Plymouth Research and Development

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:	Sharing research data		
Approver		Document No:	A&C4
Name:	Chris Rollinson	Version No:	1.0
Signature:		Effective Date:	Nov-2020
Date:	12-Nov-2020	Review Date:	Nov-2023

1. Purpose

To outline the procedure sharing research data in line with various pieces of legislation regarding how data is handled including the General Data Protection Regulation (2016)[1]; the Data Protection Act (2018)[2],the related Data sharing code of practice[3] and the Good Clinical Practice Guidelines (2016)[4]. This SOP will be used as the basis for any specific data sharing agreement.

2. Scope

The SOP applies to all clinical research data held on Trust servers and managed by the UHP Information Technology (IT) & Data Management team. It applies to all research data shared outside of the UHP and also research data shared within the UHP with those not directly involved in the research, whether or not the data remain wholly within the defined secure area, and control, of the UHP.

3. Responsibilities

The Research Governance Manager (RGM) will be responsible for the oversight of the sharing of research data generated from in house clinical research. In the absence of the RGM a member of the Research Governance Team may deputise.

4. Documents needed for this SOP

- Research data sharing application form
- Research data sharing agreement template

  Located at: G:\RandD\Shared\Templates & Forms for research\Data Sharing Agreements

5. Related documents

[1] General Data Protection Regulations https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

[2] Data Protection Act (2018) https://www.gov.uk/data-protection/the-data-protection-act

[3] Data sharing code of practice https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

[4] Good Clinical Practice Guidelines https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials

[5] MRC Policy and Guidance on Sharing of Research Data 1 from Population and Patient Studies https://mrc.ukri.org/publications/browse/mrc-policy-and-guidance-on-sharing-of-research-data-from-population-and-patient-studies see page 24 for definition of *bona fide* research

[6] Health Research Authority http://hra-decisiontools.org.uk/consent/content-sheet-support.html#three

[7] Information Commissioners Anonymisation Decision making Framework which can be accessed http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf

[8] EU Commission decisions on the adequacy of the protection of personal data in third countries https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[9] Information Commissioner's Office International transfers https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

[10] NHS Digital Data Sharing Framework Contract Guidance Version 1.0 : https://digital.nhs.uk/services/data-access-request-service-dars/data-access-request-service-dars-process

