STANDARD OPERATING PROCEDURE 15
Information Handling

Part 3: Sharing Data

Version:	**3.0**	Effective Date:	08 March 2022
Issue Date:	22 February 2022	Review Date:	08 March 2024
Author:	Jill Wood, Quality Assurance (QA) Manager, Warwick Clinical Trials Unit (WCTU)		
WCTU Reviewers:	Adam De Paeztron, Trial Manager, WCTU Greg Scott, QA Support Officer, 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 3.0	08 March 2022	Updated key links to ensure alignment with UoW information management policies. Removal of CAG and NHS Digital 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

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. Scope of the term 'sharing' extends not just to physical movement of data but also to providing access in order to view or download data.

This SOP is applicable to anyone involved in transferring any data internally within the University of Warwick (UoW) or externally **to** a third party at any stage of a clinical research project. It is also applicable to those members of staff involved in receipt and processing of data being transferred **from** a third party. This SOP is applicable to all types of data, paper or electronic.

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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
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	The UK General Data Protection Regulation (UK GDPR) provides a non-exhaustive list of common identifiers that, when used, may allow the identification of the individual to whom the information in question may relate. These identifiers include: name, unique identification number, location data and an online identifier. The 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 of that natural person.
Data Sharing Agreement (DSA)	Formal contract that clearly documents which data are being shared, how the data can be used, and for how long.

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.

The UK GDPR was brought into force to protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data. It 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.

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 WCTU managed studies the following responsibilities apply:

Senior Project Managers (SPM)	• Ensuring up to date information about data assets within their portfolio is documented in the WCTU Information Asset Register and that data flowing in or out of the assets is also recorded (see SOP 37 'Maintenance of the WCTU Information Asset Register' for more information).
Head/Deputy Head of Operations	• Review and sign-off of any Data Sharing Green Light Forms prior to the transfer of data to WCTU from a third party.
Academic lead	• Ownership and responsibility for their data asset and the information flowing in or out. Notify R&IS or

	SPM/Head/Deputy Head of Operations of the intention to receive or share data.

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 DSA should be in place for all datasets that are sent or received unless there are alternative contracts that define the terms of the sharing.

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.

4.3 How?

The following sections provide details of the processes to be followed for the transfer or sharing of data.

4.3.1 Understanding which data will be shared and the risks associated with its transfer

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. All data sharing and processing risks should be considered in the project risk assessment. Any processing should be checked against 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. The associated SOP should then be implemented with regards to appropriate methods of transfer according to its classification.

