UNIVERSITY OF WARWICK

STANDARD OPERATING PROCEDURE SOP 15 Part 1

Information Handling

Security, Protection and Management of Data for Clinical Research

Version:	6.0
Approval Date:	30/09/2026
Effective Date:	14/10/2026
Review Date:	13/10/2028
Review Lead:	Jill Wood, QA Manager, Warwick Clinical Trials Unit (WCTU)
WCTU Reviewers:	Emilie Cummerson, Data Entry Clerk, WCTU Sue Arthur, Data Entry Clerk, WCTU Anower Hossain, Assistant Professor, WCTU Christina May, Clinical Trials Monitor, WCTU Sara Wood, Clinical Trials Manager, WCTU Georgina Ray, Clinical Trials Manager, WCTU Nadia Wustrack-Law, Clinical Trials Coordinator, 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 6.0	14 Oct 2026	Comprehensive revision to align with ICH-GCP E6(R3), MHRA Data Integrity Guidance and WCTU risk-based quality management processes. SOP restructured to reflect CtQ, risk assessment, monitoring, data validation and data governance principles, with updates throughout to improve clarity, consistency and regulatory alignment. Split into clear chapters.
Version 5.0	16 Apr 2024	Addition of section with guidance related to information security concerns (lost, damaged and stolen devices). More information of identifying risks and signposting to university policies.
Version 4.0	08 March 2022	Removal of detail related to Data Lock, Data Breach, Archiving and signposts added to separate SOPs. Addition of ALCOAC principles. Updates to Information Security links in line with organisational changes. Inclusion of WCTU specific data security information prior to removal of part 2 (Electronic Data Security) inc. passwords and access to systems. Minor modifications throughout.
Version 3.0	25 July 2019	Re-write after implementation of Data Management Process. Update to requirements for Self-Evident Corrections and more information about critical on-receipt data checks and appropriate documentation. Addition of appropriate review and approval as a key document.
Version 2.1	21 July 2016	Biennial review: Minor amends and clarifications to text throughout.

Version 2.0	21 March 2014	Link to SOP 15 Parts 2 and 3. New section added on the use of self-evident corrections. Text re filing of data checking documentation added to section 4.3.8.
Version 1.3	14 May 2012	New sections added: checking procedures, electronic data capture and dealing with potential breaches of participant confidentiality.
Version 1.2	27 January 2010	Bi-annual review: Timelines amended in flowchart. Incorrect section references amended.
Version 1.1	31 January 2008	Bi-annual review: Format change. Slight amendments to text to clarify specific procedures.
Version 1.0	March 2006	

Uncontrolled when printed

UNIVERSITY OF WARWICK

CONTENTS

1 PURPOSE AND SCOPE 5

2 ACRONYMS 5

3 DEFINITIONS 6

BACKGROUND 7

4 7

5 RESPONSIBILITIES 7

6 WHEN 8

7 HOW 9

7.1 CHAPTER 1: DATA GOVERNANCE PRINCIPLES 10

7.2 CHAPTER 2: RISK-BASED PLANNING FOR DATA INTEGRITY 11

7.2.1 DATA FLOW MAPPING 11

7.2.2 IDENTIFICATION OF CRITICAL TO QUALITY FACTORS 11

7.2.3 IDENTIFICATION OF CRITICAL DATA AND PROCESSES 11

7.2.4 ASSESSMENT OF RISKS TO DATA INTEGRITY AND SECURITY 12

7.2.5 MONITORING 12

7.2.6 DATA VALIDATION PLAN 12

7.2.7 DATA MANAGEMENT PLAN 13

7.3 CHAPTER 3: DATA MANAGEMENT ACTIVITIES 14

7.3.1 COLLECTION OF DATA 14

7.3.2 ENTRY OF DATA 14

7.3.3 IMPLEMENTATION OF THE DATA VALIDATION PLAN 15

7.3.4 QUERY MANAGEMENT 15

7.3.5 SELF-EVIDENT CORRECTIONS 16

7.3.6 DELETION OF INCORRECT DATA 16

7.4 CHAPTER 4: CONFIDENTIALITY AND INFORMATION GOVERNANCE 17

7.4.1 PROCESSING PERSONAL DATA 17

7.4.2 RETENTION AND DELETION OF PERSONAL DATA 17

7.4.3 DATA SHARING AND TRANSFER 17

7.4.4 DISCLOSURE OF CONFIDENTIAL INFORMATION 17

7.5 CHAPTER 5: DATA SECURITY 19

7.5.1 ACCESS MANAGEMENT (INC. TRAINING AND COMPETENCY) 19

Uncontrolled when printed

7.5.2 Audit Trails and Traceability 19
7.5.3 Management of Security Incidents 20
8 Associated Templates and Documents 20
9 Appendix 1: WCTU systems access authorisation 21
10 Appendix 2: Considerations for Data Entry by Investigator vs Sponsor 22

