# SOP 730, Computer System Validation

| | |
|---|---|
| **For Use in:** | Research |
| **By:** | All staff |
| **For:** | All staff involved in the conduct of research |
| **Division responsible for document:** | Research & Development |
| **Key words:** | Computer System Validation |
| **Name of document author:** | Francesca Dockerty |
| **Job title of document author:** | Clinical Trial Monitor |
| **Name of support to document author:** | Martin Pond |
| **Job title of support to document author:** | Head of Data Management,<br>Norwich Clinical Trials Unit, UEA |
| **Name of document author's Line Manager:** | Julie Dawson |
| **Job title of author's Line Manager:** | Research Services Manager |
| **Supported by:** | Julie Dawson NNUH<br>Sarah Ruthven UEA |
| **Assessed and approved by the:** | Julie Dawson: Research Services Manager NNUH<br>Sarah Ruthven: Research Manager UEA |
| **Date of approval:** | 04/04/2023 |
| **To be reviewed before:**<br>This document remains current after this date but will be under review | 04/04/2026 (3 years, unless legislation or process changes) |
| **Reference and / or Trust Docs ID No:** | 17357 |
| **Version No:** | 2 |
| **Description of changes:** | Updated glossary, new step 4, 5, 6 in section 10, new template, Section 9 updated. Reference to SOP 700 included. |

This Standard Operating Procedure (SOP) is available on the Research & Development pages on the NNUH website

Copies printed from the website are only valid on the day of printing.

## 1. Contents

## 2. Definitions of Terms Used / Glossary

| | |
|---|---|
| CI | Chief Investigator |
| CSV | Computer System Validation |
| eCRF | Electronic Case Report Form |
| ICH GCP | International Conference on the Harmonisation of Good Clinical Practice |
| MHRA | The Medicines and Healthcare Products Regulatory Agency |
| PI | Principal Investigator |
| R&D | Research and Development |
| RGC | Research Governance Coordinator |
| RSM | Research Services Manager |
| SOP | Standard Operating Procedure |
| SI | Statutory Instrument |
| URS | User Requirement Specification |

## 3. Objectives

This SOP describes the process for Computer System Validation (CSV) for use in assessment of the suitability and ensuring the software is fit for purpose.

## 4. Scope

This SOP applies to Vendor supplied or in-house built software programmes for use in Clinical Trials ICH GCP E6 /SI 2004/1031and 2006/1928 as amended.

## 5. Purpose

It is vital that any computer system/software used for a clinical trial has undergone a full validation process known as Computer System Validation (CSV).

The purpose of validation is to demonstrate that a system is developed, used, maintained, evolved and eventually decommissioned, in a controlled, documented manner that is consistent with its intended use.

CSV must cover software, hardware, processes and people (users). The overriding rationale for validation is that it ensures quality, timeliness, and efficiency, by effectively addressing risks.

The Medicines and Healthcare Products Regulatory Agency (MHRA) routinely look at computer system validation as part of their routine inspection, therefore it is necessary to ensure any systems used have undergone a validation process and all associated documentation and audits are in place.

## 6. Due Diligence

### System/software from a vendor supplier:

- Although the vendor may say that they have fully validated the system this is not adequate for use in a clinical trial unless an in-house validation has been undertaken
- Validation needs to be undertaken to ensure that the user requirements, specification and funtionality of the system meet those requirements
- Testing of the system for those requirements needs to be undertaken prior to system release to ensure the system is fit for purpose
- An audit of the CSV is required and a certificate should be issued following approval of the system

### System/software supplied from the sponsor of a study:

- If a system is supplied for use on the study by the Sponsor, evidence of validation of that system needs to be provided, e.g. a validation certificate and any supporting documentation
- Contact R&D office for advice and audit of the documentation supplied
- Whilst it is the sponsor responsibility to ensure the system is validated, evidence needs to be seen

### System/software built in-house:

- For any system build it is vital that the end product does what it was intended to do
- This should be decided at the beginning by producing User Requirement Specification (URS) and functionality Documentation
- The full validation process must then be followed

## 6.1 Due Diligence Minimum Requirements

- Validation reports should be checked ensuring they correspond to the version of the software being used
- If it details the system's functionality then ensure all the functionality being used is covered in the report

- If you receive a validation pack; does it show the system to be successfully validated? Has all the functionality intended for use been tested and has it passed?
- Is it evident who the tester was and have they signed and dated everything correctly?