4.3.3 Transfer of data between research study investigator sites and the UoW

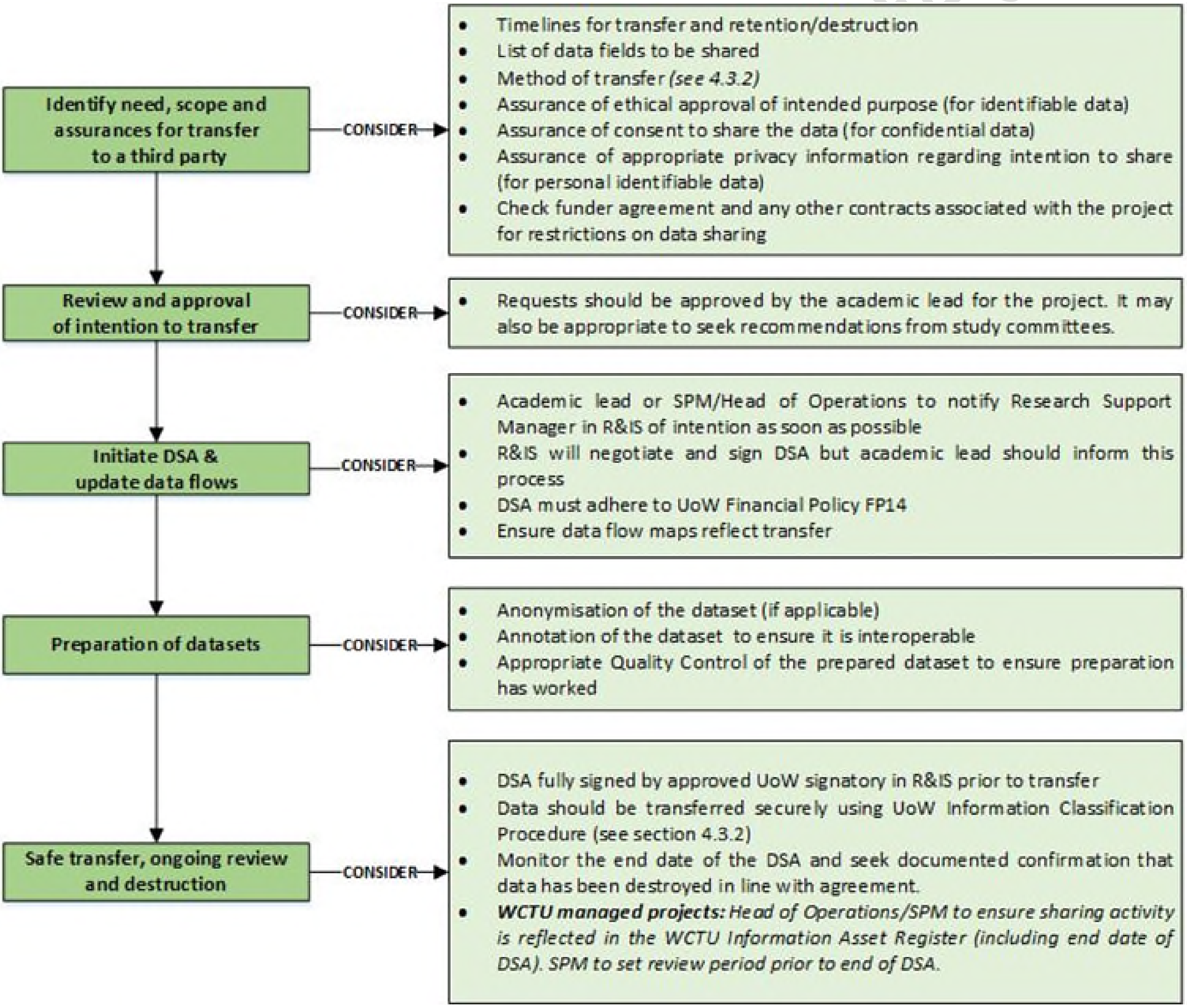
If investigator sites will transfer personal and/or confidential data to the UoW on behalf of study participants then certain conditions should be satisfied prior to sharing:

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.

4.3.4 Transfer of data generated from clinical research studies to a third party

Where non-aggregated data are to be shared with persons or 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. Access to information in these classifications by a third party requires a Data Sharing Agreement (DSA) to be in place to clearly define the responsibilities of each party, the scope for the use of the data, details of the data fields and the secure method of transfer. The flow chart below outlines the process for transferring data to a third party, including how to initiate a DSA.


Identify need, scope and assurances for transfer to a third party
CONSIDER
Review and approval of intention to transfer
CONSIDER
Initiate DSA & update data flows
CONSIDER
Preparation of datasets
CONSIDER
Safe transfer, ongoing review and destruction
CONSIDER

- Timelines for transfer and retention/destruction
- List of data fields to be shared
- Method of transfer *(see 4.3.2)*
- Assurance of ethical approval of intended purpose (for identifiable data)
- Assurance of consent to share the data (for confidential data)
- Assurance of appropriate privacy information regarding intention to share (for personal identifiable data)
- Check funder agreement and any other contracts associated with the project for restrictions on data sharing

