Computer System Validation & Data Integrity

Document No.:	POL007 v5.0
Author:	Lorn Mackenzie
Issue Date:	22 MAY 2026
Effective Date:	05 JUN 2026

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 ensure that computerised systems used to capture, process, analyse, store, or report study data are reliable and suitable for their intended purpose. In accordance with the UK Clinical Trials Regulations, ICH GCP E6(R3), and the MHRA GxP Data Integrity Guidance, Sponsors are required to ensure that such systems are validated, secure, and capable of generating accurate, complete, and retrievable data throughout their lifecycle.

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

1.4 This Policy sets out the principles and expectations for CSV within NHSL and/or UoE sponsored research.

2 Scope

2.1 This Policy applies to all Investigators who are responsible for ensuring that computerised systems used in studies sponsored by NHSL and/or UoE are appropriately validated and fit for purpose. It also applies to ACCORD staff involved in the identification, assessment, and documentation of validated computer systems used in such studies.

2.2 The creation and maintenance of computerised systems is out with the scope of this Policy. This is delegated to study teams and typically undertaken by external suppliers or institutional service providers.

3 Policy

3.1 Identification of CSV Requirements

3.1.1 A CSV review is required for any computerised system used in a NHSL and/or UoE sponsored study where the system has the potential to impact participant safety, data integrity, or the reliability of trial results. This includes systems used to capture, process, analyse, store, transfer, or report clinical trial data.

3.1.2 The requirement for CSV review is identified during the Combined Risk Assessment (GS002). Studies which are typically subject to a combined risk assessment include CTIMPs/CIMDs (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 trial locations.

3.1.3 During the risk assessment (GS002), the Sponsor identifies all computerised systems used in the study and determines whether a CSV review is required. A review is required when any of the following apply:

- The system is not validated under a recognised quality management system;
- The system has been configured or customised for the study;
- The system performs trial-critical functions (e.g., eCRF, safety reporting, randomisation, electronic diaries, electronic TMF/ISF);
- The system generates or manages essential documents or source data;
- The system performs automated calculations or data transformations;
- The system interfaces with other systems in a way that could affect data integrity

3.1.4 For studies not subject to a Combined Risk Assessment (GS002), the Sponsor does not conduct a CSV review and does not oversee validation activities. In these studies, the Investigator is responsible for ensuring that any computerised system used to capture, process, analyse, store, transfer, or report study data is:

- Appropriately validated for its intended use;
- Supported by documented procedures;
- Governed under institutional or supplier quality systems;
- Capable of generating accurate, complete, and retrievable data in line with ICH GCP E6(R3).

3.1.5 Investigators must obtain and retain evidence of system suitability and ensure that validation activities are proportionate to the risks associated with the system's use.

3.2 Use of Routine Clinical Care Systems

3.2.1 Systems used solely for routine clinical care (e.g., EHRs, e-prescribing, LIMS) do not require full Sponsor validation; however, for studies subject to combined risk assessment (GS002), the Sponsor must document their suitability and ability to generate accurate, complete, and retrievable data at site feasibility (GS013). Any risks or gaps identified will be escalated to the QA Manager for proportionate mitigation.

3.3 Electronic TMF/ISF Systems

3.3.1 Electronic systems used for TMF or ISF management must provide controlled access, audit trails, version control, and secure storage that prevents unauthorised alteration or loss of data. These systems must support the integrity, authenticity, and retrievability of essential documents throughout the study and for the full archive period.

3.3.2 For studies subject to a Combined Risk Assessment (GS002), the Sponsor will review and approve any electronic system used for TMF/ISF management. The review will assess validation status, governance arrangements, access controls, audit trail capability, and long-term archiving provisions.

3.3.3 Where a site uses a location-owned eISF platform (e.g., Florence), the Sponsor will document its use at site feasibility (GS013) and confirm that the system is appropriately governed by the institution and capable of generating accurate, complete, and retrievable essential documents. Any risks or gaps identified will be escalated to the QA Manager for proportionate mitigation.