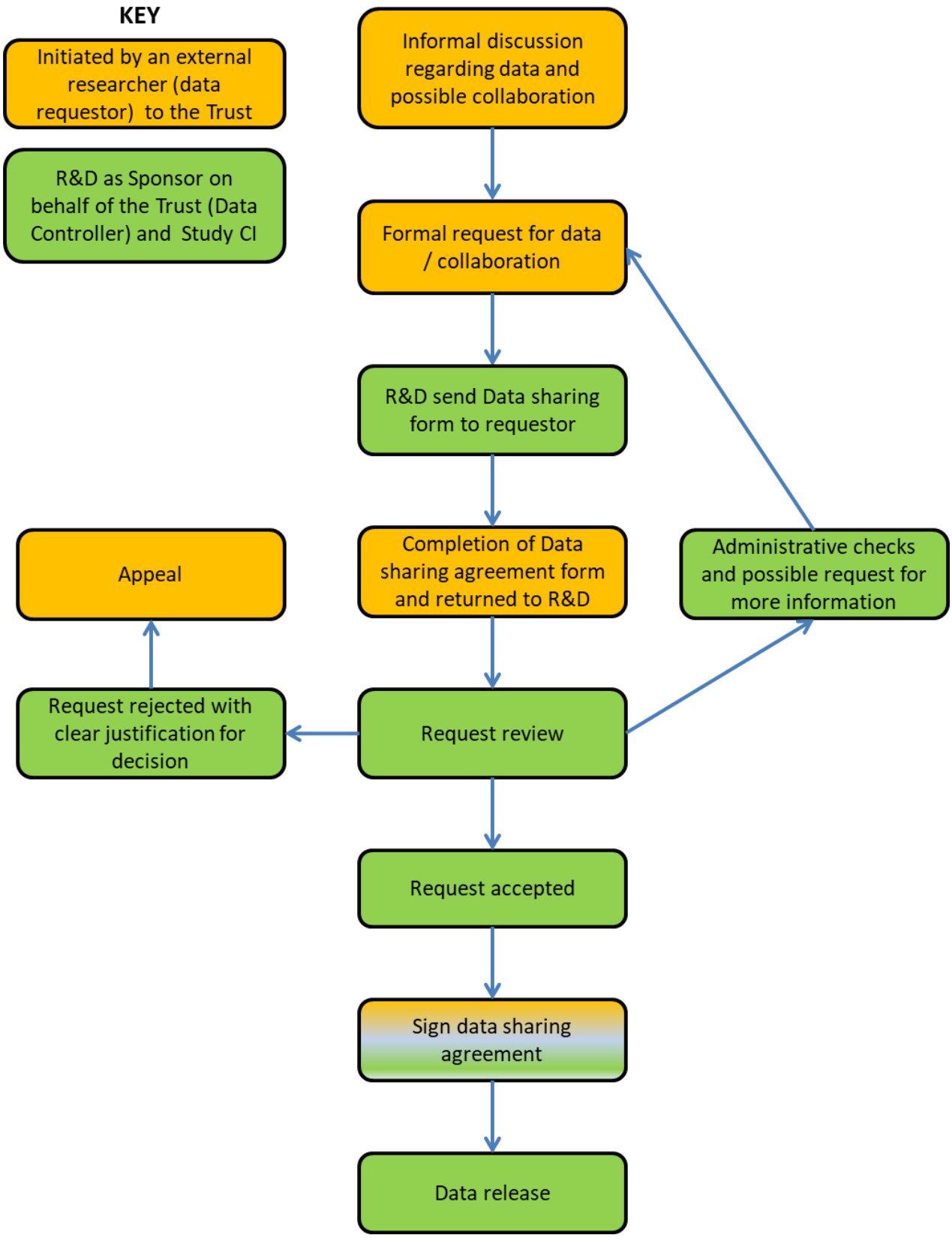
[11] Information Commissioner's Office Lawful basis for processing special category data https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

6. Definitions

R&D:	Research & Development Office
RD&I:	Research, Development & Innovation Dept.
SOP:	Standard Operating Procedure
UHP:	University Hospitals Plymouth NHS Trust
Data Controller:	The data controller will be the organisation responsible for the management and oversight of the data. The data controller determines the purposes for which and the manner in which any personal data is, or are to be processed. The data controller is responsible for the lawfulness, fairness and transparency, data minimization, accuracy, storage limitation and integrity, and confidentiality of personal data for Trust sponsored research (the R&D office acting on behalf of the Trust as Data Controller).
Data processor:	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. "Processing", in relation to information or data means, obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: a) organisation, adaptation or alteration of the information or data, b) retrieval, consultation or use of the information or data, c) disclosure of the information or data by transmission, dissemination or otherwise making available, or d) alignment, combination, blocking, erasure or destruction of the

	information or data (For research this maybe the research team and when contracted to do so PenCTU).
Information Asset Owner (IAO):	Is responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited (The R&D office on behalf of the Trust acts as the IAO). For research studies the Chief Investigator is usually delegated the task of ensuring the study data is handled and managed appropriately, although the R&D office on behalf of the Trust retains overall responsibility.
Information Asset Administrator (IAA):	Is responsible for the day-to-day management of data within a study. An IAO may delegate responsibility for management of confidential information to an IAA. (For research this maybe the research team and when contracted to do so PenCTU).
Personal data	Personal data is any information that may lead to the identification of a living person.
Special category data	Special category data is personal data that needs more protection because it is sensitive. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9. Special category data includes the following information: 1. Race and ethnic origin. 2. Religious or philosophical beliefs. 3. Political opinions. 4. Trade union memberships. 5. Biometric data used to identify an individual. 6. Genetic data. 7. Health data. 8. Data related to sexual preferences, sex life, and/or sexual orientation.
Anonymised data	Anonymised data is where all personal data including patient or participant identifiers (which can include name or initials, address, date of birth, hospital or NHS number) have been permanently removed. Anonymised data is not covered by the Data Protection Act (DPA 2018).
Pseudonymised data	Pseudonymised data is where all personal identifiers (which can include name or initials, address, date of birth, hospital or NHS number) are replaced with a unique identifier (e.g. patient study number). The key should be held separately from patient identifiers, and allow for study un-blinding if required by the protocol.