Uncontrolled when printed

1 Purpose and Scope

To describe procedures for the management and protection of data (paper and electronic) from clinical research projects that ensures data are managed in a manner that preserves the scientific integrity of the research and are processed in a way that is compliant with regulations and laws that govern personal and confidential data. This SOP is applicable to all staff working on clinical research projects.

There are several procedures closely related to the management of data that are not addressed in this SOP. The following SOPs may need to be read in conjunction with this document.

- *Statistical Considerations (SOP 8)*
- *Clinical Trial Software Development (SOP 14)*
- *Data Sharing (SOP 15 (part 3))*
- *Extraction for Data for Analysis and Data Lock (SOP 15 (part 4))*
- *Case Report Forms (CRF) (SOP 16)*
- *Risk Assessment and Monitoring (SOP 18)*
- *Quality Control (SOP 19)*
- *Archiving (SOP 23)*
- *Essential Training and Training Records (SOP 24)*
- *Data Breach Incident Management Procedure (SOP 36)*
- *Clinical Data Management System (CDMS) Planning & Maintenance (SOP 42)*
- *Document Management (SOP 45)*

when printed

2 Acronyms

ALCOAC	Attributable, Legible, Contemporaneous, Original, Accurate, Complete
CDMS	Clinical Data Management System
CI	Chief Investigator
CRF	Case Report Form
CTIMP	Clinical Trial of Investigational Medicinal Product
CtQ	Critical to Quality
DCF	Data Clarification Form
DEC	Data Entry Clerk
DFM	Data Flow Map
DIL	Data Information Leaflet
DMP	Data Management Plan
DPA	Data Protection Act
DVP	Data Validation Plan
ePRO	Electronic Patient Reported Outcomes
eQMS	Electronic Quality Management System
FRS	Functional Requirement Specification
GCP	Good Clinical Practice
GDPR	General Data Protection Regulation
HE	Health Economics
HRA	Health Research Authority
ICH	International Conference on Harmonisation
IMP	Investigational Medicinal Product

MHRA	Medicines and Healthcare products Regulatory Agency
MP	Monitoring Plan
MRC	Medical Research Council
PI	Principal Investigator
PIS	Participant Information Sheet
PROMs	Patient Report Outcome Measures
QA	Quality Assurance
QAM	Quality Assurance Manager
QC	Quality Control
RA	Risk Assessment
REC	Research Ethics Committee
RCT	Randomised Controlled Trial
RDC	Remote Data Capture
R&IS	Research & Impact Services
SAE	Serious Adverse Event
SDV	Source Data Verification
SECs	Self-Evident Corrections
SIV	Site Initiation Visit
SOP	Standard Operating Procedure
TC	Trial Coordinator
TM	Trial Manager
T/SMF	Trial/Study Master File
TNO	Trial Number
T/SMG	Trial/Study Management Group
TM/TC	Trial Manager/ Trial Coordinator
UK GDPR	UK General Data Protection Regulation
UoW	University of Warwick
WCTU	Warwick Clinical Trials Unit

3 Definitions

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 are applicable to data subjects that are living or deceased.
Clinical Data Management System (CDMS)	A tool used for the collection, tracking, processing, and storage of data used in clinical research.
Data Management Plan (DMP)	A formal document that outlines how data are to be handled, both during a research project and after completion. It should be written to support the requirements of the protocol.
Self-Evident Correction (SEC)	A list of corrections to the CRF that can be made by the sponsor's data management staff without the requirement for case-by-case referral to the investigator. It is good practice to agree with site investigators prior to implementation.

