DIVISION OF RESEARCH AND INNOVATION

Document Number: GOSH/ICH/SOP/R/003	Version Number: 2
Title: Computer Systems Validation (CSV) for Systems used in Research	
Effective Date:	*Same as implement by date*

	Name	Position
Authored by:	Beth Reeves	R&D Clinical Trials Manager
Approved by:	Dr Vanshree Patel	R&D Head of Governance, Clinical Trials and Contracts

1. Scope

This SOP is applicable to

- All Great Ormond Street Hospital for Children (GOSH) or Institute of Child Health (ICH) staff who will be involved in the validation of computer systems used for research studies.

Further to the requirements listed in this SOP, personnel must also comply with:

- Any additional study-specific requirements mandated by the PI, Sponsor or R&D.

All computer systems used in clinical research studies, particularly those that impact on the quality of the source and/or study data and/or participant safety, should be validated. Retrospective validation may be required for legacy systems. Systems that are not used for research activities are not in the scope of this SOP (e.g. Microsoft Excel spreadsheet used to keep track of stationary order within the CRF).

2. Purpose

The purpose of this SOP is to provide an overview of the general validation principles to be applied when using a bespoke or a commercial off-the-shelf product for clinical research activities from a GCP compliance perspective. Computer System Validation (CSV) is essential to demonstrate that the system is fit for the intended purpose.

3. Definitions/Abbreviations

Clinical Research – As per UK Framework for Health and Social Care Research and HRA/MRC 'Is my study research?' tool.

Computer System Validation (CSV) – A process of establishing and documenting that the specified requirements of a computer system can be reliably and consistently fulfilled throughout the system's lifecycle.

System Administrator – Person with access rights to a system permitting activities such as data deletion, database amendment or system configuration changes. System administrator access should be restricted to the minimum number of people possible and should not be assigned to individuals with a direct interest in the data.

System Owner – Person who is responsible for a computer system throughout its lifecycle (this person is likely to also be the Information Asset Owner if applicable).

Audit Trail - information associated with actions that relate to the creation, modification or deletion of data in a system, facilitating the reconstruction of the history of such events.

4. Responsibilities

Duties may be delegated but the responsibility always remains with those listed.

4.1 For Trust wide systems used for research activities; the R&D office are responsible for working with the system owner to ensure the system is suitably validated for the research use.

4.2 For divisional or department systems used for research activities; the divisional or departmental quality representative (as applicable) is responsible for working with the system owner to ensure the systems are suitably validated for research use.

4.3 For study specific systems; the Sponsor is responsible for ensuring the systems are suitably validated for research use. The Sponsor may delegate the validation to the CI.

4.4 For study specific systems additional validation may be required to demonstrate that the system is fit for purpose on site (e.g. is compatible with the sites software and/or hardware); the PI is responsible for ensuring any such validation is completed.

5. Procedure

There should be validation of the development or installation of the computer system itself (this may be done by a third party such as ICT if the system is not research specific), and also validation of any research and/or study specific configuration, builds, applications and/or programming undertaken subsequently using the validated system. These are undertaken together to demonstrate that the system (and its use for research or a study) are 'fit for purpose'; including that:

- The system conforms to the requirements for completeness, accuracy, reliability, and consistent intended performance established in the validation plan.
- The integrity of the data (including any metadata that describe the attributes of other data and provide context and meaning) are ensured.
- Data changes are documented and there is no deletion of entered data (i.e., maintain an audit trail, data trail, edit trail).
- There is controlled access to the system and a list of authorised users.
- The signature process associated with a system (if applicable) is equivalent to a wet ink signature and control over signed records is maintained.
- There is an adequate back-up.
- Study blinding (if applicable) is safeguarded, (e.g., maintain the blinding during data entry and processing).

The system may need to be tested on more than one device and/or by more than one user to ensure consistency. The validation should cover the whole life-cycle of the system (set up, use, upgrades/amendments and decommissioning/transfer to a new system) as well as quality assurance measures and operational controls (e.g. data retention, back up, security, audit trails, interface with other systems, access rights, and staff training). Validation (or re-validation and/or additional validation in the case of upgrades or system changes) should ideally be completed before the system is in use. If this is not possible it must be completed as soon as possible.

Validation of a system will comprise five sections.

- Risk Assessment
- Validation Plan
- Validation Test Sheets and Report
- Procedures/Instructions
- Change Control

5.1 Risk Assessment

The necessary level of validation of a system is dependent upon the intended use of the system, the potential of the system to affect participant protection and reliability of study results, and the system configurability.

A risk assessment must be completed to determine the level of validation required. The risk assessment template (TMP/R/006) should be used. Risk assessment documentation must be retained in accordance with the Archiving SOP.

5.2 Validation Plan

A validation plan will be developed as deemed necessary by the initial risk assessment. The validation plan will define the system requirements and the functions to be tested. The validation plan template (TMP/R/007) should be used. Validation documentation must be retained in accordance with the Archiving SOP.

5.3 Validation Test Sheets and Report

Tests of major functions listed in the validation plan must be carried out and recorded. The test sheet template (TMP/R/008) should be used.

The validation report is produced to summarise the validation results. The validation report template (TMP/R/009) should be used.

Validation documentation must be retained in accordance with the Archiving SOP.

5.4 Procedures/Instructions

Following validation the system owner should work with the relevant quality lead to ensure that there are adequate processes developed to cover system setup, installation, use, maintenance and decommissioning. Such procedures should be based on the validation report (including mitigations for any system limitations) and written using the Written Procedure Template (TMP/R/001).

The procedure(s) should describe data collection and handling, maintenance, security measures and access, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the people involved (such as system owner, administrator(s) and user(s) should be clear, and the users should be provided with appropriate training.

5.5 Change Control

Once the system has been validated; there should be a mechanism in place for version control of the validated system and a formal process to manage any changes to the system, or its use, to ensure the validated state is maintained.

The change control documentation should include:

- Change request (submitted to system owner) (TMP/R/010 or equivalent)
- Change assessment (TMP/R/011)
- Updated risk assessment (if applicable)
- New validation plan detailing level of re- validation or additional validation necessary.
- New validation testing and report of re- validation or additional validation (as required by the validation plan)

Documentation (including any superseded versions) must be retained in accordance with the Archiving SOP.

6. Related Documents

- SOP: Archiving
- GOSH/ICH/TMP/R/006: CSV Risk Assessment Template
- GOSH/ICH/TMP/R/007: CSV Validation Plan Template
- GOSH/ICH/TMP/R/008: CSV Testing Sheet Template
- GOSH/ICH/TMP/R/009: CSV Validation Report Template
- GOSH/ICH/TMP/R/001: Written Procedure Template
- GOSH/ICH/TMP/R/010: CSV Change Control Template
- GOSH/ICH/TMP/R/011: CSV Change Assessment Template

7. References

- MHRA Good Clinical Practice Guide (Grey Guide) – Chapter 14
- The Medicines for Human Use (Clinical Trials) Regulations
- GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems
- INS-GCP-3 Guidance for the conduct of GCP Inspections Annex III
- MHRA 'GXP' Data Integrity Guidance and Definitions