3.3.4 Shared drives, network folders, and SharePoint sites typically do not meet the regulatory requirements for TMF/ISF management because they often lack full audit trail capability, do not provide controlled version management, and may allow unauthorised modification, deletion, or overwriting of essential documents. These limitations present risks to data integrity, inspection readiness, and the long-term reliability of essential documents.

3.3.5 Where a validated eTMF or eISF system is not available and an alternative electronic storage solution is proposed (e.g., shared drive, network folder, SharePoint site), the institution or service provider must complete a documented risk assessment before any study documents are stored electronically. This assessment must identify system limitations and define proportionate mitigations—such as restricted write access, controlled upload processes, manual version logs, or periodic QC checks—to

ensure essential documents remain accurate, complete, and retrievable throughout the study.

3.3.6 For studies subject to a Combined Risk Assessment (GS002), the Sponsor must review and approve the risk assessment and confirm that the proposed mitigations are adequate. If the mitigations are deemed inadequate, essential records must be maintained in paper format. For studies not subject to GS002, the Sponsor does not review or approve these risk assessments. The Investigator and their institution are responsible for ensuring that the storage solution is suitable, that risks are assessed and mitigated, and that documentation is maintained in a manner that supports inspection readiness. All risk assessments and mitigation plans must be retained within the TMF/ISF.

3.3.7 Low-risk study documents are defined as non-essential records that do not impact subject safety, data integrity, or regulatory compliance and are readily replaceable (e.g., CVs, GCP certificates, superseded documents, administrative correspondence, draft documents, and other non-critical records). These may be stored temporarily on an institutional network drive, shared drive, or SharePoint location prior to transfer into the validated eTMF/eISF or validated archiving platform or paper TMF/ISF. These locations must be institutionally managed and routinely backed up. Where a document does not meet the low-risk definition, a proportionate risk assessment must be documented to identify system limitations, and define appropriate mitigations such as restricted write access, manual version tracking, and periodic QC checks (see section 3.3.6). Temporary storage locations must not be used as the primary or long-term repository for essential documents. All documents must be migrated to the validated system or paper file as soon as practicable.

3.4 Validation Requirements by System Type

3.4.1 Validation requirements differ according to the type of computerised system used in a clinical trial. Each category of system presents a different level of complexity, configuration, and risk, and therefore requires a proportionate approach to demonstrating that it is fit for purpose.

3.4.2 The following subsections set out the Sponsor's expectations for each system type. They describe the level of validation evidence required, how that evidence should be assessed, and how it must be documented to ensure that all systems used in NHSL and/or UoE sponsored research support data integrity, participant protection, and compliance with applicable regulatory requirements.

Off-the-shelf Systems

3.4.3 Off-the-shelf systems are commercially available software products used without modification to their core functionality (e.g., Microsoft Excel, standard statistical packages). These systems are generally validated by the developer as part of their product lifecycle. When used in a clinical trial, study teams must ensure that:

- The system is used within its intended and documented functionality;
- Any spreadsheets, templates, or tools created within the system are checked for accuracy (e.g., formula verification, locked cells, protection against unintended changes);
- Appropriate access controls are applied; and
- Outputs are reviewed and verified to ensure accuracy and consistency.

3.4.4 Documentation should demonstrate that the system is suitable for its intended use in the study and that any study-specific configurations (e.g., spreadsheet formulas) have been tested and verified. The Sponsor will assess validation evidence for off-the-shelf systems for combined risked assessed studies (GS002) to confirm that the system supports data integrity, participant safety, and regulatory compliance.

Study-specific Configuration

3.4.5 Some off-the-shelf systems allow configuration or customisation to support study-specific processes (e.g., REDCap). These systems require additional validation to ensure that the configured elements function as intended. Study teams must ensure that:

- User requirements and system specifications are documented;
- Study-specific configuration (e.g., forms, edit checks, workflows) is tested and verified;
- A validation plan and validation report are produced, proportionate to system complexity;
- User instructions and training materials are available;
- Audit trail functionality is enabled and reviewed; and
- System release and change control processes are documented.

3.4.6 The Sponsor will assess validation evidence for configured systems for combined risked assessed studies (GS002) to confirm that the system supports data integrity, participant safety, and regulatory compliance.