Personal Data	Any information relating to an identified or identifiable living 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.
Data Security	Data Security is a process of protecting files, databases, and accounts on a network by adopting a set of controls, applications, and techniques that identify the relative importance of different datasets, their sensitivity, regulatory compliance requirements and then applying appropriate protections to secure those resources.
Encryption	The process of converting information or data into a code, especially to prevent unauthorised access.

4 Background

Clinical research data must be generated, collected, processed, retained and reported in a manner that ensures participant rights, safety and wellbeing are protected and that trial results are credible and reliable.

Data governance arrangements should be proportionate to the risks posed by the trial and should focus on processes and data that are critical to participant protection and the reliability of trial results.

Data integrity should be maintained throughout the data lifecycle in accordance with the ALCOA+ principles:

- Attributable
- Legible
- Contemporaneous
- Original
- Accurate
- Complete
- Consistent
- Enduring
- Available

Personal data must be processed in accordance with UK GDPR, the Data Protection Act 2018 and the Common Law Duty of Confidentiality, where applicable.

5 Responsibilities

CI:	Ensure appropriate data management procedures are in place to preserve the integrity of the research data. Individual tasks can be delegated to appropriately trained members of the research team, but the CI must retain responsibility for approval of the DMP.
Principal Investigator (PI):	Ensure the integrity of the study data is maintained at a given investigator site.
Typical delegation for WCTU managed studies:	

Uncontrolled when printed

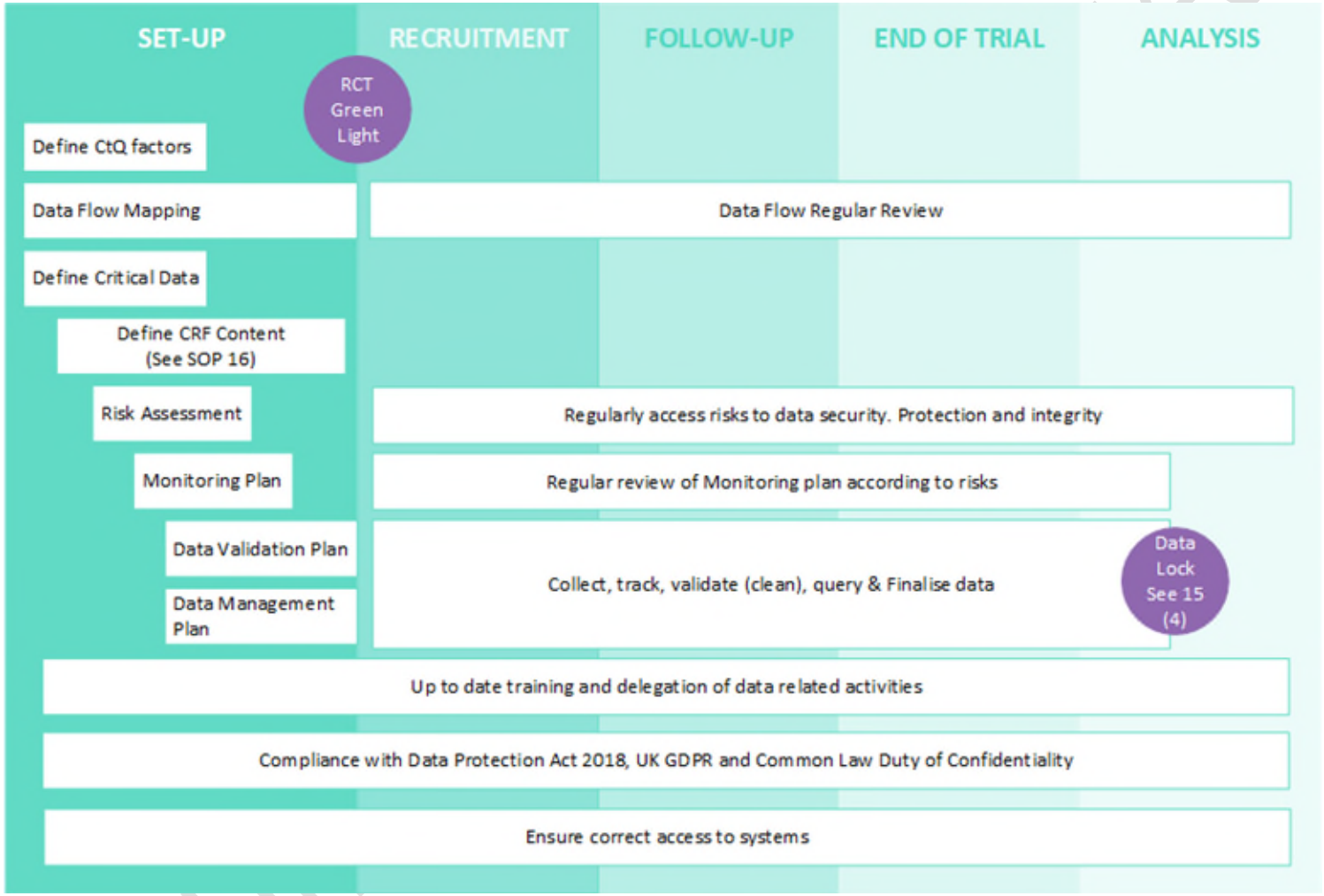
TM/TC:	• Coordinate the development, review, and approval of study DMP. • Manage all aspects of trial data collection in conjunction with approved protocol and DMP as delegated by the CI.
Statistician:	• Ensuring the statistical integrity of the trial data throughout its lifecycle. • Reviewing and providing input into the study CRFs, DMP and protocol.
Programming Team:	• Developing and maintaining the CDMS under instruction from the study team.
DEC:	• Handling data management tasks under the supervision of the TM/TC.
QA Manager:	• Ensuring that staff adhere to the principles and practices outlined in this SOP.
All individuals	• Following University information security policies and procedures and completing any mandatory information governance and data security training. • Registering any non-Warwick supplied IT equipment, for which they are personally responsible, and which is attached to the University network, with ITS. • Notifying ITS of security problems and responding in a timely manner to security alerts put out by ITS. • Taking reasonable steps to ensure there is no unauthorised access to systems for which they are responsible. • Creating strong passwords and maintaining the confidentiality of passwords. • Complying with Data Protection Legislation, GCP guidance and any regulatory requirements for maintaining the confidentiality of participant information

