STANDARD OPERATING PROCEDURE 15
Information Handling

Part 1: Security, Protection and Management of Data for Clinical Research

Version:	V5.0	Effective Date:	16 Apr 2024
Issue Date:	09 Apr 2024	Review Date:	16 Apr 2026
Author:	Jill Wood, QA Manager, Warwick Clinical Trials Unit (WCTU)		
WCTU Reviewers:	James Griffin, Research Fellow, WCTU Jenny Thirlwall, Clinical Trials Manager, WCTU Laurilee Sprauve, Data Entry Clerk, WCTU Rosie Henvey, 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, Assistant Director, R&IS (Systems & Strategic Projects) & Head of Research Governance		
Review Lead:	WCTU QA Team		

Uncontrolled when

Contents

Uncontrolled when printed

Revision Chronology:	Effective date:	Reason for change:
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

STANDARD OPERATING PROCEDURE 15
Information Handling
Part 1: Security, Protection and Management of Data for Clinical Research

1. Purpose and Scope

This Standard Operating Procedure (SOP) describes procedures for the management and protection of data (both 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. SOPs which may need to be read in conjunction with this are listed below:

- *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)*
- *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)*

2. Definitions

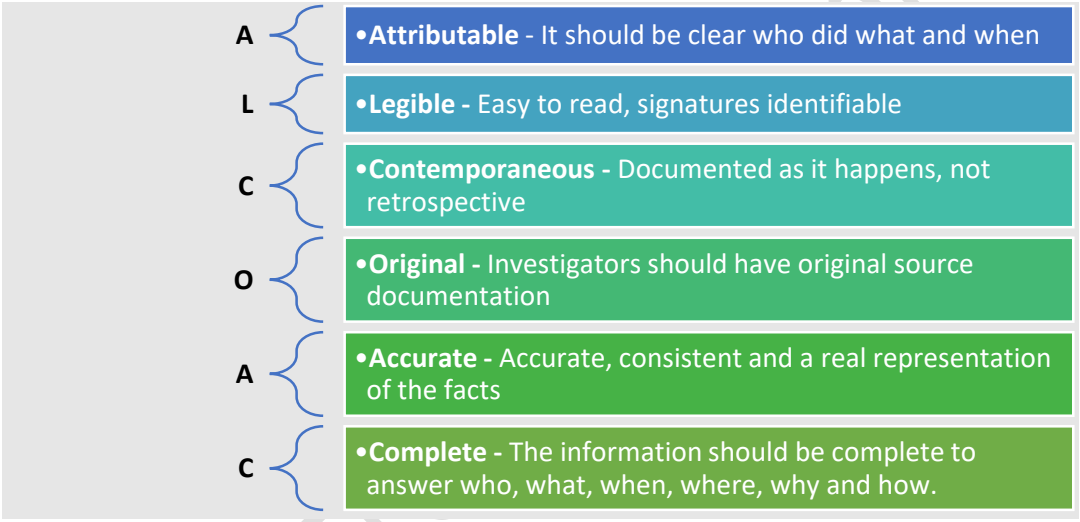
Confidential Data	Information that is given with the expectation that it is kept confidential. It is not always, but in most cases likely to be related to an identifiable person. Unlike personal data, confidential data are always sensitive and never in the public domain and are applicable to data subjects that are both 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 the project is completed. 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. These should be agreed with investigators prior to implementation.
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

Uncontrolled when printed

	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.

3. Background

Data collected for clinical research must follow rigorous and formalised data management procedures which are intended to ensure that the study's data are as complete and accurate as possible. For Clinical Trials of Investigational Medicinal Products (CTIMPs), The Medicines for Human Use (Clinical Trials) Regulation states that 'All clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification' (Part 2 (9) Schedule 1 SI 2004/1031). Staff working on clinical research studies should follow the ALCOAC principles to ensure the integrity of the data:



PID and pseudonymised data should be processed in a way that is compliant with the principles of the UK General Data Protection Regulation (UK GDPR) and confidential data must be handled in accordance with the Common Law Duty of Confidentiality to protect the rights and freedoms of data subjects. The UK GDPR requires that appropriate security measures are in place to safeguard against unauthorised or unlawful access/processing of personal identifiable data.