- Is it evident how test fails have been rectified?
- Is there any cause for concern such as a missing follow-up test after a fail or undecipherable testing?

- Are the dates sequential?
- Was all testing completed before the product was released?

- Were all the specification requirements and test scripts agreed and signed off before the build had been completed?
- Was the validation report issued prior to release?

- Can any concerns be addressed?
- Can they be self-validated or mitigated in another way?

- Conduct a formalised risk assessment, document any findings and record any mitigating action to be taken
- Ensure the mitigation actions are carried out, completed, and evidence retained

## 7. Rules

- Each development and validation step must be documented to ensure that a full audit trail is available; actions and corrections must be agreed, implemented and traceable
- All documentation should be verified by the system developer/manager retained and available for audit. Without the supporting documentation the validation will not be recognised as valid.

## 8. User Specifics

System validation does not stop with the systems development; there are also the users to consider.

You can have a very reliable and fully validated system, but if the users are not able to use it correctly there are likely to be user generated errors that could potentially lead to non-compliance e.g. a user is performing a study specific configuration of an electronic Case Report Form (eCRF) and is not aware that certain fields need to be flagged as mandatory and are not automatically categorised as such. This could result in data not being collected or edit checks relating to subject eligibility not being effective as the data point needed to fire the edit check has not been collected.

Common findings relating to the user aspect of validation include:

- The product being released to the customer before the training material (i.e. user guide) has been developed and released
- Users being given access to the system with no training
- Users being given inappropriate (higher level) access such as the ability to make data changes
- User material not being reviewed or updated following the release of a new version with new functionality
- Users not being notified of system updates that included changes to functionality
- Internal processes and SOPs are not followed and as a result the formal review and approval of key documents such as validation plans, test scripts and reports are not completed

## 9. Contracts

The organisation responsible for contracting the supplier must conduct a vendor risk assessment as per Joint Research SOP 700, Vendor Selection, Approval & Oversight and ensuring the provider and the system meet regulatory requirements.  A completed risk assessment needs to be reviewed by the Sponsor and finalised prior to signing contracts.

## 10. Development and Validation Life Cycle Process

A development and validation plan should be produced prior to development commencing. This will document each step of the process and describe what is required for each step. It will also describe the revision and correction process required.

Development team members and System Manager should be listed in the plan. Reference to supporting documentation should be made. Each step and each document should be signed off by the System Manager as fit for purpose or recommendations added for revision.

Any revision or corrections must be carried out and documented before the sign off process can be conducted.

**Each step must be completed before the next step can commence.**

**Step 1 - Requirements (User Requirements and Functionality Specification):**

- The first phase involves understanding what are the needs to the design and what is its function, purpose, etc
- The specifications of the input and output of the final product are studied and marked
- Suitable audit trail

**Step 2 - System Design:**

- The requirement specifications from the first step are studied in this step and system design is prepared
- System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture
- The software code to be written in the next stage is created now

**Step 3 - Implementation:**

- With inputs from system design, the system is first developed in small programs called units, which are integrated into the next step
- Each unit is developed and tested for its functionality which is referred to as Unit Testing

### Step 4 - Integration and Testing:

- All the units developed in the implementation step are integrated into a system after testing of each unit
- The software designed, needs to go through iterative software testing to find out if there are any flaw or errors, and to ensure that it performs as expected
- Testing is done to ensure that the sponsor does not face any problem during the installation of the software