7. Process flow chart



8. Procedure

Step	Action	Responsibility
1	**Facilitating data sharing** The UHP will facilitate appropriate research data sharing to maximize the value of research data. In common with other institutions engaged clinical research, the lawful basis on which UHP relies to process personal data is Article 6(1)(e) of the GDPR which describes processing of personal data that is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". Where special category data is also being processed UHP must also be satisfied that there is a lawful basis under Article 9 of GDPR[11]. For research the lawful basis, is usually, under this article is 9(2)(j). Therefore, any data shared will be required to fulfil this requirement. Requestors are expected to use the data to generate new knowledge and understanding with the intention to publish research findings for wider scientific community and eventual public benefit [5], and to demonstrate this in their application to access the data. In any publications, the requestor should acknowledge the contribution of the original study team in accordance with academic standards. Requesters should be employees of a recognised academic institution, health service organisation or commercial research organisation with experience in medical research; and should be able to demonstrate their ability to carry out the proposed study e.g. through their own, or supervisor's, peer review publications. UHP will share research data in a timely and responsible manner, recognising that original study investigators should have a period of exclusivity before key trial data are made available to other researchers. Researchers wishing to access data are encouraged to approach the study investigators prior to approaching R&D for more information about the study, to ensure the data is appropriate for their purpose and avoid duplication of research effort. Where study investigators are no longer in post, the R&D Dept, as Sponsor and Data Controller, will appoint a member of UHP R&D staff to facilitate access to relevant documentation about the data.	R&D Office & Information Governance.
2	**Mode of data sharing** Data may be shared either by transferring the data out of the UHP secure servers or by granting the recipient researcher access to the data while it remains on the UHP secure servers. A Data Sharing Agreement is required for the former, and a Data Access Request for the latter. The Data Access Request is a simplified form	R&D Office.

	of the Data Sharing Agreement, which removes the need for institutional sign off, and descriptions relevant to transfer and storage of the data. The information asset owner (usually the trial Chief Investigator) or the lead recipient researcher will be responsible for justifying the purpose of sharing a particular dataset(s). The responsibility for implementing the Research data sharing procedure will be the RD&I Depts. Research Governance team. Data will only be shared with organisations that have adequate data security policies and procedures in place. These will be clarified in the Research Data Sharing application form.	
3	**Information for Patients** Anonymised individual patient data can be shared without specific consent, as the Data Protection Act 2018 does not cover anonymised data. However, participants should be told if researchers intend to keep the data participants provide for use beyond a specific research study and if data may be shared anonymously with others in the future (see HPA for more information [6]). It is recommended that the following statement is included in the consent form and the patient information leaflet for research studies, if appropriate. "I understand that the information collected about me will be used to support other research in the future, and may be shared anonymously with other researchers."	R&D Office.
4	**Anonymisation of Data** Anonymising data is a process that balances producing safe data with reduced utility of the data, recognising that whether data are anonymised or not, is a function of both the data and the data environment [7]. Fully anonymising the data, such that the risk of disclosing information referring to individuals is negligible is required in order for the data to be exempt from the Data Protection Act. Pseudonymisation is a form of de-identification, in which information remains personal data. The legal distinction between anonymized and pseudonymised data is its categorization as personal data. Pseudonymous data still allows for some form of re-identification (even indirect and remote), while anonymous data cannot be re-identified. Therefore, pseudonymised data cannot be considered to be outside the Data Protection Act [2], however, such data may still be shared subject to appropriate safe guards as laid out in this policy.	R&D Office, Caldicott Guardian and Information Governance.
5	**Resource implications** Preparation of the data for sharing may require significant UHP resources in order to appropriately	R&D Office.

anonymise the data and prepare the data for sharing, including providing appropriate documentation. The burden is likely to be higher for archived studies, or where no UHP R&D staffs are currently assigned to the study, or where full anonymisation is required.