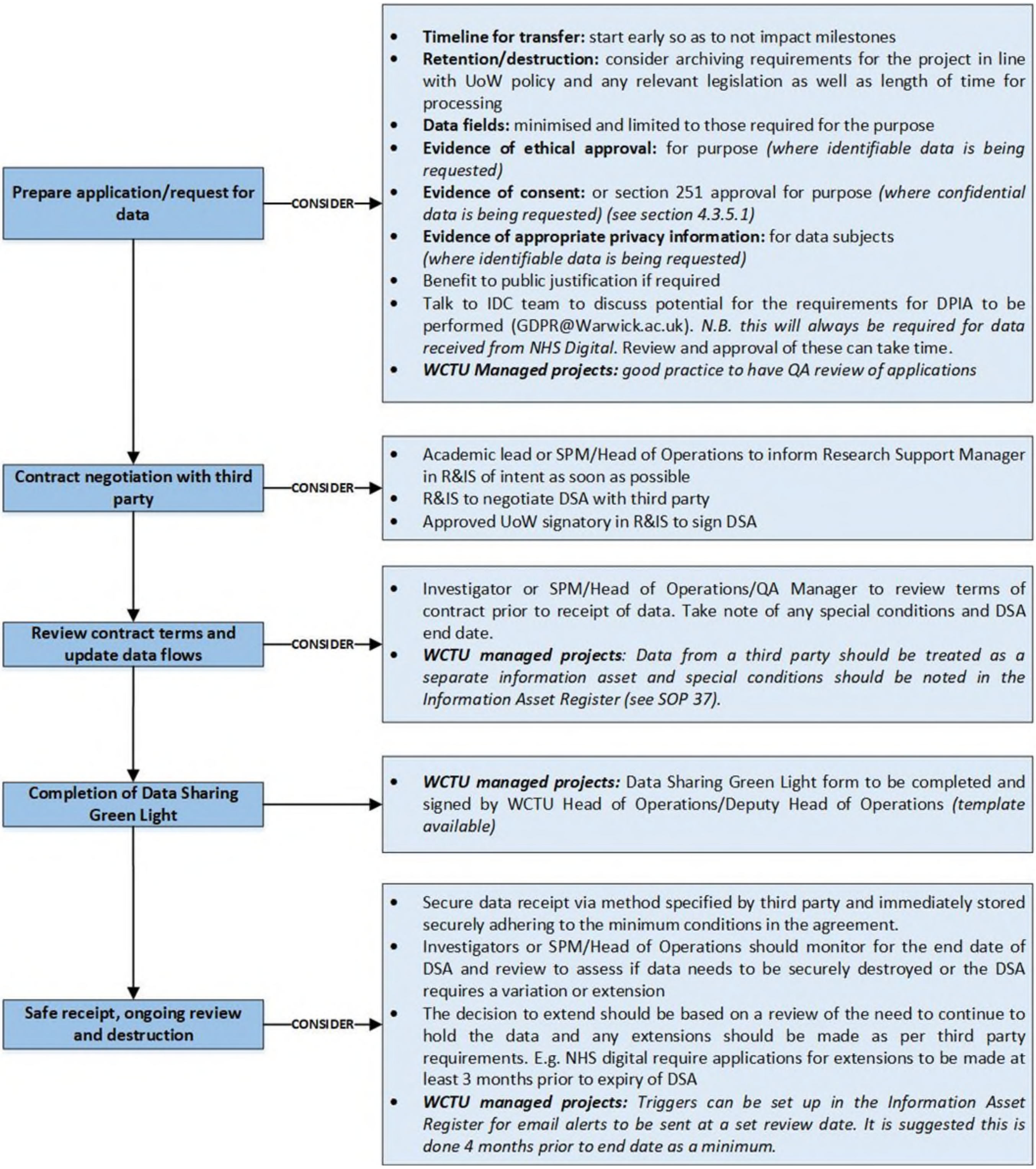
- Requests should be approved by the academic lead for the project. It may also be appropriate to seek recommendations from study committees.

- Academic lead or SPM/Head of Operations to notify Research Support Manager in R&IS of intention as soon as possible
- R&IS will negotiate and sign DSA but academic lead should inform this process
- DSA must adhere to UoW Financial Policy FP14
- Ensure data flow maps reflect transfer

- Anonymisation of the dataset (if applicable)
- Annotation of the dataset to ensure it is interoperable
- Appropriate Quality Control of the prepared dataset to ensure preparation has worked

