STANDARD OPERATING PROCEDURE 15
Information Handling

Part 3: Sharing Data

Version:	**4.0**	Effective Date:	14 May 2024
Issue Date:	30 April 2024	Review Date:	30 April 2026
Author:	Jill Wood, Quality Assurance (QA) Manager, Warwick Clinical Trials Unit (WCTU)		
WCTU Reviewers:	Kim Stewart, Senior Project Manager (SPM), WCTU Rebecca Kandiyali, Associate Professor, Health Economics, WCTU Sara Wood, Trial Manager (TM), WCTU Kerry Raynes, Trial Manager (TM), WCTU Susie Hennings, (SPM), WCTU George Bouliotis, Associate Professor, 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, Assistant Director, R&IS (Systems & Strategic Projects) & Head of Research Governance		
Review Lead:	WCTU QA Team		

Contents

Revision Chronology:	Effective date:	Reason for change:
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

STANDARD OPERATING PROCEDURE 15
Information Handling

Part 3: Sharing Data in Clinical Research

1. Purpose and Scope

The purpose of this Standard Operating Procedure (SOP) is to define the principles and practices of sharing data with internal and external parties. The scope of the term 'transfer' or 'sharing' (which can be used interchangeably), extends not just to physical movement of data but also to providing access for others to view or download data. Any party that is not part of the University of Warwick (UoW) is considered an external party even if there is a formal research collaboration arrangement. Data sharing in relation to data sharing statements for publication are covered in SOP 22.

This SOP is applicable to anyone involved in handling clinical research data or dealing with requests to access or share data with other people within the university or with other organisations.

2. Definitions

Personal Identifiable Data (PID)	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 is likely to be identifiable unless justified otherwise.
Special Category Data	This is PID 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 is 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 interests 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 UKGDPR where a data processor or 'supplier' ill process data on the controller's behalf.
Record of Process 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.

3. Background

The sharing of data is an essential part of working in a collaborative clinical research environment. Without sharing of data we could not realise effective delivery of research, meet participant expectations or contribute towards the societal benefit of research. Data sharing can also improve the cost effectiveness and efficiency of research. To share data there must be safeguards in place to control the context in which data are shared to ensure:

- The security of the data, including its intellectual property
- The maintenance of participant anonymity (unless appropriate approvals have been sought to use identifiable data)
- Successful transfer (sending and receipt) of data
- Correct/appropriate use of the data
- Appropriate retention and destruction of data

The transfer of data (including personal and confidential data) from any research study must comply with UoW policies, principles of Good Clinical Practice (GCP), the UK GDPR and the common law duty of confidentiality where they are applicable. Data must not be shared if the conditions of these are not met.

The UK GDPR requires that appropriate security measures are in place to safeguard against unauthorised or unlawful access/ processing of personal data. Anonymised or aggregated data are not regulated by the UK GDPR, providing the anonymisation or aggregation has not been done in a reversible way.

The common law duty of confidentiality says that confidential information should not be shared outside of 'reasonable' expectations without prior consent unless it is in the public interest for the purposes of safeguarding or there is a legal basis for this to be shared without consent, for example Section 251 approval which can be granted by the Confidentiality Advisory Group (CAG). Please note that this legal basis is distinct from any legal basis that applies under the UK GDPR for the processing of personal data.

The 5 safes outline principles for safe sharing of data:

SAFE projects	SAFE people	SAFE settings	SAFE data	SAFE outputs
Will the project/person in receipt of the data be using the data appropriately?	Trusted people that we know are knowledgeable and well trained?	Do they have the approvals they need and the facilities to store and manage the data safely?	Do you know what the risks are around unauthorised disclosure?	What will be the outputs of the project, are there any risks of disclosure?