### Step 5 - Deployment of the System:

- Once the functional and non-functional testing is done, the product is deployed in the use environment or released
- Consideration should be given to the role of the environment in maintaining a validated state and thereby maintaining data integrity, through both contingency measures (such as taking regular backups) and preventative measures (logical and physical security, including account access, firewalls and anti-virus software)

### Step 6 - Maintenance:

- This step occurs after installation, and involves making modifications to the system or an individual component to alter attributes or improve performance. These modifications arise either due to change requests initiated by the customer, or defects uncovered during live use of the system. The user is provided with regular maintenance and support for the developed software.
- Maintaining hardware is also an important aspect of maintaining the validated state. This might include deploying software patches on a regular or prescribed basis, and conducting regular scans for known and emerging vulnerabilities (for example, penetration testing).

## 11. Revalidation

Computer systems should be revalidated to maintain the validation status during the entire life of the system. Revalidation is either time based, or event driven:

Time Based - Computer systems should be regularly revalidated. Type of revalidation and frequency depend on system criticality and stability

- Systems supporting highly critical applications should undergo full revalidation after two years. Test procedures should be the same as for initial validation
- Systems supporting medium critical applications should be reviewed for compliance of the actual configuration with documentation and ongoing tests with tests plans. If evaluation findings meet acceptance criteria, no revalidation is required
- Systems supporting low critical applications don’t need revalidation
- Time based qualification can be omitted if the system has been revalidated for other reasons, for example, after changes

Event driven revalidation is mostly triggered through changes of hardware, software or accessories. Any change to the system should include an assessment of what type of revalidation is required

- Systems should be revalidated after installation of new versions of software
- Functions that are new or have been changed should be validated
- In addition, a regression test should be performed to verify correct functioning of the complete system

The detailed evaluation and final decision on type and extent of revalidation should be made by the system owner and supported by IT

- The decision what and how to revalidate should be based on risk assessment and should be justified and documented
- Criteria for the extent of revalidation are the criticality of the system and the type of change

## 12. Change Control/Management

Post-release any changes to the software which may have an effect on the user requirements, functionality and specification must undergo a revalidation process which mirrors the original validation. Therefore there should be a mechanism in place to ensure awareness of full version control of a system.

It is vital the changes to the software/system are identified; follow the life cycle process to ensure all original outcomes are met before the updated system is released for use.

It is important that the change control procedure used is fully documented at each stage, documentation retained to demonstrate that the process has been followed, any bugs are fixed and an overall assessment of use is approved by the system manager prior to release.

There must be a process in place to track any changes following the release of a substantial amendment, ensuring that the software/data capture system is suitable to incorporate any changes required. The software/system may need to be changed and therefore will require a change control/change management life cycle CSV. This may need to be undertaken for the changes and also to ensure the validity and functionality of the entire system. Do the changes have an effect on the software, hardware, processes or the people (users).

For systems provided by the Sponsor or Vendor you must perform due diligence and gather evidence of a life cycle change control/management process prior to release for use.

Change control should be carried out during all phases of system design, development and use. It applies to all configuration items as defined in the initial set-up. Information on change control should include:

- System ID and location
- Persons who initiated, approved and implemented the change
- Description of the change, including the reason for the change and the benefit
- Priority
- Expected impact on validation
- Date of implementation

Other important points are:

- Changes are managed by the system owner
- Change control procedures should be able to handle planned and unplanned changes. An example of an unplanned change is replacing a defect hard disk with a new one
- Change control should always include a risk assessment on how the change may impact system performance
- All changes should be recorded in a change control history log document

## 13. Other considerations

### Security:

- User access security levels
- Password access limits (limited to single user only)
- Maintaining a current user list
- Removal of access

### Disaster Recovery Plan:

- A system should have a disaster recovery plan; which must be tested and updated if there is a change control/management implemented

### Back up and restore:

- Back up and restore of data must be included in the life cycle process and must be tested, this includes the change control/management process

### Deviation:

- Any deviations should be fully assessed, documented, and actions agreed for follow-up
- Users must be aware of the deviation process

### Documentation Management:

- Decide at the very first stage how the Life Cycle documentation will be managed and stored and who holds the responsibility for this.