6 When

Data management procedures are required throughout the lifetime of the study, from the point of design up until the end of the retention period for the data. A plan for how data will be managed should be in place prior to study activation (RCT Green Light) and should be reviewed regularly in response to protocol modifications, operational changes within the trial or changes in regulatory requirements

Uncontrolled

7 How


SET-UP
RECRUITMENT
FOLLOW-UP
END OF TRIAL
ANALYSIS
RCT Green Light
Define CtQ factors
Data Flow Mapping
Data Flow Regular Review
Define Critical Data
Define CRF Content (See SOP 16)
Risk Assessment
Regularly access risks to data security. Protection and integrity
Monitoring Plan
Regular review of Monitoring plan according to risks
Data Validation Plan
Data Management Plan
Collect, track, validate (clean), query & Finalise data
Data Lock See 15 (4)
Up to date training and delegation of data related activities
Compliance with Data Protection Act 2018, UK GDPR and Common Law Duty of Confidentiality
Ensure correct access to systems

7.1 CHAPTER 1: Data Governance Principles

Data management activities should be designed and conducted to:

- Protect the rights, safety and wellbeing of trial participants.
- Ensure the reliability of trial results.
- Maintain data integrity throughout the data lifecycle.
- Protect personal and confidential information from unauthorised access, disclosure, alteration or destruction.
- Ensure data are attributable, legible, contemporaneous, original, accurate and complete.
- Apply controls that are proportionate to the risks associated with the trial and the importance of the data being processed.

The level of oversight, validation, monitoring and quality control should be justified using a risk-based approach.

Uncontrolled when printed

7.2 CHAPTER 2: Risk-Based Planning for Data Integrity

Prior to commencing data collection, processes should be established to identify critical data and critical processes, assess risks to data integrity and participant safety, and define appropriate controls. For WCTU studies, these arrangements should be documented in the RAMP (T19) and maintained throughout the study lifecycle.

7.2.1 Data Flow Mapping

A Data Flow Map (DFM) should be prepared during study setup to describe how study data will be managed:

The DFM should identify:

- Data controllers and processors
- Data transfers
- Storage locations
- Information classifications according to the Universities Information Classification Standard.
- Security controls according to the Universities Handling Information Standard.