Bespoke System

3.4.7 Bespoke systems are developed specifically for a study and therefore require the highest level of validation oversight. These systems present increased risk due to their unique design and potential for untested functionality. Study teams must ensure that:

- detailed user requirements and functional specifications are documented;
- a validation plan defines the scope, testing strategy, acceptance criteria, and responsibilities;
- comprehensive testing is performed, including functional, integration, and user acceptance testing;
- a validation report summarises testing outcomes and confirms system readiness;
- system security, backup, and disaster recovery arrangements are documented and tested;
- audit trail capability is implemented and verified;
- system interactions and data flows are documented; and
- long-term accessibility and support arrangements are in place.

3.4.8 The Sponsor will review validation evidence for bespoke systems for combined risked assessed studies (GS002) to ensure that the system is robust, secure, and capable of supporting reliable clinical trial data.

3.5 Change Management

3.5.1 Changes to a computerised system or its study-specific configuration must be controlled to ensure the validated state is maintained throughout the system's lifecycle. All changes must be documented, justified, assessed for impact, and approved before implementation. The level of change control required must be proportionate to the system type and the potential impact on participant safety, data integrity, or trial conduct.

3.5.2 For studies subject to a Combined Risk Assessment (GS002), the Sponsor QA team must be informed of any proposed changes to systems used for trial-critical activities. The Sponsor will review the change, assess its impact on validation status, and confirm whether additional testing or documentation is required prior to release.

3.5.3 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.

3.6 Audit Trail

3.6.1 Computerised systems used in NHSL and/or UoE sponsored studies must include an audit trail that reliably records the creation, modification, and deletion of electronic data. The audit trail must identify who performed each action, when it occurred, and the reason for any change, and must be protected from alteration. Audit trail information must be accessible to authorised third parties such as monitors, auditors, and inspectors.

3.6.2 For studies subject to a Combined Risk Assessment (GS002), the Sponsor will confirm that audit trail functionality is enabled and appropriate as part of the CSV review.

3.7 Quality Control (QC) Check

3.7.1 Where data are entered manually into an electronic system, or where electronic data files (such as laboratory outputs) are manipulated prior to upload into a study database, appropriate quality control measures must be in place to ensure accuracy, completeness, and traceability. QC may be performed by a second operator or through validated electronic checks, and the approach must be proportionate to the criticality of the data. The method used to verify critical data must be documented, for example within the study's Monitoring and SDV Plan (CM004).

3.7.2 Where laboratory outputs or other externally generated data files are reformatted, calculated, merged, or otherwise transformed before upload, the original source file, the manipulated file, and a record of the transformation performed must be retained to allow full reconstruction of the data flow. Any manual or semi-manual manipulation must be documented and subject to QC. If electronic tools (e.g., Excel formulas, macros, scripts) are used to perform these transformations, they must be verified or validated to demonstrate that they operate accurately and consistently.

3.7.3 QC activities and outcomes must be recorded and available for review by monitors, auditors, and inspectors.

3.7.4 Where study data are obtained through systems or processes other than direct entry into the eCRF (such as bulk data uploads, device outputs, laboratory information systems, or external data-capture platforms), the acquisition, transfer, and upload of such data to the eCRF must be controlled to ensure accuracy, completeness, and

traceability. The detailed procedural requirements for managing these processes (including data mapping, transformation, quality checks, error handling, and PI review) must be documented in the study-specific Data Management Plan or equivalent.

3.8 System Security and Data Backup

3.8.1 Computerised systems used must have appropriate physical and logical security controls to protect the confidentiality, integrity, and availability of study data. Access to each system must be restricted to authorised users, with permissions assigned and approved by the system owner and reviewed regularly. There must be a defined process for promptly revoking access when staff leave their post or when delegated duties end. Validation activities must confirm that authentication and access-control functions operate correctly and prevent unauthorised access.

3.8.2 Patient-related data must be handled in accordance with the UK General Data Protection Regulation (GDPR) and applicable NHS Lothian policies. The collection, transfer, and storage of identifiable information, including CHI numbers, must comply with SOP GS008 *Processing Personal Identifiable Information: Caldicott Approval & Information Governance Review*.