4. Procedure

4.1 Responsibilities

Chief Investigator (CI):	Responsible for ensuring that 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):	Responsible for the integrity of the study data at a given investigator site.

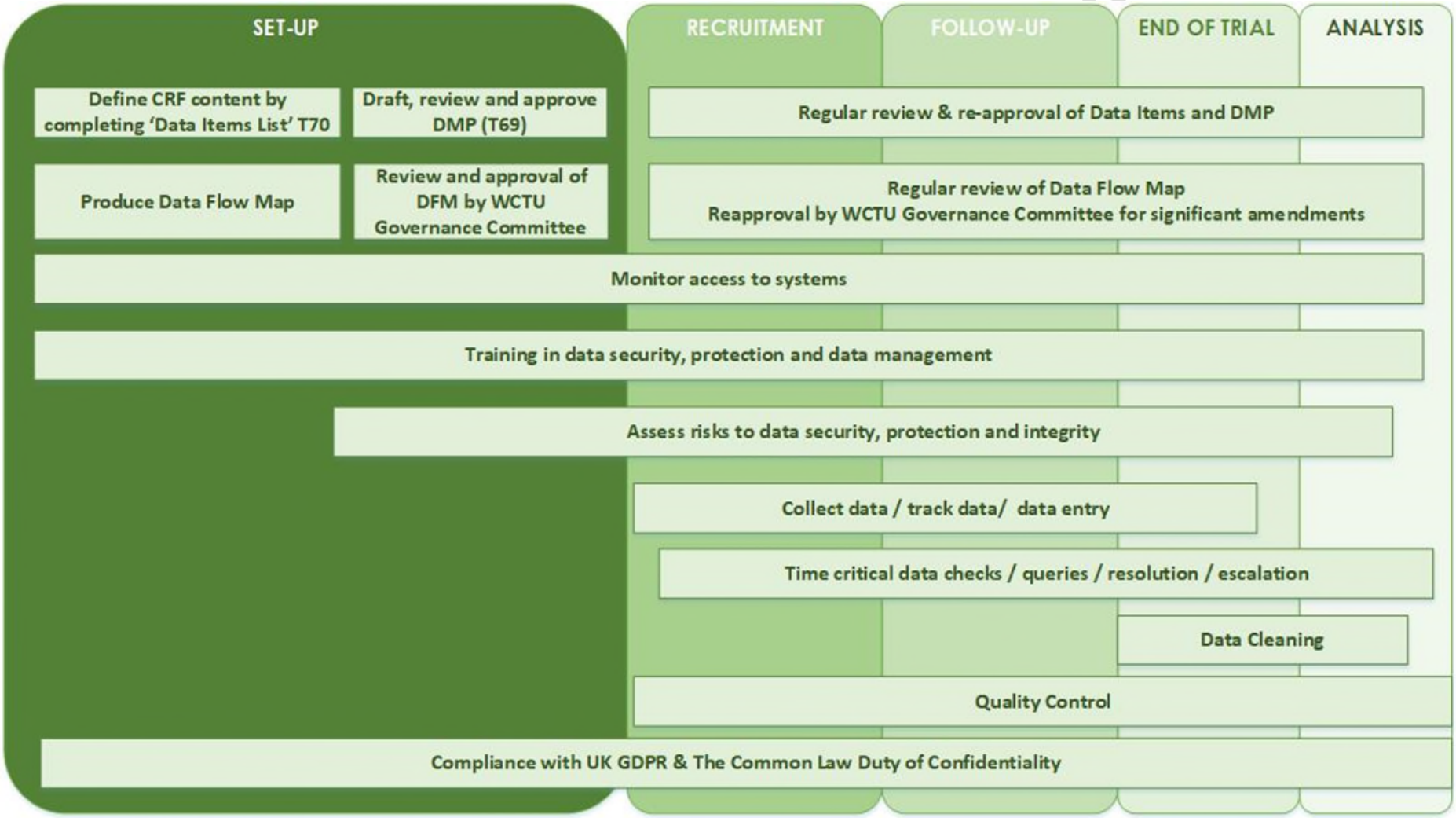
Typical delegation for WCTU managed studies:	
Trial Manager/Trial Coordinator (TM/TC):	• Coordinating the production, review, and approval of study DMP. • Managing all aspects of trial data collection in conjunction with approved protocol and DMP as delegated by the CI.
Statistician:	• Ensuring the mathematical integrity of the trial data throughout its lifecycle, • Reviewing and providing input into the study DMP and protocol.
Programming Team:	• Developing and maintaining the CDMS
Data Entry Clerk (DEC):	• Handling data management tasks as outlined in the approved DMP under the supervision of the TM/TC.
QA Manager:	• Ensuring that staff adhere to the principles and practices outlined in this SOP.
All individuals	• 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 they are responsible for. • Creating strong passwords and maintaining the confidentiality of passwords. • Complying with Data Protection Legislation, GCP guidance and any regulatory requirements for the maintenance of confidentially of participant identity.