## 14. Retrospective Validation / Legacy Systems

Validation of an existing system, whether it was purchased or internally developed, is called retrospective validation. Retrospective validation is employed:

- When a system not previously validated is allocated to GCP studies
- When a system that was validated has lapsed to a non-validated status
- Including when the standard of validation performed is no longer considered adequate

Where retrospective validation is required it will be based (as much as possible) on recovering the equivalent documents for prospective validation. The effort required to generate these documents depends on:

- The adequacy of existing documentation
- The degree of system customisation
- The intention for future changes

## 15. Decommissioning

Ensure a detailed plan for decommissioning of a system is in place.

If the decommissioning of a system is to allow the introduction of a new system, then the plan must include a detailed description of data transfer from the old system to the new system.

The plan must include archiving requirements for the old system, which must detail location of storage, access and read rights to the old system once archived.

## 16. CSV Audit

For Vendor supplied systems refer to SOP 700 NNUH Vendor Selection and Oversight. The Pre-qualification Questionnaire & Risk Assessment form must be completed and approved by the Chief Investigator (CI)/Principal Investigator (PI) and by the Research Services Manager (RSM) or Research Governance Coordinator (RGC).

For systems supplied by external sponsors refer to SOP 720 Risk Assessment of Clinical Trials Sponsored by NNUH and UEA. The primary risk assessment mist be recorded on the Edge database attribute and approved by the RSM or RGC.

A change control/change management audit must be performed prior to the changes being released for use. This will ensure the system changes are suitable.

When a system is decommissioned an audit should be undertaken to ensure there is a decommissioning plan available and that the plan is being followed. It is vital that the data transfer is acceptable and data storage and access once archived is acceptable to ensure data integrity.

For in-house built systems:

- A full CSV audit will be required and undertaken by R&D
- The audit will be undertaken prior to release to ensure all steps of the validation life cycle process has been followed and the appropriate documentation is complete and has been approved and maintained
- Once the audit is complete and actions are resolved the audit will be signed off by R&D and a validation certificate will be issued
- The validation certificate will be valid for 2 years
- An audit must be undertaken every 2 years; if the system is still in use
- A validation certificate will be issued following each successful audit
- Where there is a change control/management for a system then a change control/change management will be required for the changes
- R&D will issue an approval certificate to use the updated system

## 17. References and Related Documents

| References |
|---|
| ICH GCP E6 / SI 2004/1041 |
| |

| SOP No. | SOP Title |
|---|---|
| SOP 700 | NNUH Vendor Selection and Oversight. |
| SOP 720 | Risk Assessment of Clinical Trials Sponsored by NNUH and UEA |

## 18. Approval

| | |
|---|---|
| **Author** | Francesca Dockerty / Martin Pond |
| **Role** | Clinical Trial Monitor **/** Head of Data Management, Norwich Clinical Trials Unit, UEA |
| **Approved & Authorised NNUH** | Julie Dawson |
| **Role** | Research Services Manager |
| **Signature** | DocuSigned by:<br>Julie Dawson<br>4CBAB366CF354A2... |
| **Date** | 05 April 2023 \| 7:27 BST |
| **Approved & Authorised UEA** | Sarah Ruthven |
| **Role** | Research Manager |
| **Signature** | DocuSigned by:<br>Sarah Ruthven<br>6EB42B4E497249C... |
| **Date** | 04 May 2023 \| 4:11 BST |

## 19. Reason for Update and Training Implication

This SOP replaces the previous version number V1

| Changes made | What changes have been made to the contents of the document |
|---|---|
| Reason | • New layout<br>• Revision in procedure |
| Training Implication | **No** |
| Actions required | • NA |