4. Procedure

4.1 Responsibilities

Each person who handles or processes the data is responsible for ensuring they are complying with the appropriate regulations, policies, procedures, and contractual agreements that are in place. The person signing any agreement has overall responsibility. For DSA/DPAs relating to clinical research, R&IS generate the agreements and the process is tracked via the IDEATE system. Contractual agreements can only be signed by an approved signatory in R&IS or the Legal and Compliance team. For WCTU managed studies the following responsibilities apply:

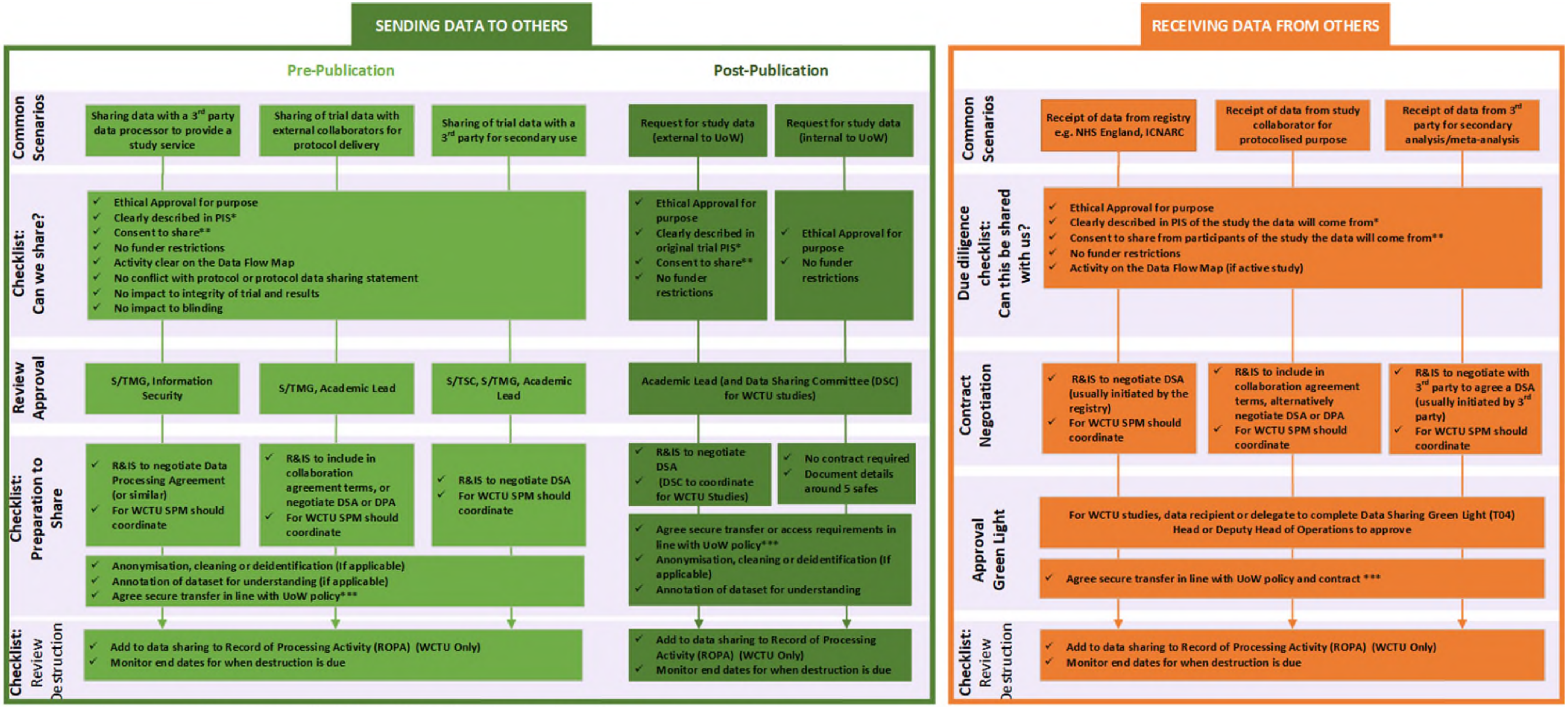
Senior Project Managers (SPM)	• Negotiation of agreements with R&IS for pre-publication sharing of data • Ensuring up to date information is documented in the WCTU Information Asset Register *(see SOP 37 'Maintenance of the WCTU Information Asset Register' for more information).*
Head/Deputy Head of Operations	• Review and sign-off of ata Sharing Green Light Forms prior to receipt of data from a third party.
Academic lead	• Responsible for the safety and security of their data assets and the information flowing in or out.
Data Sharing Committee (DSC)	• Receive, review, and approve applications from third parties to share datasets from closed and published trials held by WCTU. • Support negotiation of contracts for post-publication sharing activity • Oversight of data sharing activity

4.2 When?

This SOP is applicable prior to, during and after a research project where data are to be transferred or received. Consideration should be given prior to the onset of the research to ensure appropriate time and resource will be available. A fully signed agreement should be in place for all IPD that are sent or received unless otherwise advised by R&IS or the Legal and Compliance Team.