3.8.3 Systems must have reliable data-backup and restoration processes to ensure data can be recovered in the event of loss or corruption. Backup procedures must be defined, implemented, and tested to demonstrate that data can be restored accurately to a known point in time, that backup files are accessible and durable, and that the restoration process functions as intended. Evidence of backup and restoration testing must be retained, including an audit trail of backup activities.

3.9 Archiving

3.9.1 Electronic data must be stored and archived in a manner that ensures long-term accessibility, readability, and integrity. Systems used for data storage or archiving must protect data from unauthorised access, alteration, or loss throughout the required retention period, in accordance with GS005.

3.9.2 Any electronic platform used as an eISF or eTMF archive must be validated and capable of preserving essential documents for the full regulatory retention period. Archived data must remain intact, retrievable, and readable without reliance on obsolete hardware or software. Where archiving is managed by the institution, the Investigator is responsible for ensuring that institutional archiving processes meet

these requirements and that essential documents remain accessible to authorised parties, including monitors, auditors, and inspectors.

3.10 Supplier and vendor assessment

3.10.1 For studies subject to a Combined Risk Assessment (GS002), the Sponsor must ensure that external suppliers involved in the provision, hosting, configuration, or support of computerised systems are suitable for their intended role (QA009 Vendor Assessment)

3.11 Disaster recovery

3.11.1 Systems used for trial-critical activities must have business continuity and disaster recovery arrangements in place to ensure that essential processes can continue during system outages or failures. These arrangements must be proportionate to system risk and may include downtime procedures, alternative data-capture methods, and defined recovery timeframes. Where continuity arrangements are institution-managed, the Investigator is responsible for ensuring that institutional processes meet these requirements. For GS002 studies, the Sponsor may review continuity and recovery provisions as part of CSV oversight.

3.12 Training and competency

3.12.1 All users of computerised systems must be appropriately trained and competent to perform their assigned tasks. Training must ensure that users understand system functionality, data-entry requirements, security responsibilities, and any study-specific procedures relevant to their role.

3.12.2 Training requirements must be role-appropriate and risk-proportionate. Where a user has already been trained and is demonstrably competent in the same system for another study, repeat training is not required unless system functionality, study-specific configuration, or user responsibilities differ.

3.12.3 All training must be documented and refreshed when significant system changes occur, when a user's role changes, or when a risk assessment identifies a need for additional training.

3.12.4 The Investigator is responsible for ensuring that site staff are adequately trained and that training records are maintained and available for review. For studies subject to a Combined Risk Assessment (GS002), the Sponsor may request evidence of training

during monitoring, audit, or inspection to confirm that system use is compliant and that staff competency is maintained.

3.13 Periodic review of systems

3.13.1 Computerised systems must undergo periodic review to confirm that they remain suitable for their intended purpose. Periodic review should consider system performance, access rights, audit trail functionality, validation status, and any changes in regulatory or organisational requirements. The frequency and scope of review must be proportionate to system risk. For studies subject to combined risk assessment (GS002), the Sponsor perform CSV spot-checks as part of ongoing oversight (QA002).

4 References and Related Documents

- GS002 Combined Risk Assessment
- QA010 Use of Computerised Systems in Research
- QA010-T01 Computer System Validation Checklist
- GS008 Processing Personal Information: Caldicott Approval & Information Governance Review.
- GS013 Location Feasibility
- GS005 Archiving Research Essential Records
- QA002 Audit Preparation, Conduct and Reporting
- QA009 Vendor Assessment
- CR013 CRF Design and Implementation
- CM004 Developing Monitoring and SDV Plans
- NHS Lothian Data Protection Policy
- NHS Scotland Confidentiality Code of Practice
- NHS Lothian Digital IT Security Policy
- The UK General Data Protection Regulation (retained EU Regulation 2016/679) and the Data Protection Act 2018 MHRA Guidance on GxP Data Integrity

