UNIVERSITY OF WARWICK

STANDARD OPERATING PROCEDURE 15 Part 3

Information Handling

Sharing Data in Clinical Research

Version:	5.0
Approval Date:	20/08/2026
Effective Date:	03/09/2026
Review Date:	02/09/2026
Review Lead:	Jill Wood, Quality Assurance (QA) Manager, Warwick Clinical Trials Unit (WCTU)
WCTU Reviewers:	James Griffin, Assistant Professor, WCTU Manoj Nanji, Research Development Officer, R&IS Raegan Barrows, Clinical Trial Manager, WCTU
Sponsor Reviewers:	Mathew Gane, Research Governance & QA Manager, Research & Impact Services (R&IS)
WCTU approval:	Natalie Strickland, Head of Operations, WCTU
Sponsor approval:	Carole Harris, Associate Director Research Culture, Governance and Compliance, R&IS

Revision Chronology:	**Effective date:**	**Reason for change:**
Version 5.0	3 September 2026	Biennial review: Rewrite for clarity but principles have not changed. Minor clarifications. Enlargement of visuals for accessibility. Addition of definitions for pseudonymous and anonymous data and addition of responsibilities for all staff, R&IS and the CI.
Version 4.0	14 May 2024	Re-written to include the WCTU Data Sharing Committee and to expand upon some common data sharing scenarios and processes.
Version 3.0	08 March 2022	Updated key links to ensure alignment with UoW information management policies. Removal of CAG and NHS England References now separate SOPs are in place. Move to new SOP format.
Version 2.0	07 May 2020	Biennial review: re-written to incorporate updated data protection requirements. Change of process for oversight of data sharing activities. Addition of 'green light' process for processing of data that has been shared with us from a third party. Update to new template.
Version 1.1	05 March 2018	Biennial review: change to new format. Web links updated. Minor amends to text
Version 1.0	25 June 2015	N/A new SOP

UNIVERSITY OF WARWICK

CONTENTS

1 Purpose and Scope

The purpose of this SOP is to define the requirements for sharing research data with internal and external parties.

For the purposes of this SOP, the terms 'transfer' or 'sharing' are used interchangeably and include, both the movement of data and the provision of access to data (e.g. allowing others to view or download data).

Any organisation or individual outside the UoW is considered an external party, regardless of whether a formal research collaboration is in place. Data sharing in relation to data sharing statements for publication are covered in SOP 22.

This SOP applies to all individuals involved in handling clinical research data, including those requesting, approving, receiving, accessing, transferring, or sharing data within the University or with external organisations.

2 Acronyms

CAG	Confidentiality Advisory Group
DARS	Data Access Request Service
DFM	Data Flow Map
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DSA	Data Sharing Agreement
DSC	Data Sharing Committee
GDPR	General Data Protection Regulation
GCP	Good Clinical Practice
IPD	Individual Patient Data
mNCA	Model Non-Commercial Agreement (Site Agreement)
PID	Personal Identifiable Data
PIS	Patient Information Sheet
QA	Quality Assurance
R&IS	Research & Impact Services
ROPA	Record of Processing Activities
SOP	Standard Operating Procedure
SPM	Senior Project Manager
TMG	Trial Management Group
TNO	Trial Number
TSC	Trial Steering Committee
UoW	University of Warwick
WCTU	Warwick Clinical Trials Unit

3 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. This means that pseudonymised data are likely to be identifiable unless justified otherwise.