4.3 How?

Sharing of data prior to or post publication of results or sending vs receipt of data can involve different considerations. Figure 1 summarises the pathway for a set of common, but not exhaustive scenarios. Further details on each step are in the corresponding parts of this SOP.



SENDING DATA TO OTHERS

Pre-Publication

Post-Publication

Common Scenarios

- Sharing data with a 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?

Pre-Publication:

- ✓ 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

Post-Publication (external to UoW):

- ✓ Ethical Approval for purpose
- ✓ Clearly described in original trial PIS*
- ✓ Consent to share**
- ✓ No funder restrictions

Post-Publication (internal to UoW):

- ✓ Ethical Approval for purpose
- ✓ No funder restrictions

Review Approval

- S/TMG, Information Security
- S/TMG, Academic Lead
- S/TSC, S/TMG, Academic Lead
- Academic Lead (and Data Sharing Committee (DSC) for WCTU studies)

Checklist: Preparation to Share

Sharing data with a 3rd party data processor:

- ✓ R&IS to negotiate Data Processing Agreement (or similar)
- ✓ For WCTU SPM should coordinate

Sharing of trial data with external collaborators:

- ✓ R&IS to include in collaboration agreement terms, or negotiate DSA or DPA
- ✓ For WCTU SPM should coordinate

Sharing of trial data with a 3rd party for secondary use:

- ✓ R&IS to negotiate DSA
- ✓ For WCTU SPM should coordinate

All pre-publication scenarios:

- ✓ Anonymisation, cleaning or deidentification (If applicable)
- ✓ Annotation of dataset for understanding (if applicable)
- ✓ Agree secure transfer in line with UoW policy***

Post-Publication (external to UoW):

- ✓ R&IS to negotiate DSA
- ✓ (DSC to coordinate for WCTU Studies)

Post-Publication (internal to UoW):

- ✓ No contract required
- ✓ Document details around 5 safes

All post-publication requests:

- ✓ Agree secure transfer or access requirements in line with UoW policy***
- ✓ Anonymisation, cleaning or deidentification (If applicable)
- ✓ Annotation of dataset for understanding

Checklist: Review Destruction

Pre-Publication:

- ✓ Add to data sharing to Record of Processing Activity (ROPA) (WCTU Only)
- ✓ Monitor end dates for when destruction is due

Post-Publication:

- ✓ Add to data sharing to Record of Processing Activity (ROPA) (WCTU Only)
- ✓ Monitor end dates for when destruction is due

RECEIVING DATA FROM OTHERS

Common Scenarios

- Receipt of data from registry e.g. NHS England, ICNARC
- Receipt of data from study collaborator for protocolised purpose
- Receipt of data from 3rd party for secondary analysis/meta-analysis

Due diligence checklist: Can this 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 the data will come from**
- ✓ No funder restrictions
- ✓ Activity on the Data Flow Map (if active study)

Contract Negotiation

Receipt of data from registry:

- ✓ R&IS to negotiate DSA (usually initiated by the registry)
- ✓ For WCTU SPM should coordinate

Receipt of data from study collaborator:

- ✓ R&IS to include in collaboration agreement terms, alternatively negotiate DSA or DPA
- ✓ For WCTU SPM should coordinate

Receipt of data from 3rd party:

- ✓ R&IS to negotiate with 3rd party to agree a DSA (usually initiated by 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

- ✓ Agree secure transfer in line with UoW policy and contract ***

Checklist: Review Destruction

- ✓ Add to data sharing to Record of Processing Activity (ROPA) (WCTU Only)
- ✓ Monitor end dates for when destruction is due

** for identifiable or pseudonymised data . ** for confidential data . *** https://warwick.ac.uk/services/idg/it-compliance/guidance/sops/imsop02/*