The DFM should be reviewed throughout study setup and approved before any study data are processed or transferred. If applying for UoW Sponsorship, this will be required as part of the application. Otherwise, this should be completed, reviewed and approved prior to any processing activities. Early data flow mapping facilitates identification of necessary:

- data sharing requirements,
- contractual requirements
- data transparency arrangements around data sharing

For WCTU managed studies approval is via the WCTU Governance Committee by submitting in advance to WCTUQA@warwick.ac.uk. Approval will be via committee or by a member of the WCTU QA team on behalf of the committee in line with the committee Terms of Reference.

A data flow map builder template with guidance **T41** is available.

7.2.2 Identification of Critical to Quality Factors

Prior to study initiation, CtQ factors should be identified to ensure appropriate focus is given to activities important to participant safety, participant rights and wellbeing, and the reliability of trial results.

For WCTU managed studies, CtQ factors should be documented in accordance with SOP 18 'Risk Assessment and Monitoring' and reviewed throughout the study lifecycle where significant changes occur.

7.2.3 Identification of Critical Data and Processes

Critical data and processes should be identified during study setup and documented within the study risk management documentation.

Critical data are data that are essential to:

- Participant safety

Uncontrolled when printed

- Protection of participant rights
- Assessment of primary and key secondary study objectives
- Reliability and interpretation of study results

Critical processes are processes that support participant protection and data reliability. Examples may include informed consent, randomisation, safety reporting, data collection, database management and data transfer activities.

The identification of critical data and critical processes should inform monitoring activities, validation checks, quality control activities and escalation procedures. For WCTU managed trials, these should be documented in the Critical Data and Business Continuity Plan sections of the RAMP **T19**. Further information can be found in SOP 18 'Risk Assessment & Management' and SOP 40 'Business Continuity'.

7.2.4 Assessment of Risks to Data Integrity and Security

Risks relating to data integrity, participant confidentiality, participant safety and trial reliability should be identified, assessed and documented in the trial risk assessment. Controls and mitigations should be proportionate to identified risks and inform the resulting monitoring and validation plans. See SOP 18 for more detailed procedures about assessment of risk.

For WCTU managed studies, risks should be documented within the RAMP.

For WCTU Managed Studies, a DPIA has been conducted at a quality system level. Studies processing data outside the scope of the DPIA, or where data privacy risks have not been adequately considered through the risk assessment process, should consider whether a study-specific DPIA is required. More information can be found by visiting the Universities Legal and Compliance webpages.

7.2.5 Monitoring

The Monitoring Plan should describe activities used to oversee critical processes and critical data and verify that identified mitigations remain effective. Refer to SOP 18 'Risk Assessment & Monitoring' for more detail on this process.

7.2.6 Data Validation Plan

A documented Data Validation Plan (DVP) should describe the strategy for identifying data discrepancies, inconsistencies and missing data throughout the study lifecycle. The DVP should be proportionate to the risks identified for the study and focus on critical data and critical processes. It should define:

- The validation activities to be performed
- The data to which the activities will be applied
- The frequency and timing of validation activities
- The responsibilities for performing and reviewing validation activities

Validation activities may include:

- Manual, programmed or automated review of incoming data
- Cross-CRF consistency checks

Uncontrolled when printed

- Review of missing data
- Appropriate delegation checks
- Range checks.

Automatic checks incorporated within the CDMS should be described within the Functional Requirements Specification (FRS). Additional validation activities should be described within the DVP.

For WCTU managed trials, the template DVP is within the RAMP template (T19).

7.2.7 Data Management Plan

A DMP must be produced for all studies.

The DMP should describe the operational procedures that will be used to support the collection, processing, review, correction and retention of study data.

The DMP should be informed by and align to:

- The protocol
- Critical to Quality assessment
- Risk Assessment
- Monitoring Plan
- Data Validation Plan
- Data Flow Map

An approved version of the DMP should be in place prior to study initiation and reviewed throughout the study lifecycle in response to significant changes, e.g. Substantial Modification to Protocol, CRF/Database updates). It may also be good practice to review a few months after data collection starts to ensure it is fit for purpose.

Study-specific working instructions may be referenced where they contain detailed operational instructions; however, processes that are critical to the integrity, quality or interpretation of study data should be described or referenced within the DMP. A template is available **T69**. Working instructions should be developed, approved and reviewed according to **SOP 34** 'Trial Specific Working Instructions'.