Special Category Data	This is personal data related to: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation.
Confidential data	Information that is given, with the expectation that it is kept confidential. It is not always, but in most cases likely to be related to an identifiable person. Unlike personal data, confidential data are always sensitive and never in the public domain and is applicable to data subjects that are both living or deceased.
Identifier	Information that, when used, may allow the identification of the individual to whom the information may relate. Examples include: Name Identification number *(not including randomly assigned Trial Number (TNO))* Location data Online identifier The UK General Data Protection Regulation (GDPR) makes it clear that other factors can identify an individual. These include one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
Individual Participant Data (IPD)	Data where there is a record per participant and the data has not been summarised or aggregated.
Data Controller	Organisation which alone or with others determines the means of processing
Data Processor	Organisation which processes data on behalf of the controller under their instruction (Also referred to as 'suppliers' in UK GDPR)
Data Sharing Agreement (DSA)	Formal agreements, usually between two data controllers. Good practice when valuable, high volume or sensitive data will be shared. The data controllers will each have interest in the data.
Data Processing Agreement (DPA)	Formal agreements, usually between a data controller and a data processor. A DPA is a requirement under article 28 of UK GDPR where a data processor or 'supplier' will process data on the controller's behalf.
Record of Processing Activity (ROPA)	An internal record that contains information on all personal data processing activities carried out by an organisation. See SOP 37 for WCTU studies.
Pseudonymised Data	Personal data in which direct identifiers (such as names, NHS numbers, or email addresses) have been replaced with a code or unique identifier. However, a separate key exists that can link the data back to the individual, meaning re-identification remains possible. This remains under the remit of the UK GDPR.
Anonymised Data	Data that have been processed so that individuals can no longer be identified, either directly or indirectly, from the information held. Anonymous data are not subject to UK GDPR principles.
Data Security & Protection Toolkit (DSPT)	The NHS's annual self-assessment framework that enables organisations to demonstrate compliance with data security, information governance, and information protection requirements when handling NHS data and systems.

4 Background

Sharing data is an essential part of conducting clinical research in a collaborative environment. Effective data sharing supports the delivery of research, helps meet participant expectations, contributes to the societal benefits of research and can improve the cost effectiveness and efficiency of research.

Data must only be shared where appropriate safeguards are in place to ensure:

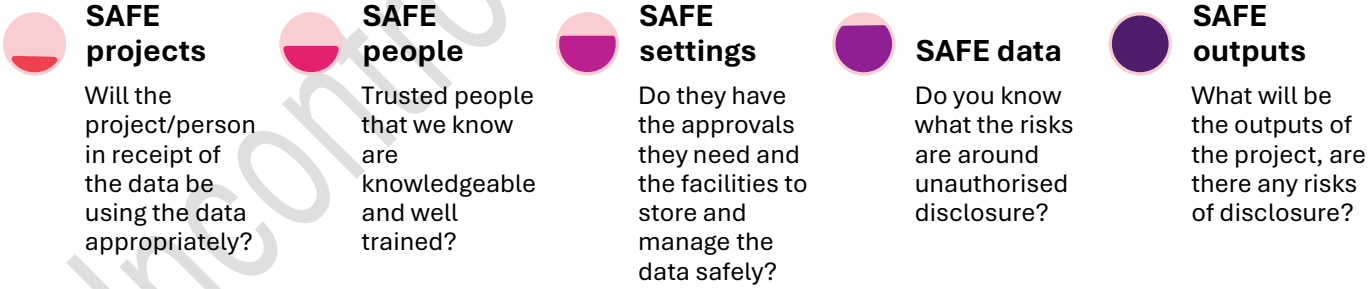
- The security of the data, including protection of intellectual property
- The confidentiality and privacy of participants (unless appropriate approvals and legal bases are in place for the use of identifiable data
- Secure and successful transfer of data
- Appropriate and authorised use of the data
- Appropriate retention and destruction of data.

The sharing of data from research studies must comply with UoW policies, principles of GCP, the UK GDPR and the common law duty of confidentiality where applicable. Data must not be shared unless these requirements are met.

UK GDPR requires organisations to implement appropriate security measures to protect personal data from unauthorised or unlawful processing, accidental loss, destruction, or damage. Data that have been effectively anonymised are outside of the scope of UK GDPR.

The common law duty of confidentiality requires confidential information to be used and disclosed only for the purpose for which it was originally provided, unless the individual has consented to another use of disclosure, there is an overriding public interest, or there is another lawful basis permitting disclosure. For example, support under Section 251 of the NHS Act 2006 may be granted by the Confidentiality Advisory Group (CAG). This is separate from, and does not replace, any legal basis required under UK GDPR for the processing of personal data.

