# COMPUTER SYSTEM VALIDATION

| | |
|---|---|
| **DOCUMENT NO.:** | **POL007 v2.0** |
| **AUTHOR:** | **Lorn Mackenzie** |
| **ISSUE DATE:** | **29 APRIL 2020** |
| **EFFECTIVE DATE:** | **13 MAY 2020** |

## 1 INTRODUCTION

1.1 The Academic & Clinical Central Office for Research & Development (ACCORD) is a joint office comprising clinical research management staff from NHS Lothian (NHSL) and the University of Edinburgh (UoE).

1.2 Sponsors must maintain oversight of computerised systems used in clinical trials that capture, process, analyse and report clinical trial data.

1.3 To demonstrate computer systems are “fit for purpose”, particularly those that impact on the quality of the trial data (and subject safety), the Sponsor must ensure the validation, integrity and security of the data. Examples of systems include; pharmacovigilance databases, eCRF systems, clinical trial databases, electronic transfer of data, electronic diaries for subjects and electronic trial master files.

1.4 The process of establishing documented evidence that a computerised system will consistently perform as intended is known as Computer System Validation (CSV).

## 2 SCOPE

2.1 This Policy applies to Investigators responsible for ensuring computer systems are validated and fit for use for all studies sponsored by NHSL and/or UoE.

2.2 This Policy also applies to ACCORD staff involved in the identification and documentation of validated computer systems used in studies sponsored by NHSL and/or UoE.

2.3 Clinical research covered by this Policy is most often CTIMPs/CIMD (Clinical Trials with Investigational Medicinal Products/Clinical Investigations with Medical Devices), but may also include other invasive, experimental or complex research involving one or more research sites.

2.4 The creation and maintenance of computerised systems is out with the scope of this Policy. This is delegated to study teams and typically procured from suppliers or other agents.

## 3 POLICY

3.1 The level of CSV should be commensurate with the risk and impact of a data integrity failure to the study and/or participant. For studies subject to a combined risk assessment (GS002), the need for a CSV review is identified during the risk assessment process.

3.1.1 When the risk assessment dictates that this is required, the Quality Assurance (QA) Manager, or designee, will perform the CSV review using the CSV Checklist (GS002-T02). The level of validation required will depend on the system and the nature of the software/hardware (i.e. whether it is an off-the-shelf package, an off-the-shelf package with a trial specific configuration, or a bespoke system).

3.1.2 For studies not subject to a combined risk assessment (GS002), the Investigator is responsible for ensuring computer systems are appropriately validated and procedures are implemented to minimise the potential risk to data integrity.

### 3.2 Off-the-shelf Package

3.2.1 Off-the-shelf packages, for example MS Excel, are validated by the software developers before being released for sale. Excel may be used by study teams to undertake some simple analysis (e.g. analysis which does not impact on study outcomes and / or patient safety) however there must be a documented check on formatting of cells and any formulae that has been input into the system. This could simply be recording the ranges of the cells that have been checked, writing down the formulae or confirming the spreadsheet is consistent with the written specification prior to the use of the system.

### 3.3 Trial-specific Configuration

3.3.1 For trial-specific configuration systems using a commercial off-the-shelf package for example a REDCap database, the following documentation would be the minimum expected;

- User specification
- Testing documentation
- Validation Plan
- Validation Report
- User instructions and training of users
- Documented release
- Audit trail capability

### 3.4 Bespoke System

3.4.1 Bespoke application development, e.g. some Electronic Case Report Form (eCRF) systems, require more comprehensive validation documentation.

3.4.2 Validation of a bespoke system will require extensive testing and documentation will typically include;

- User specification
- Functional specification
- Testing Documentation

- Validation Plan
- Validation Report
- Risk Assessment
- User Manual
- Training Records
- Records of release
- System Back-Up
- Security system
- Audit trail capability
- System Interactions
- Continued accessibility

### 3.5 Documentation

3.5.1 The supplier of the computerised system should provide the functional specifications and design specifications.

3.5.2 In addition, a written validation plan and validation report is required for CSV.

3.5.3 Planned validation activities will be documented in a validation plan. The validation plan will define features of the system and how they will be tested to ensure they function as expected and the measure by which a test will be deemed successful will be included.

3.5.4 Test documentation will be developed in accordance with the validation plan. The validation report documents how the system maintains the validity, security and integrity of the study data. The testing should challenge the intended use and functionality of the system and the software's internal and external interfaces.

3.5.5 Evidence of test methods and test scenarios should be demonstrated and reviewed/approved by an appropriate reviewer, usually by a member of the software development team (i.e. programmer/designer) or study team (i.e. trial manager).

3.5.6 Details of the level of validation documentation required for each type of system is highlighted in the CSV Checklist (GS002-T02).

### 3.6 Change Management

3.6.1 To manage any changes to the computerised system and ensure the validated state is maintained during its lifecycle, there must be a sufficient change control process in place.