4.2 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 green light.

Uncontrolled when printed

4.3 How?


SET-UP
RECRUITMENT
FOLLOW-UP
END OF TRIAL
ANALYSIS
Define CRF content by completing 'Data Items List' T70
Draft, review and approve DMP (T69)
Regular review & re-approval of Data Items and DMP
Produce Data Flow Map
Review and approval of DFM by WCTU Governance Committee
Regular review of Data Flow Map
Reapproval by WCTU Governance Committee for significant amendments
Monitor access to systems
Training in data security, protection and data management
Assess risks to data security, protection and integrity
Collect data / track data/ data entry
Time critical data checks / queries / resolution / escalation
Data Cleaning
Quality Control
Compliance with UK GDPR & The Common Law Duty of Confidentiality

4.3.1 Compliance with the UK GDPR and the Common Law Duty of Confidentiality

Depending on the nature of the study, consideration should be made for how personal identifiable and confidential data are handled to ensure compliance with the UK GDPR and the Common Law Duty of Confidentiality. The study protocol and Patient Information Sheet (PIS) should outline how personal and confidential data will be handled, and the data management procedures should detail the practicalities of ensuring compliance with these approved documents including the deletion and anonymisation of data within the appropriate timelines. It is the personal responsibility of all staff handing data to be aware of its classification and to handle it in accordance with the University's Information Management Policy Framework.

Further information on the UK GDPR principles: The principles | ICO
Further information on UK GDPR & Common Law Duty of Confidentiality in research: UK GDPR & Common Law Duty of Confidentiality MRC

4.3.2 Generation, review, and approval of DMP

A DMP must be produced for all studies to describe specific procedures for assuring data quality and integrity. A template is available to populate (**T69**). The first approved version of the DMP should be in place at the point of study Green Light.

Study specific working instructions can be used and referenced by the DMP if they contain trial specific details of processes but essential information relating to integrity, quality or interpretation of the data should be in the DMP. Any working instructions should be maintained and approved by the trial team in line with SOP 34 'Generation, Review and Approval of Trial Specific Working Instructions'. The DMP and associated working instructions should be regularly reviewed in response to changes within the trial and within the regulatory landscape.

The DMP (and any subsequent revision) should be **approved by the CI.**

For **WCTU Managed Studies**, input, and review of the DMP should also be sought from the following:

- Statistician
- QA
- Health Economics (HE) (if DMP references HE data)
- Other people that contribute expertise/decisions relating to data
- Senior Project Manager

Approval should be managed using an appropriate approval mechanism and should be in place from all parties prior to implementation. Emailapproval is acceptable if it follows the key principles outlined in **G33 'Email Approval Guidance'**.