The 5 safes outline principles for safe sharing of data:



5 Responsibilities

All individuals handling or processing research data are responsible for complying with the applicable legislation, University policies, procedures, and contractual obligations relating to the data they access

or share. DSAs and DPAs in relation to clinical research are prepared and managed by R&IS, with the process tracked through the Worktribe system. Agreements may only be signed by authorised signatories within R&IS or the Legal and Compliance Team.

For WCTU managed studies the following responsibilities apply:

Senior Project Managers (SPM)	• Supports the negotiation of agreements for pre-publication sharing of data in conjunction with R&IS. • Ensures data sharing arrangements are accurately recorded in the ROPA *(see SOP 37 'Maintenance of the WCTU ROPA')*.
Head/Deputy Head of Operations	• Review and approval of Data Sharing Green Light Forms before data are received from a third party.
Academic lead	• Ensures appropriate oversight of data associated with their research project • Ensures data are used, shared, retained, and destroyed in accordance with applicable approvals, policies, and contractual requirements.
Data Sharing Committee (DSC)	• Receive, review, and approve applications from external parties requesting access to datasets from closed and published WCTU trials. • Supports negotiation of contracts relating to post-publication data sharing • Oversight of data sharing activity
R&IS	• Prepares and manages DSAs, DPAs, and other data-sharing contracts relating to clinical research. • Supports negotiation of data-sharing agreements with external organisations. • Maintains records of agreements within the Worktribe system. • Provides advice on contractual and governance requirements relating to data sharing.
Chief Investigator	• Ensures that data sharing is consistent with the approved protocol, PIS and consent arrangements (where applicable), and applicable regulatory requirements • Provides oversight of study specific data sharing • Supports the review of data sharing requests and associated agreements where required • Ensures any study specific restrictions on data sharing are identified and communicated.
All staff	• All relevant stakeholders have visibility of, and agree to, the obligations contained within the data-sharing agreement before data are shared.

6 When

This SOP applies to the sharing, transfer, and receipt of research data before, during, and after a research project. Data-sharing requirements should be considered during study planning to ensure sufficient time and resources are available to establish the necessary governance and contractual arrangements.

A fully executed data-sharing agreement must be in place before any individual participant data (IPD) are shared or received, unless an alternative approach has been approved by R&IS or the Legal and Compliance Team.

7 How

There are multiple factors to consider when planning and approving the sharing of research data. Requirements may vary depending on whether a study is ongoing or completed, whether data are being shared or received, and the type of data involved. Figure 1 summarises the process for a number of common, but not exhaustive data sharing scenarios. Further information is provided in relevant sections of this SOP.

To protect the identity of any individual participating in research, precautions should be taken when designing research projects before sharing or publishing data. Consideration should be given to the principles of data minimisation and anonymisation prior to any data being transferred.

- *Sections 7.1, 7.2 and 7.6 of this SOP are relevant for all data sharing scenarios.*
- *For data sharing between investigator sites and the University as part of the protocol delivery (inc. provision of a complete dataset at the end of the study) go to sections: 7.5 of this SOP*
- *For data sharing outside of this scope, go to sections: 7.3 and 7.4.*