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 4.3.1, 4.3.2 and 4.3.6 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: 4.3.5 of this SOP*
- *For data sharing outside of this scope, go to sections: 4.3.3 and 4.3.4.*

4.3.1 Good practice for planning data sharing and assessing risks

It is good practice to map the flow of data to and from of each of the organisations and where applicable, the individuals involved in a project by producing a Data Flow Map (DFM) at an early stage in a project. For WCTU Projects, DFMs should be reviewed and approved by the WCTU Governance Committee by sending to WCTUQA@Warwick.ac.uk. There is a template to support production (See T41). Data sharing and processing risks should be considered in the project risk assessment and/or the WCTU Data Protection Impact Assessment (DPIA). If the processing does not align with the processing and associated mitigations in this document, a project level DPIA may be required. If processing is outside of the scope of the WCTU DPIA, visit UoW guidance on DPIA's. These documents should be reviewed at regular intervals.

4.3.2 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.

4.3.3 Sending data to others

<table>
<tr><td rowspan="3">**Can we share?**</td><td colspan="2">In order to determine if data can be shared there are a number of assurances required, whether it is pre or post-publication. These are detailed below:
✓ **Ethical Approval for purpose:** It is highly likely that sharing of data to be used for research purposes will need ethical approval. This might be achieved by the activity being covered into the study protocol or by having separate ethical approvals 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 clear and transparent to the person whose data it is. This is sometimes achieved via the Patient Information Sheet (PIS) or a transparency/privacy statement. Where anonymous data will be shared, it is still important to acknowledge in the information sheet that this might occur. When agreeing to share data with others, for whatever purpose (including the protocol delivery), a check that this intention is clear in the PIS should be done.
✓ **Consent:** If confidential information will be shared with others, there will need to be a basis in law for this. Typically, this will be consent from the person whose data it is or an alternative such as approval under Section 251 from the Confidentiality and Advisory Committee (CAG).
✓ **Funder restrictions:** Other considerations include a review to ensure there are no interacting contracts where there is a conflict to the intended sharing.</td></tr>
<tr><td>**Additional considerations for Pre-publication sharing:**</td><td>**Additional considerations for post-publication sharing:**</td></tr>
<tr><td>✓ **Clear on DFM:** For WCTU projects, all sharing activity should be detailed on the DFM and approved by the WCTU Governance Committee, see section 4.3.1.
✓ **No conflict protocol data sharing statement:** Protocols will usually contain a data sharing statement regarding intentions, any sharing decisions should not be in conflict with this</td><td></td></tr>
</table>

	✓ **No impact to integrity and blinding:** It must be ensured that release of this data will be held responsibly and will not impact the blinding or impact the overall publication of any outcomes.	
Review & Approval	✓ If there is a request to share data that is outside of the scope of the approved protocol and the main study has not been analysed and reported, the Trial Management Group (TMG) and Trial Steering Committee (TSC) should be involved in discussing the impact to the study and approving or rejecting the request. This should be clear in any resulting documentation. ✓ For projects which involve a third-party software or service providers, the Information Security Team should be involved in ensuring due diligence checks are done on the companies' security processes. SOP 32 on Vendor selection should be consulted.	✓ For all requests for data sharing post publication, the Chief Investigator or Academic lead will need to give their approval. ✓ In addition to this, for WCTU held datasets, the request will need to be considered by the WCTU Data Sharing Committee (DSC). An application form can be requested from WCTUDataAccess@warwick.ac.uk ✓ DSC Term of Reference include receipt of assurance on the essential items that should be in place to allow sharing including the approval of the academic lead.
Preparation to share	✓ An important aspect of preparing to share data (with external parties) is ensuring all the safeguards are in place. One important safeguard is a legally binding contract. This is required for all sharing, even if sharing is outlined in the protocol. For projects which are still active, R&IS will need to ensure the appropriate contracts are in place to support the approved data sharing. Early planning and preparation of the DFM should help this process. Data sharing can be covered in a variety of ways by including the contractual terms in collaboration agreements or separate DSA or processing agreements. Nominated people in R&IS will need to sign agreements/contracts. ✓ Contracts may need to outline terms associated with preserving the integrity of the blinding that should remain in place until the formal unblinding the trial (see SOP 41). ✓ Internal sharing within the university will not need a contract but all other processes should be followed and documented, including application to the WCTU DSC in the case of post-publication requests. ✓ As well as contracts, the data may require some preparation/annotation by a statistician or transfer, or access requirements arranged. Transfer and access need to comply with the universities policy on Information Classification and subsequent handling: See section 4.3.2. Information classification and transfer methods should align with contractual terms and the DFM. It is good practice to ensure acknowledgement of successful transfer and to remove any copies of the dataset in repositories used to share the data if they are not the primary repository.	