For WCTU managed studies, the DMP and any revisions must be approved by the CI using an acceptable mechanism e.g. SharePoint, Email (see **G33** 'Email Approval Guidance') or Wet Ink signature. Key stakeholders that should input into the DMP include, but are not limited to:

- Statistician
- Health Economist
- QA
- TC/TM
- DEC

Uncontrolled when printed

7.3 CHAPTER 3: Data Management Activities

Data management activities should be performed throughout the study lifecycle to ensure data remain complete, accurate, consistent, attributable and suitable to support study objectives. The nature and extent of data management activities should be proportionate to the identified risks and focused on data and processes that are critical to participant protection and the reliability of study results.

7.3.1 Collection of data

Data may be collected from participants, investigator sites, healthcare records, external organisations or electronic systems. Collection methods may include direct data entry by participants, transcription from source records into paper or electronic CRFs, data captured through RDC systems, or import of external datasets.

Where the CRF is intended to act as the source document, for example during participant interviews or telephone assessments, this should be clearly documented within the protocol and personnel responsible for collecting the data should be appropriately trained.

Data obtained from external sources, including laboratories, registries or routine healthcare datasets, should be supported by appropriate contractual, data sharing or data processing arrangements as required.

Data collection processes should be designed to minimise errors, ensure data remain attributable to their source and support timely identification of missing, inconsistent or potentially safety-critical information.

Processes should be in place to track the receipt of expected data, monitor data return against defined timelines and escalate missing, incomplete or overdue data in accordance with the DMP, DVP or Monitoring Plan.

7.3.2 Entry of Data

Data entry should only be undertaken by appropriately trained and delegated individuals.

Data should be entered accurately and in a manner that preserves the integrity of the original record. Any changes made during data entry or subsequent processing should be attributable, traceable and supported by an audit trail or equivalent documentation.

Where CDMS are used, data entry processes should be supported by appropriate system controls and user access permissions.

Quality control activities should be implemented where appropriate to verify the accuracy and completeness of data entry. The nature, frequency and extent of quality control should be proportionate to study risk and documented within the DMP, Monitoring Plan or associated study procedures. Evidence of quality control activities should be retained within the study records.

Uncontrolled when printed

There should be a mechanism to assure the coordinating centre that the PI or their delegate at site are happy with data submitted. For WCTU studies that use the Study capture system, this has a form locking facility to manage this assurance.

Considerations for training and quality control of data entry can be found in appendix 2.

7.3.3 Implementation of the Data Validation Plan

Data validation and review activities should be conducted in accordance with the approved DVP throughout the study lifecycle.

The purpose of data review is to identify and investigate missing, inconsistent, implausible or potentially erroneous data and to ensure that study data remain complete, accurate and fit for analysis.

Any issues identified should be assessed and managed in accordance with the approved query management process and resolved within appropriate timelines.

Where validation activities identify a potential protocol non-compliance, adverse event (AE) or serious adverse event (SAE), the matter should be assessed and managed in accordance with the relevant WCTU procedures.

7.3.4 Query Management

Queries should be raised where clarification or correction of data is required as a result of validation checks.

Where available, queries should be managed within the CDMS to ensure an auditable record of query creation, responses, amendments and closure. Where an integrated query management function is not available, an alternative process may be used, provided all query activity remains traceable and appropriately documented.

Responses to queries should be provided by appropriately trained and delegated individuals. Any amendments made as a result of a query should be attributable, traceable and preserve the original record. For electronic systems, this should be captured within the audit trail. For paper records, corrections should be signed or initialled, dated and remain legible.

Where query responses are documented separately from the original data record (e.g. using a Data Clarification Form), the process for applying and documenting corrections should be defined within the DMP or associated study procedures. The coordinating centre should verify that responses have been provided by an appropriately delegated individual.

Where participant follow-up is required to resolve a query, the process should be described within the DMP or relevant working instructions and conducted in accordance with the protocol and participant-facing documentation. Information obtained directly from participants should be documented in a manner that maintains an appropriate audit trail.

Uncontrolled when printed

All queries, responses and associated correspondence should be retained in accordance with the study filing structure and managed in a manner that maintains participant confidentiality, appropriate access control and data integrity.