Sending Data to Others

Common Scenarios	Sharing data with 3rd party data processor to provide a study service	Sharing of trial data with external collaborators for protocol delivery	Sharing of trial data with a 3rd party for secondary use	Request for study data (external to UoW)	Request for study data (Internal to UoW)
Checklist: Can we share?	✓ Ethical approval for purpose ✓ Clearly described in PIS* ✓ Consent to share ** ✓ No funder restrictions ✓ Activity clear on the Data Flow Map ✓ No conflict with protocol or protocol data sharing statement ✓ No impact to integrity of trial and results ✓ No impact to blinding			✓ Ethical approval for purpose ✓ Clearly described in original trial PIS* ✓ Consent to share** ✓ No funder restrictions	✓ Ethical approval for purpose ✓ No funder restrictions
Review & Approval	TMG Information Security	TMG Academic Lead	TSC TMG Academic Lead	Academic Lead (and Data Sharing Committee (DSC) for WCTU studies)	
Checklist: Preparation to share?	✓ R&IS to negotiate Data Processing Agreement (or similar) ✓ For WCTU SPM should coordinate	✓ R&IS to include in collaboration agreement terms, or negotiate DSA or DPA ✓ For WCTU SPM should coordinate	✓ R&IS to negotiate DSA ✓ For WCTU SPM should coordinate	✓ R&IS negotiate DSA ✓ (DSC to coordinate for WCTU studies)	✓ No contract required ✓ Document details around 5 safes
	✓ Anonymisation, cleaning or de-identification (if applicable) ✓ Annotation of dataset for understanding (if applicable) ✓ Agree secure transfer in line with UoW standards***			✓ Agree secure transfer or access requirements in line with UoW policy*** ✓ Anonymisation, cleaning or de-identification (If applicable) ✓ Annotation of dataset for understanding	
Checklist: Review & Destruction	✓ Add to data sharing to Record of Processing Activity (ROPA) (WCTU only) ✓ Monitor end dates for when destruction is due			✓ Add to data sharing to Record of Processing Activity (ROPA) (WCTU only) ✓ Monitor end dates for when destruction is due	

** For identifiable data **For confidential data*

****https://warwick.ac.uk/services/secretarytocouncil/info-security/im-policy-framework/standards/imst03/*

Receiving Data from Others

Common Scenarios	Receipt of data from registry E.g. NHS England, ICNARC	Receipt of data from study collaborator or protocolised purpose	Receipt of data from 3rd party for secondary analysis/ meta-analysis
Due diligence check: Can it be shared with us?	✓ Ethical approval for purpose ✓ Clearly described in PIS of the study the data will come from* ✓ Consent to share from participants of the study data will come from** ✓ No funder restrictions ✓ Activity of the Data Flow Map (if study is active)		
Contract Negotiation	✓ R&IS to negotiate DSA (usually initiated by the registry) ✓ For WCTU SPM should coordinate	✓ R&IS to include in collaboration agreement terms, alternatively negotiate DSA or DPA ✓ For WCTU SPM should coordinate	✓ R&IS to negotiate with 3rd party to agree a DSA (usually initiated by a 3rd party) ✓ For WCTU SPM should coordinate
Approval Green Light	For WCTU studies, data recipient or delegate to complete Data Sharing Green Light (T04) Head or Deputy Head of operations to approve (WCTU only) Agree secure transfer in line with UoW policy and contract***		
Checklist: Review & Destruction	✓ Add to data sharing section of ROPA (WCTU only) ✓ Monitor end dates for when destruction is due		

** For identifiable data **For confidential data*
****https://warwick.ac.uk/services/secretarytocouncil/info-security/im-policy-framework/standards/imst03/*

7.1 Good practice for planning data sharing and assessing risks

It is good practice to document the flow of data between organisations and, where applicable, the individuals involved in a research project by producing a Data Flow Map (DFM) at an early stage, for further information of DFMs and the approval process see SOP 15 (Part 1).

Data sharing and processing risks should be assessed and documented within the project risk assessment and/or the WCTU Data Protection Impact Assessment (DPIA) as appropriate. Where planned processing activities are not covered by the WCTU DPIA and its documented mitigations, a project-specific DPIA may be required. Further guidance on DPIAs can be found here: UoW guidance on DPIA's. These documents should be reviewed at regular intervals.

7.2 Information Classification and safe methods of transfer

The UoW has defined a scheme for the classification of information and how it should be handled and transferred according to its requirements for confidentiality, integrity and availability. The data classifications are defined in the University Information Management Policy Framework. When planning to share data the Information Classification Policy should be consulted.

7.3 Assessing and approving data sharing requests

<table>
<tr><td>Can we share?</td><td colspan="2">Before data are shared, appropriate assurances must be in place, The considerations below apply to both pre-publication and post-publication data sharing:

✓ Ethical Approval for purpose: Where data are to be shared for research purposes, appropriate ethical approval should be in place. This might be covered in the original study approvals or may require separate approval for secondary analyses. To understand whether ethical approval will be required, visit the R&IS website: https://warwick.ac.uk/services/ris/research-integrity/ethical-approval/decision-making/

✓ Clearly outlined in the PIS: Any known or potential sharing of personal data should be clearly communicated to participants through the PIS or a transparency/privacy statement placed somewhere that is easily accessible or in participant facing CRFs at the point of data collection. Where anonymous data may be shared for future research purposes, the PIS should also explain this to promote transparency.