4.3.3 Generation, review, and approval of Data Flow Map

For WCTU managed studies, an approved data flow map should be in place prior to the transfer of data between organisations occurring as part of the research study. The flow map should represent the current intentions for the flow of data between the data controller(s) and the data processors for the study and should include:

Uncontrolled when printed

- nature of the information to be shared (including its information classification)
- Why it is being shared
- appropriate safeguards to protect the data in transit and at rest ICO – Security

The data flow map should be reviewed and approved by the WCTU Governance Committee by submitting a draft copy or revision to WCTUQA@warwick.ac.uk. The Committee will provide feedback in writing and if relevant, confirmation of approval. Major changes to the flow of data should be submitted for reapproval prior to implementation.

A data flow map builder template **T41** is available and the link to the university policies on handling information and appropriate storage and transfer methods can be found here within the Universities Information Management Policy Framework. IG05 Information Classification Policy is helpful when determining the risk level on your data flows.

4.3.4 Assess risks to data security and integrity

Other risks to the security and integrity of processing data in addition to those associated with transfer Risks should be documented in the Risk Assessment and Monitoring Plan. Where risks are identified, there should be mitigations. Mitigations may include checks or processes that need to be documented in the DMP. Where the risk assessment does not document data related risks, a Data Protection Impact Assessment (DPIA) may be required. More information about conducting a DPIA can be found here.

For **WCTU Managed Studies**, a Data Protection Impact Assessment (DPIA) has been conducted at a quality system level. For studies that will process data outside of the scope of the WCTU DPIA or the Risk Assessment does not document data related risks in detail, staff should consider whether a project level DPIA is required. The WCTU DPIA is located here: WCTU DPIA

4.3.5 Access to systems

Access to systems involved in processing trial data should only be granted when:

- There is a clear and justified purpose
- The level of access is outlined in the information provided to participants
- Appropriate safeguards are in place to ensure the security of the data

Users should only be granted the minimum-security rights necessary to carry out their roles. User access should be reviewed and amended regularly to reflect changes. If for any reason a person no longer requires access to a system, access must be revoked as soon as possible.

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.

See Appendix 1 for details of password requirements.

Uncontrolled when printed

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 considered 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.
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	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		

4.3.6 Training on data security, protection, and management

- Data management activities should only be undertaken by appropriately trained members of staff who have been delegated by the CI (coordinating centre) or the PI (investigator sites).
- A training plan for data management activity at the coordinating centre (inc. competency thresholds if appropriate) should be defined in the DMP. See also SOP 24 'Essential Training and Training Records'.
- Completion of training and relevant evidence of competency should be documented in training records.

4.3.7 Collection of data & tracking its receipt

Data can be collected from several sources, including but not limited to:

- Direct completion by the participant (paper or electronic).
- Transcription from source data e.g., key information from participants' medical notes transcribed onto paper or electronic Case Report Forms (CRFs). Where an electronic application is used, this is termed Remote Data Capture (RDC). For most cases, RDC removes the need for completing paper forms and sending to the coordinating centre for entry.
- Transcription from interviews/conversations with participants where the CRF becomes the source document *(if this is to happen then this should be clearly documented in the protocol and evidence of training for people capturing this information should be available)*
- Datasets imported or downloaded from external sources e.g. Central Laboratories, NHS England *(subject to the appropriate data sharing/processing agreements*).

Uncontrolled when printed

The following processes should be in place with regards to collection of data:

* *For systems managed by the WCTU programming team, entry date of data is captured in the audit trail*

4.3.8 Entry of data into the CDMS

- Data entry must only be done by people who have been appropriately trained to use the system.
- All data items must be entered exactly as they appear on the data form, including spelling mistakes and grammatical errors. This will ensure that the data inputted is a true reflection of the data received. Where this will not be the case, it should be listed in the DMP and should follow the process outlines in section 4.3.10.1, Self-Evident Corrections (SECs).
- The CDMS should include a range of in-built validation checks to identify possible errors. Where this is not in place, a manual system should be in place.
- Any discrepancies arising as the result of data entry should be dealt with as per section 4.3.9 and the DMP.