- DSA fully signed by approved UoW signatory in R&IS prior to transfer
- Data should be transferred securely using UoW Information Classification Procedure (see section 4.3.2)
- Monitor the end date of the DSA and seek documented confirmation that data has been destroyed in line with agreement.
- ***WCTU managed projects:*** *Head of Operations/SPM to ensure sharing activity is reflected in the WCTU Information Asset Register (including end date of DSA). SPM to set review period prior to end of DSA.*

4.3.5 Transfer of data from third parties



Prepare application/request for data

CONSIDER

- **Timeline for transfer:** start early so as to not impact milestones
- **Retention/destruction:** consider archiving requirements for the project in line with UoW policy and any relevant legislation as well as length of time for processing
- **Data fields:** minimised and limited to those required for the purpose
- **Evidence of ethical approval:** for purpose *(where identifiable data is being requested)*
- **Evidence of consent:** or section 251 approval for purpose *(where confidential data is being requested) (see section 4.3.5.1)*
- **Evidence of appropriate privacy information:** for data subjects *(where identifiable data is being requested)*
- Benefit to public justification if required
- Talk to IDC team to discuss potential for the requirements for DPIA to be performed (GDPR@Warwick.ac.uk). *N.B. this will always be required for data received from NHS Digital*. Review and approval of these can take time.
- ***WCTU Managed projects:*** *good practice to have QA review of applications*

Contract negotiation with third party

CONSIDER

- Academic lead or SPM/Head of Operations to inform Research Support Manager in R&IS of intent as soon as possible
- R&IS to negotiate DSA with third party
- Approved UoW signatory in R&IS to sign DSA

Review contract terms and update data flows

CONSIDER

- Investigator or SPM/Head of Operations/QA Manager to review terms of contract prior to receipt of data. Take note of any special conditions and DSA end date.
- ***WCTU managed projects****: Data from a third party should be treated as a separate information asset and special conditions should be noted in the Information Asset Register (see SOP 37).*

Completion of Data Sharing Green Light

- ***WCTU managed projects:*** Data Sharing Green Light form to be completed and signed by WCTU Head of Operations/Deputy Head of Operations *(template available)*

Safe receipt, ongoing review and destruction

CONSIDER

- Secure data receipt via method specified by third party and immediately stored securely adhering to the minimum conditions in the agreement.
- Investigators or SPM/Head of Operations should monitor for the end date of DSA and review to assess if data needs to be securely destroyed or the DSA requires a variation or extension
- The decision to extend should be based on a review of the need to continue to hold the data and any extensions should be made as per third party requirements. E.g. NHS digital require applications for extensions to be made at least 3 months prior to expiry of DSA
- ***WCTU managed projects:*** *Triggers can be set up in the Information Asset Register for email alerts to be sent at a set review date. It is suggested this is done 4 months prior to end date as a minimum.*

4.3.6 Internal Transfer of data

As a general rule, transfer of data within the UoW does not require a DSA, however it is good practice to follow the 5 safes:

SAFE projects

- Will the project/person in receipt of the data be using the data appropriately?

SAFE people

- Trusted people that we know are knowledgeable and well trained?

SAFE settings

- Do they have the approvals they need and the facilities to store and manage the data safely?

SAFE data

- Do you know what the risks are around unauthorised disclosure?

SAFE outputs

- What will be the outputs of the project, are there any risks of disclosure?

4.3.7 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 Digital, DARS should be contacted and the process described in SOP 36 should be followed.

For **WCTU staff**, please see SOP 36 'Data Breach Incident Management Procedure' for additional information.

List of Abbreviations

CAG	Confidentiality Advisory Group
CI	Chief Investigator
DARS	Data Access Request Service
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DSA	Data Sharing Agreement
DSPT	Data Security and Protection Toolkit
GDPR	General Data Protection Regulation
GCP	Good Clinical Practice
HRA	Health Research Authority
IGARD	Independent Group Advising on the Release of Data
ISO	International Organisation for Standardisation
ONS	Office of National Statistics
QA	Quality Assurance
R&IS	Research & Impact Services
SOP	Standard Operating Procedure
SPM	Senior Project Manager
TSC	Trial Steering Committee
UoW	University of Warwick
WCTU	Warwick Clinical Trials Unit

Templates and Associated Guidance

T04 Data Sharing Green Light Form