✓ Legal Basis and Confidentiality: Where confidential information will be disclosed, an appropriate legal basis must be in place. Typically, this will be participant consent or an alternative such as approval under Section 251 from the CAG.

✓ Funder, contractual and sponsor requirements: Any proposed data sharing should be reviewed to ensure it does not conflict with existing contractual, funder, sponsor, intellectual property, or regulatory obligations.</td></tr>
<tr><td></td><td>Additional considerations for Pre-publication sharing:</td><td>Additional considerations for post-publication sharing:</td></tr>
<tr><td></td><td>✓ DFM: For WCTU projects, all planned sharing activity should be documented on the approved DFM.

✓ Protocol consistency: Proposed data sharing should be consistent with the study protocol data sharing statements.</td><td></td></tr>
</table>

	✓ **Protection of study integrity:** Data sharing must not compromise the integrity of the study, including maintenance of any required blinding or the validity of planned analyses.	
Review & Approval	✓ Where a request falls outside of the scope of the approved protocol and the primary study analyses have not yet been completed and reported, the TMG and TSC should consider the request and determine if it should be approved. This should be clear in minutes. ✓ Where third-party software, platforms or service providers will be used, appropriate due diligence should be completed. The Information Security Team should be involved in ensuring due diligence checks are done on the companies' security processes. Refer to: SOP 32 'Vendor selection'.	✓ The Chief Investigator or Academic lead will need to give their approval. ✓ For datasets held by WCTU, requests must also be reviewed by the WCTU Data Sharing Committee (DSC). An application form can be requested from WCTUDataAccess@warwick.ac.uk ✓ The DSC should obtain assurance that appropriate governance, approvals, and contractual arrangements are in place before approving the request.
Preparation to share	Before data are shared, appropriate safeguards must be established. **Contracts and agreements**: For external data-sharing arrangements, an appropriate contractual mechanism should be in place before any data are transferred. Depending on the circumstances, this may include a collaboration agreement, DSA, DPA or other. For active studies, R&IS should be involved in establishing the required agreements. Agreements must be signed by an authorised signatory. ✓ **Protection of blinding:** Where applicable, contracts should include measures to preserve study blinding until formal unblinding has occurred. (see SOP 41). ✓ **Internal sharing:** Data sharing within the university will not need a separate contract; however, all other governance requirements within this SOP remain applicable. For post-publication requests involving WCTU-held datasets, review by the DSC is still required.	

	✓ **Dataset preparation:** Data may require preparation, annotation, anonymisation or pseudonymisation by a statistician before sharing.. Transfer and access arrangements must comply with the University's Information Classification and subsequent handling standards and the approved DFM. It is good practice to: • Confirm successful receipt of shared data • Restrict access to authorised individuals only • Remove temporary copies of datasets from transfer locations once no longer required.
Review and destruction	For WCTU studies, all data sharing activity should be recorded in the WCTU Record Of Processing Activities (ROPA). (see SOP 37: ROPA). The ROPA should record any data sharing arrangements, relevant contracts, review and expiry dates and any actions required relating to retention, return, or destruction of data as specified by the data controller(s). The SPM or the DSC chair should add these as applicable.

7.4 Receiving data from others

Can we receive the data?	Before receiving data from another organisation or internal team, appropriate assurance should be obtained that the data are being shared lawfully and in accordance with any applicable ethical, regulatory and contractual requirements. This should include, where appropriate: ✓ Confirmation that the sharing is consistent with the participant information provided to individuals when the data were collected. ✓ Confirmation that any required ethics approvals are in place. ✓ Confirmation that an appropriate legal basis exists for sharing personal or confidential information. ✓ Confirmation that the data sharing is consistent with any applicable contractual, sponsor, or funder requirements. Evidence may include review of the study protocol, PIS, consent materials, ethics approvals, or other supporting documentation.
Contract negotiation	In most cases, the organisation providing the data will initiate contractual arrangements. R&IS should be involved in review and negotiation. The receipt of data by UoW may already be included in other agreements such as a collaboration agreement where the terms