	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'.
Access to CDMS	Evidence of training should be documented before access to CDMS can be granted. Individual log in credentials should be used to access CDMS and appropriate authentication in place. For system access requirements see section (4.3.4).	
Audit trail considerations	Where a CDMS will be used that is not managed by the WCTU programming team, there should be a method for indicating the form has been entered, by whom and when.	

Controlled when printed

4.3.9 Checking incoming data

- All incoming data should be inspected and checked according to timelines defined by the DMP or Monitoring Plan (MP).
- There should be a manual or automated process detailed in the DMP for checking incoming data. The nature of the checks should have input from statistical and clinical members of the study team and may include checks for:
    - logic
    - consistency
    - missing data
    - incorrect/implausible data
- If inspection of a data form reveals the need for clarifications, this should be followed up with the investigator site as soon as possible.
- There should be a documented process for tracking queries that have been sent and remain unresolved so they can be monitored and escalated if responses are not received within the expected timelines.
- If any of the checks indicates a potential protocol non-compliance, it should be dealt with according to SOP 31 'Handling Non-Compliance, Misconduct and Serious Breaches of GCP and/or Study Protocol'.
    - There must be a process to check the person completing data on the CRF is appropriately delegated to do so and it can be verified that that person completed the form or entry of the data.
- The timeliness of checks on incoming data and the regularity of statistical data cleaning should be risk assessed and outlined in the DMP and/or MP. Where these checks have taken place, there should be documentation to demonstrate they were undertaken as per the DMP or MP.
- The DMP should include how quickly they should be checked and how this should be done. Some incoming data may need to be checked in a more time sensitive manner for identification of safety or compliance issues where prompt intervention may be required. This should be considered when deciding how often such data should be assessed.

The DMP should detail the following in relation to data checks:

- ✓ When and who will perform the checks
- ✓ Outcome of the check, was it satisfactory or requiring further escalation?
- ✓ Details of the escalation (where required) and signpost to any outcome and should be appropriate to the urgency
- ✓ How the check, outcome and any associated escalations will be documented.

4.3.10 Resolution of queries

- It is good practice to use a Data Clarification Form (DCF) for raising queries with investigator sites, this can work for paper CRFs or RDC. This can be a DCF per site, per form or per participant with a list of queries. DCF guidance can be found next to this SOP (**G01**)
- Any amendments made to the original or copies of the CRF in response to queries raised should be clear with regards to who made the change and when. For RDC systems, the site would make the appropriate changes directly into the system. The requirement for recording who made the change and when will be provided via the audit trail where systems managed by the WCTU Programming Team are used. For paper-based systems, physical application of a name and date will be needed. It is essential that the method of correction ensures that the original entry is still legible.
- For paper systems where a response to a query is provided on a DCF rather than directly editing the CRF, it should be clear from the DCF that the coordinating centre will make the changes and that the investigator site should do the same on their copy. There should be a space on the DCF

Uncontrolled when printed

for the site to confirm this has been done and they give permission for us to do the same. The person signing the DCF should be appropriately delegated by the PI, and this should be checked by the coordinating centre on receipt of the DCF.

- Where it is appropriate to query data relating to Participant Reported Outcome Measures (PROMs), this can be dealt with by phone, but the exact method and number of contact attempts should be detailed in the DMP, and this approach detailed in the Patient Information Sheet (PIS).
- Where a phone call is used to obtain missing data from a participant, the audit trail should be maintained by detailing the method, date and person obtaining the data next to the correction.
- Whatever method is used, the query and any correspondence relating to it must be recorded and the paperwork filed with the data forms, ensuring all data are anonymised where this is relevant.

