in SOP template format and rewording of Para 6.3