	of sharing were known in advance. Internal sharing will not require contracts but the governance considerations are still applicable and should be documented.
Approval & Greenlight	For WCTU managed studies, the recipient should complete a **Data Sharing Green Light Form**. This should be approved by the Head or Deputy head of operations prior to receipt of the data to provide assurance that appropriate due diligence has been completed. There is a template form available to complete: **T04**. Where IPD are received from organisations external to the University, the recipient should ensure that the information classification is understood and that appropriate technical and organisational measures are in place to protect the data on transfer and receipt.
Review and destruction	For WCTU studies, receipt of data should be recorded in the WCTU ROPA. The ROPA should record relevant contracts, review and expiry dates, and any data retention, return or destruction requirements. Responsibilities for oversight of data-sharing activities are defined within the terms of reference of the relevant governance committees. In addition, SPMs and Academic Leads are responsible for regularly reviewing data sharing arrangements within the ROPA and ensuring that any required actions, including contract review, data return, or data destruction, are completed.

NOTE: Any contract related to data sharing should adhere to UoW Financial Policy FP14, include timelines for transfer and retention/destruction and include the data fields to be shared and the Method of transfer.

7.5 Exchange of data between research study sites and the UoW

Where data will be exchanged between research study sites and the UoW, the following conditions should be met before data are shared:

Confidential Data	Where confidential information relating to participants will be shared, there must be an appropriate basis for disclosure, such as: • Participant consent; or • An alternative legal basis, such as support under Section 251 of the NHS Act 2006. For more information on section 251 approval, see SOP 43 'Seeking and Maintaining Approval from the CAG'.
Personal Data	Where personal data are shared, there must be transparency regarding how personal data will be collected, used, and shared. For participant data, this information is typically provided through the Participant Information Sheet (PIS) and Privacy Notice. Guidance on transparency requirements is available from the Health Research Authority (HRA). For UoW sponsored studies, the Collaborator Privacy Notice should be provided or signposted where collaborator personal data are collected. This may include Site Signature Logs, Delegation Logs, Trial Charters, or other study documentation.
Site Agreements	An appropriate site agreement must be in place before data are exchanged between the investigator site and UoW. This may include a Model Non-Commercial Agreement (mNCA) or another approved contractual arrangement.
Transfer arrangements	Data transfers must comply with the University's Information Classification Policy and use an approved transfer method appropriate to the classification of the information being shared and documented on the DFM.

7.6 Breach of security or agreement non-conformity

A security breach is any actual or suspected incident that compromises, or may compromise, the confidentiality, integrity, or availability of information. This includes incidents that could undermine public confidence in the ethical and lawful management of research data.

All staff are responsible for protecting the University's information, systems and infrastructure, as well as protecting information entrusted to the University by third parties where protection is required by contract, legislation, ethics or policy.

All staff should immediately report any observed or suspected security incidents where a breach of the University's security policies has occurred, any security weaknesses in, or threats to, systems or services.

For information on how to report a breach, go SOP 36 and read alongside the institutional Information Security pages: https://warwick.ac.uk/services/legalandcomplianceservices/dataprotection/breaches/

Where a third-party breach an agreement they must report to the university immediately so appropriate actions can be taken. R&IS should be informed of any breach of contract that UoW are party to in relation to research. Similarly, if a university employee breaches an agreement, they must inform the third party and report the breach using the process described above. For non-conformances related to DSAs with NHS England, Data Access Request Service (DARS) should be contacted via the mechanisms outlined in SOP 36 'Data breach management procedure' which covers the reporting of breaches via the DSPT to DARs where required.

Any breach of a DSA affecting a WCTU managed study should also be assessed to determine whether it requires reporting through the WCTU non-compliance process outlined in SOP 31.

8 Associated Templates and Documents

T04	Data Sharing Green Light Form
T41	Data Flow Map Builder