4.3.10.1 Use of Self-Evident Corrections (SECs)

- A SEC is where changes to the CRF can be made by trial data management staff without the requirement for item-by-item referral to the PI or their delegate. These may be used in specific, limited circumstances which must be considered and defined on a trial-by-trial basis and documented in the DMP. Use of SECs can reduce the effort to correct obvious mistakes and therefore the time that both the data management personnel and investigator spend on data corrections.
- Statisticians should be involved in discussions to determine where/if this process may be implemented.
- The use of SECs must not however be a substitute for a formal data query process.
- Before implementing the use of SECs, there should be prior agreement of the intended list of fields where SECs may be implemented by the PI or their delegate at each investigator site.
- When a SEC is used, it is good practice to record which Trial Numbers (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.

Table 1. Common examples of SECs

Adding information available on other forms that has been left blank on a particular form e.g. date of birth, hospital name
Where a Yes/No box has not been ticked but information has been completed in a subsequent text box that provides the answer to the Yes/No question
The correction of the common error that occurs in early January when dates are written using the previous year

4.3.10.2 Escalation for non-response to queries for missing or incorrect data

- The DMP should outline the timelines for return or entry of all data. Timelines for forms that include items where there is a time sensitivity related to the checks should have expected timelines for return in line with the risk and how quickly such issues need to be addressed. These expectations should be communicated during site set-up and activation.
- Progress against these expectations should be monitored by the study team. The DMP should outline any escalation plan for if the return rate of data is outside of the expectations communicated to the site.

4.3.11 Deletion of personal data

Personal data should be securely removed after it has been used for stated purposes. The removal process will depend upon the software used to secure the data. For further advice on encryption and

Uncontrolled when printed

secure deletion methods contact the ITS helpdesk. Personal data associated with research participants should not be stored on the network drive without use of additional encryption, where possible it should be contained within the CDMS.

4.3.12 Disclosure of confidential information

Very occasionally, information contained in a participant's response to a form may indicate an issue which may jeopardise the safety of the participant or another person. If there is any indication in a trial participant's response of a serious problem, or any issue in relation to their personal safety or to the safety of others, this should be reported to the CI or their delegate (e.g. nominated clinician on the trial team) who will decide on the appropriate action.

This may on very rare occasions necessitate a breach of participant confidentiality to maintain their safety. Disclosure of such information may be necessary in situations where failure to disclose appropriate information would expose the participant, or someone else, to a risk of serious harm (including physical or sexual abuse) or death.

The trial protocol (and application to the research ethics committee) should specify the process to be followed if the CI considers it is necessary to breach confidentiality, including to whom information may be disclosed and how this will be documented.

In such circumstances the participant should be informed that information will be shared with another party and the nature of the information to be shared, unless the CI considers it unsafe to do so.

4.3.13 Data Security Concerns

If you have had a university device which has been stolen or lost the following policy outlines how this should be reported: IS10: Mobile & Remote Working Policy.

In addition to this, any report should include

- WMS IT: WMS-it@warwick.ac.uk
- WCTU QA Team: WCTUQA@warwick.ac.uk

A lost or stolen device may also constitute a data breach so the process in SOP 36: WCTU Data Breach Process should be followed.

You can also raise any information governance or security risks to the Information Governance Working Group by contacting WCTUQA@warwick.ac.uk.

Uncontrolled when printed

List of abbreviations

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
DCF	Data Clarification Form
DEC	Data Entry Clerk
DMP	Data Management Plan
DPA	Data Protection Act
ePRO	Electronic Patient Reported Outcomes
eQMS	Electronic Quality Management System
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

Uncontrolled when printed

Appendix 1: WCTU Strong Password Requirements

- Must contain a minimum of 12 characters
- Must include characters from 3 of these categories:
    - Upper case letters
    - Lower case letters
    - Numbers from 0-9
    - Non-alphanumeric characters (excluding currency symbols)
    - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages
- Lockout after 5 attempts (15-minute duration)
- Password history (the system will remember 24 passwords before the same password can be reused)

Available Templates & Guidance

G01 Data Clarification Form Guidance

T69 Data Management Plan Template

T41 Data Flow Map Builder

G33 Email Approval Guidance

Uncontrolled when printed