The UHP R&D will assess resource implications and may charge data requestors for services if necessary. Such charges will not be seeking to generate income, simply to recover costs. The RGM will ensure sufficient resources are available to undertake work required, prior to signing the Data Sharing Agreement.

Where funders are willing to support data sharing activity, the UHP R&D recommends Chief Investigators consider including the statistician and data management time for preparing a data sharing pack in the funding application. This will contain data dictionaries, blank case report forms, and associated documentation. Documentation will highlight fields that are considered to pose a risk to identification and provide summary data for these fields.

Data Sharing Review

R&D Office, Caldicott Guardian, Information Governance and IMT Information Security Officer.

The application for sharing research data will be reviewed by the RGM (or deputy), the Information Governance team, Calidcott Guardian, IMT Information Security Officer and the R&D Finance team (as appropriate) to ensure that:

1. a valid reason has been provided to access the data and that the data requested is relevant and necessary to fulfil the stated purpose
2. appropriate steps have been taken to minimise risk of identifying participants, taking into account whether consent for data sharing was sought from the research participants (the reviewers should consider both the data and the environment together when assessing the risk of re-identification, recognising that manipulating the data may adversely affect the utility of the data)
3. where data are to be removed from UHP secure servers, data security policies and procedures of the recipient organisation, including country of data recipient (if sharing abroad), and any other applicable regulatory requirements are adequate.

The Chief Investigator or a representative will be invited to provide. The RGM (or deputy) will recommend a decision to approve or not the data sharing request and will communicate the decision with explanation to the requestor in a timely manner. Where the application has been rejected, the RGM will describe what modifications are required to enable approval.

The application to share research data will detail:

1. Specific data requirements

2. Proposed research to be undertaken using the data
3. Publication plan for the proposed research
4. Justification of the data access request
5. Summary description of data requested
6. All data custodian(s): usually the chief investigator(s) of study(ies) involved in the agreement
7. Data owner(s): i.e. study sponsor (R&D Office) for UHP.
8. Data recipient: this will be (a) named individual(s)/organisation(s) who will have access to the data
9. Details about the controlled access approach for sharing anonymised / pseudonymised individual patient data / study data aiming to protect patients' privacy and confidentiality
10. Details on data destruction or data archiving by the recipient
11. Secure data transfer method
12. Time period for which the approval has been granted
13. Where relevant, obligation on data recipients to commit to and apply security and confidentiality measures to the shared data according to NHS Digital (previously the Health & Social Care Information Centre) Data Sharing Framework, which can be referred to for more guidance [10].
14. Any constraints/requirements specified by data custodian/data controller

Transfers of data outside the EU

The UHP acts in accordance with the GDPR (2016) [1] which restricts transfers of personal data outside the EEA unless the rights of the individual are protected in another way. Wherever possible the UHP will fully anonymise any data to be shared outside the EEA. If full anonymisation is not possible, while maintaining the utility of the data, the Caldicott Guardian will assess and advise on the steps to be taken to ensure there is an adequate level of protection [7]. In addition to the member states, the European Commission has assessed a number of countries as having an adequate level of protection [9]. For more information on international transfers, see the ICO website [9]

R&D Office, Caldicott Guardian, Information Governance and IMT Information Security Officer.

Research Data Sharing Agreement

Third parties must sign an agreement before they can access data held by the UHP.

Where data are to be removed from the UHP secure servers this will take the form of a Research Data Sharing Agreement signed by the legal entities representing UHP.

R&D Office, Information Governance and Director of Corporate Business

A written Data Sharing Agreement based on the UHP R&D Data Sharing Agreement template will detail:

1. Purpose
2. Disposition of data sharing and confidentiality
3. Publication and intellectual property
4. Annex A. Data specification
5. Annex B. Anonymisation or pseudonymisation and sharing process?

9. Changes from last revision

List here any changes since the last revision.