7.3.5 Self-Evident Corrections

SECs are predefined corrections that may be applied without case-by-case referral to the investigator site where the correct value is obvious and can be determined from existing study documentation. Statistical agreement should be sought for any that are implemented.

The use of SECs should be justified, documented within the DMP/WIs and applied only in circumstances where there is no ambiguity regarding the correct value.

SECs should not replace routine query management processes and should be implemented in a manner that maintains transparency, traceability and data integrity.

Good practice involves:

- Prior agreement of the intended list of SECs by the PI or their delegate at each investigator site.
- Providing investigator sites with a record of which TNOs and fields have been subject to a SEC. This can be sent to the investigator site as part of the DCF or as a list at the end of the trial.

7.3.6 Deletion of incorrect data

Where data have been entered incorrectly and cannot be corrected through the normal query or amendment process, deletion of the incorrect data may be necessary. Any deletion must be appropriately justified, documented and supported by a clear audit trail that allows reconstruction of the original entry, the reason for deletion, who authorised the action and when it occurred.

Prior to deletion, consideration should be given to any potential impact on data quality, reporting, monitoring activities or statistical analyses. Evidence of this assessment and any required approvals should be retained. Individuals performing data deletions must be appropriately trained and authorised to undertake the activity.

Uncontrolled when printed

7.4 CHAPTER 4: Confidentiality and Information Governance

Personal and confidential data should be processed in a manner that protects the rights and freedoms of data subjects and maintains public trust in research.

Appropriate organisational, technical and procedural controls should be implemented to ensure compliance with applicable legislation, ethical approvals and contractual obligations.

7.4.1 Processing Personal Data

Personal data should be processed lawfully, fairly and transparently and only for purposes that are consistent with the approved study documentation.

The study protocol, PIS, DIL, DFM and related study documentation should clearly describe how personal data will be collected, used, stored, shared and retained.

Staff handling personal data should understand the classification of information they process and apply appropriate safeguards throughout the data lifecycle.

7.4.2 Retention and Deletion of Personal Data

Personal data should only be retained for as long as necessary to fulfil the purposes for which it was collected and to meet applicable regulatory, contractual and archival requirements.

When personal data are no longer required, they should be securely deleted, anonymised or otherwise disposed of using methods appropriate to the medium and information classification.

The retention and deletion strategy should be described within study documentation where applicable.

For WCTU studies, this information should also be recorded in the Record of Processing Activities (ROPA). Further information about this requirement is in SOP 37 ‘ROPA’.

7.4.3 Data Sharing and Transfer

The transfer or sharing of study data should only occur where there is an appropriate legal, ethical and operational basis to do so.

Data sharing arrangements should be documented within the DFM and supported by appropriate agreements where required.

Appropriate safeguards should be implemented to protect data during transfer, storage and processing, with consideration given to information classification and risk. More information on data sharing is located in part 3 of this SOP.

7.4.4 Disclosure of Confidential Information

Exceptional circumstances may arise where information obtained during a study indicates a risk of serious harm to a participant or another individual.

Uncontrolled when printed

In such circumstances, disclosure of confidential information may be necessary where permitted by law, ethical approval or approved study procedures.

Any disclosure should be limited to the minimum information necessary, appropriately documented and managed in accordance with the study protocol and applicable organisational procedures.

Uncontrolled when printed

7.5 CHAPTER 5: Data Security

Appropriate technical and organisational controls should be implemented to protect study data against accidental or unlawful loss, destruction, alteration, unauthorised disclosure or unauthorised access.

Security controls should be proportionate to the sensitivity of the information and the risks associated with the study.

7.5.1 Access management (inc. Training and competency)

Access to systems used to process study data should be restricted to appropriately trained and delegated individuals. Access to the CDMS should be applied using the role-based access defined in the FRS.

Users should only be granted the minimum level of access necessary to perform their role.

Access permissions should be reviewed periodically and amended or removed promptly when roles change or access is no longer required.

Individuals undertaking data management activities should have documented evidence of appropriate training, competency and delegation prior to being provided access and performing study tasks.

For WCTU Managed Studies, all systems that manage personal identifiable data should authenticate users before permitting access. Minimum authentication requirements should consist of unique individually assigned usernames and use of a strong password. Access authorisation requirements for WCTU systems and quality control processes are outlined in appendix 1.