Review and destruction	For WCTU studies, sharing of data should be recorded in the WCTU Record Of Processing Activities (ROPA). (see SOP 37: ROPA and Information Asset Register). The ROPA should record when any data sharing contracts expire or need to be reviewed for compliance so that the appropriate committees can have oversight of sharing activity. The SPM or the DSC chair should add these as applicable.

4.3.4 Receiving data from others

Can we share?	When planning to receive data from others (internal or external) it is important that we receive assurance that that all due diligence has been performed and that we feel confident that this is being shared in line with the expectations of the person whose data it is, and it has the appropriate ethical approvals in place. Often, assurance can be provided by checking the PIS for the study in which the data was collected to ensure there is transparency about the fact their data may be shared with others and in the case of confidential data, consent or an alternative legal basis is in place to share the information.
Contract negotiation	Usually in the case of receiving data from others, it will be the organisation sending the data that will instigate the data sharing offer in the form of a contract which will be negotiated with R&IS, however it 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 checklist for working out if we can share is still applicable.
Approval & Greenlight	For staff in WCTU, to ensure due diligence processes have been undertaken, the recipient of the data 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. There is a template form available to complete: **T04**. Where IPD are to be shared with external organisations not obliged to comply with University of Warwick SOPs, it should always be ensured that the recipient is aware of the information's classification and their obligations to protect it.
Review and destruction	For WCTU studies, sharing of data should be recorded in the WCTU ROPA. The ROPA should record when any data sharing contracts expire or need to be reviewed for compliance so that the appropriate committees can have oversight of sharing activity responsibilities relating to oversight of data sharing will be included in their terms of reference and individuals will be contacted to escalate queries or expiring contracts, however SPMs and Academics are expected to regularly review their processing activities via the ROPA and act when needed to review agreements or delete data. The SPM or the academic lead should add these as applicable.

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.

4.3.5 Exchange of data between research study investigator sites and the UoW

If data will be exchanged between investigator sites and the UoW, then certain conditions should be satisfied prior to sharing:

Confidential Data	Personal Data
Consent or an alternative legal basis (e.g. Section 251 approval) For more information of obtaining section 251 approval, see SOP 43 ‘Seeking and Maintaining Approval from the Confidentiality Advisory Committee (CAG)’.	Transparent information about how a participant or collaborators PID will be handled at the point of the data collection or at the earliest opportunity (e.g. via the PIS) For participants, guidance is available on the HRA Website regarding appropriate transparent information for participants. For UoW Sponsored studies, there is a collaborators privacy notice. Signposts to this should be placed on Site Signature and Delegation Logs, charters or any other document used to collect collaborators PID.
Site agreement should be in place – e.g. Model Non-Commercial Agreement (mNCA)	

4.3.6 Breach of security or agreement non-conformity

Breaches of security are defined as any serious breach of security, of confidentiality, or any other incident that could undermine the public confidence in the ethical management of data.

Staff are responsible for protecting the University’s information assets, systems and infrastructure, and for protecting the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations.

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 to the institutional Information Security pages: https://warwick.ac.uk/services/idc/dataprotection/breaches/guidance

If there is any breach of an agreement by a third party e.g. loss of data or transfer of data without permission, they must inform 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.

For **WCTU staff**, please see SOP 36 ‘Data Breach Incident Management Procedure’ for additional information on data breaches and reporting of non-compliances to DARs.

List of Abbreviations

CAG	Confidentiality Advisory Group
CI	Chief Investigator
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
mCNA	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
TM	Trial Manager
TMG	Trial Management Group
TNO	Trial Number
TSC	Trial Steering Committee
UoW	University of Warwick
WCTU	Warwick Clinical Trials Unit

Templates and Associated Guidance

T04 Data Sharing Green Light Form