3.6.2 If there are any changes to the computer system or its configuration after release i.e. to correct an error or a modification in functionality, the reason for the change should be identified, approved and documented prior to release of a new version of the system.

3.6.3 ACCORD QA personnel must be informed of proposed changes to the computer system prior to system release.

3.6.4 Some eCRF systems may have their own version tracking facility. For studies monitored by ACCORD, version control of eCRFs will be tracked by the assigned ACCORD Clinical Trials Monitor in accordance with ACCORD SOP CR013 CRF Design and Implementation.

### 3.7 Audit Trail

3.7.1 An audit trial is necessary to document any changes or deletion of electronic data on a computer system.

3.7.2 There must be the ability to verify who entered the initial data item and when, with date and time stamping and evidence of who subsequently made changes to the data. The reason for any change must also be recorded.

3.7.3 The audit trail must be accessible by third parties (e.g. monitor, auditor, inspector) and there must be sufficient protection of the audit trail such that no direct modification of the stored information may be made, but read access is possible at any time.

3.7.4 Confirmation of the audit trail functionality will be demonstrated by QA personnel prior to sign-off of the CSV checklist (GS002-T02).

### 3.8 Quality Control (QC) Check

3.8.1 For data entered into an electronic system manually, there should be an additional check on the accuracy of the data. This may be done by a second operator or by electronic means, and must be recorded. There must also be a documented plan for the verification of critical data e.g. Source Data Verification (SDV) Plan (CM004 Developing a Monitoring and SDV Plan).

3.8.2 If data accuracy checks are performed electronically, the system's function must be validated to show accuracy.

### 3.9 Security

3.9.1 Physical and logical controls must be in place to restrict access to the system, including a process for revoking computer system access when a staff member leaves post or delegated duties on a study have ended. Access control should be strictly managed and controlled.

3.9.2 Validation should ensure that the function for unlocking and accessing the system is only available to authorised users and prevents unauthorised security access.

3.9.3 Authorised users and their level of access should be approved and assigned by the system owner and documented.

3.9.4 Patient related data must be treated with complete confidentiality and stored, analysed and processed in accordance with the General Data Protection Regulation (GDPR) and applicable NHSL policies. The collection, transfer and storage of patient identifiable information, including CHI numbers, must be in accordance with SOP GS008 Patient Identifiable Information: Caldicott Approval & Information Governance Review and applicable NHSL policies.

### 3.10 Data Back-up

3.10.1 The back-up and restoration of data procedures should exist in case data is lost and must be validated to the include the following;

- Frequency of back up i.e. daily
- The ability to restore the database at a given date and time in the past
- Verification of the ability to retrieve back up data and files
- Check for the accessibility, durability and accuracy of data and files retrieved
- Proof that the restore process functions
- An audit trail of the back up and restoration

### 3.11 Data Storage and Archiving

3.11.1 Electronic data should be stored and archived appropriately. The validation of data storage and archiving should ensure data accessibility, readability and integrity.

### 3.12 Other Considerations

3.12.1 Additional consideration should be given where a 'cloud' or 'virtual' service is used (that is online storage of data generally hosted by third parties), in consultation with NHSL Information Governance and IT Security.

3.12.2 Identifiable data must not be held on 'cloud' servers.

3.12.3 Contracts defining responsibilities will be considered at the Combined Risk Assessment (SOP GS002) with requirements documented.

3.12.4 For further guidance relating to CSV, please contact the assigned Sponsor Representative, Clinical Trials Monitor and/or QA team.

## 4 REFERENCES AND RELATED DOCUMENTS

- GS002 Combined Risk Assessment
- GS002-T02 Computer System Validation Checklist
- GS008 Patient Identifiable Information: Caldicott Approval & Information Governance Review.
- CR013 CRF Design and Implementation
- CM004 Developing a Monitoring and SDV Plan
- NHS Lothian Data Protection Policy
- NHS Scotland Confidentiality Code of Practice
- NHS Lothian eHealth IT Security Policy
- General Data Protection Regulation
- MHRA GxP Data Integrity Guidance and Definitions

## 5 DOCUMENT HISTORY

| Version Number | Effective Date | Reason for Change |
|---|---|---|
| 1.0 | 18 AUG 2017 | New Policy. |
| 2.0 | 13 MAY 2020 | Requirement to inform ACCORD of proposed changes to computer systems prior to system release added to 3.6.3. Requirement to record the reason for any change added to 3.7.2. Policy updated at 3.7.4 to confirm ACCORD QA personnel will confirm audit trail functionality. Minor administrative changes throughout |

## 6 APPROVALS

| Sign | Date |
|---|---|
| SIGNATURE KEPT ON FILE<br><br>AUTHOR: Lorn Mackenzie, QA Manager, NHSL, ACCORD | |

| | |
|---|---|
| SIGNATURE KEPT ON FILE<br><br>APPROVED: Heather Charles, Head of Research Governance, NHSL, ACCORD | |
| SIGNATURE KEPT ON FILE<br><br>AUTHORISED: Gavin Robertson, QA Coordinator, NHSL, ACCORD | |