A training plan for data management activity at the coordinating centre (inc. competency thresholds if appropriate) should be defined in the DMP.

SOP 24 'Essential Training and Training Records' outlines all data security training UoW should complete.

Completion of training and relevant evidence of competency should be documented in training records.

Evidence of QC checks completed as part of training sign off or ongoing management should be filed in the TMF.

7.5.2 Audit Trails and Traceability

Study data should be maintained in a manner that supports traceability throughout the data lifecycle.

Electronic systems used to manage study data should maintain audit trails that enable reconstruction of significant data-related activities, including the creation, modification and deletion of data.

Audit trails should be retained, protected from unauthorised modification and be available for review where required.

Uncontrolled when printed

Where electronic audit trails are not available, alternative methods should be used to maintain appropriate traceability.

Audit trails should be reviewed where appropriate to verify that data changes are authorised, attributable and consistent with approved procedures. Review activities should be proportionate to risk and focused on critical data or activities that may impact data integrity.

7.5.3 Management of Security Incidents

Actual or suspected data security incidents should be reported, assessed and managed promptly.

Security incidents may include, but are not limited to:

- Loss or theft of devices.
- Unauthorised access to systems or data.
- Accidental disclosure of confidential information.
- Suspected cyber security incidents.
- Loss, corruption or destruction of study data.

Incidents should be managed in accordance with applicable organisational procedures and escalated where necessary to enable assessment of potential impacts on participant confidentiality, participant safety, regulatory compliance and data integrity. Organisational policies related to data security can be found here: https://warwick.ac.uk/services/secretarytocouncil/info-security/im-policy-framework/.

For WCTU studies, anything related to a suspected data breach should be managed according to the processes in SOP 36 'Data Breach Incident Management Procedure' as well as organisational procedures.

8 Associated Templates and Documents

T69	Data Management Plan Template
T41	Data Flow Map Builder
G33	Email Approval Guidance
T19	RAMP Template (including DVP)

Uncontrolled when printed

9 Appendix 1: WCTU systems access authorisation

The table below describes the processes for granting and revoking access to common WCTU systems.

Those requesting access should be different from the subject of the access request and requests should consider whether appropriate training and delegation is in place to support the request.

System	Access requests	Authorisation	Quality Control
CDMS **(WCTU Programming Team Managed)**	Programming Team Helpdesk request by the nominated System Owner:	WCTU Programming Team	Systems should be reviewed quarterly to ensure appropriate access is maintained. The review outcome should be documented in the table provided by the QA team and filed alongside the Coordination Centre Delegation Log. To facilitate this further, maintaining an access log may be helpful practice.
WCTU Mdrive document repository	SPM/TM or Operations lead to submit Starters/Movers/Leavers Form	WCTU QA Team *(or approved delegate)*	
Resource email accounts	Request by resource owner via the Self-Service Portal.	ITServices	
PGP software Symantec Desktop Encryption (PGP)*	PGP Administrator(s) are responsible for granting access and removing when access is no longer required. There should always be a minimum of 2 administrators.		
Microsoft SharePoint/Teams channels	Channel or team owner(s) are responsible for granting access and removing when access is no longer required. SharePoint sites should be set up via the WCTU QA Team following the process in SOP 47.		

**** PGP may be required if holding confidential or highly confidential information on network drives and there is no approved alternative – see University's Handling Information Standard.***

Uncontrolled when printed

10 Appendix 2: Considerations for Data Entry by Investigator vs Sponsor

	RDC by investigator site	Entry at coordination centre
Training considerations	SIV or Video demonstration Working instructions Training log and/or delegation log	DMP Working instructions Coordination centre delegation log
Quality Control (QC)	Can be achieved by Source Data Verification and where it is deemed appropriate and necessary to do so. This should be documented in the DMP or Monitoring Plan. See also, SOP 18 'Risk Assessment and Monitoring'.	The elements of data that require checking, the frequency, the escalation strategy and where this will be documented should be detailed in the Monitoring Plan or DMP and should be proportionate to the risk e.g. high-risk items such as primary end point may be subject to 100% checking or have a smaller allowance for errors. For more information, see SOP 19 'Quality Control'.

Uncontrolled when printed