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
3.0	08 JUL 2022	Reference to data protection legislation amended in sections 3.94 and 4. Change of author and approver.
4.0	04 MAR 2024	CSV Checklist (QA010-T01) moved from SOP GS002 (Combined Risk Assessment) to new SOP QA010 (Use of Computerised Systems in Research). Minor administrative changes. Change of author.
5.0	05 JUN 2026	Transfer to new ACCORD Policy template Updated to align with new Clinical Trial Regulations and ICH-GCP (R3). These changes reflect a major strengthening of CSV expectations and data integrity standards. Expanded requirements for eTMF/eISF systems, including audit trails, version control, long-term archiving, and governance expectations. Introduction of mandatory risk assessments for any non-validated electronic storage solution used for essential documents. Updated, proportionate validation expectations for off-the-shelf, configured, and bespoke systems. Strengthened change-management, QC, system security, backup, and disaster-recovery requirements. New expectations for periodic review of computerised systems, with Sponsor CSV spot-checks for GS002 studies.

6 Approvals

Sign	Date
 AUTHOR: Lorn Mackenzie, QA Manager, NHSL, ACCORD	21-May-2026
 Heather Charles (21-May-2026 14:44:08 GMT+1) APPROVED: Heather Charles, Head of Research Governance, NHSL, ACCORD	21-May-2026
 Gavin Robertson (21-May-2026 13:16:27 GMT+1) AUTHORISED: Gavin Robertson, QA Coordinator, NHSL, ACCORD	21-May-2026

POL007 Computer System Validation & Data Integrity v5.0

Final Audit Report 2026-05-21

Created:	2026-05-21 (British Summer Time)
By:	Roisin Ellis (v1relli8@exseed.ed.ac.uk)
Status:	Signed
Transaction ID:	CBJCHBCAABAAOChDUiW44uViCoEra30PsTyj8ex6e-GO

"POL007 Computer System Validation & Data Integrity v5.0" History

Document created by Roisin Ellis (v1relli8@exseed.ed.ac.uk)
2026-05-21 - 1:10:25 PM GMT+1- IP address: 62.253.82.244

Document emailed to Lorn Mackenzie (lorn.mackenzie@nhslothian.scot.nhs.uk) for signature
2026-05-21 - 1:11:22 PM GMT+1

Document emailed to heather.charles@nhslothian.scot.nhs.uk for signature
2026-05-21 - 1:11:22 PM GMT+1

Document emailed to Gavin Robertson (gavin.robertson@nhslothian.scot.nhs.uk) for signature
2026-05-21 - 1:11:23 PM GMT+1

Email viewed by Gavin Robertson (gavin.robertson@nhslothian.scot.nhs.uk)
2026-05-21 - 1:12:22 PM GMT+1- IP address: 90.240.128.160

Document e-signed by Gavin Robertson (gavin.robertson@nhslothian.scot.nhs.uk)
Signature Date: 2026-05-21 - 1:16:27 PM GMT+1 - Time Source: server- IP address: 90.240.128.160 - Signature Appearance Selected: DRAW

Email viewed by Lorn Mackenzie (lorn.mackenzie@nhslothian.scot.nhs.uk)
2026-05-21 - 1:42:05 PM GMT+1- IP address: 52.102.16.165

Document e-signed by Lorn Mackenzie (lorn.mackenzie@nhslothian.scot.nhs.uk)
Signature Date: 2026-05-21 - 1:42:17 PM GMT+1 - Time Source: server- IP address: 62.253.82.242 - Signature Appearance Selected: IMAGE

Email viewed by heather.charles@nhslothian.scot.nhs.uk
2026-05-21 - 2:43:51 PM GMT+1- IP address: 52.102.16.149

Signer heather.charles@nhslothian.scot.nhs.uk entered name at signing as Heather Charles

2026-05-21 - 2:44:06 PM GMT+1- IP address: 62.253.82.243

Document e-signed by Heather Charles (heather.charles@nhslothian.scot.nhs.uk)

Signature Date: 2026-05-21 - 2:44:08 PM GMT+1 - Time Source: server- IP address: 62.253.82.243 - Signature Appearance Selected: TYPE

Agreement completed.

2026-05-21 - 2:44:08 PM GMT+1