TAYSIDE MEDICAL SCIENCE CENTRE POLICY

CLINICAL RESEARCH COMPUTER SYSTEM VALIDATION

POLICY NUMBER:	TASC POLICY 009 v4
AUTHOR:	Marcus Achison
EFFECTIVE DATE:	24 Sept 2024
REVIEW DATE:	24 Sept 2026

1. Introduction

This policy outlines the design, development, validation, functional testing, User Acceptance Testing (UAT), maintenance and security of computerised systems used for data collection and handling in clinical research. Examples of such systems include clinical trials data capture systems, randomisation systems, statistical packages and laboratory analysers. The process of establishing documented evidence that a computerised system will consistently perform as intended is known as computer system validation.

2. Scope

This policy applies to all staff involved in the creation and validation of computer systems used in clinical research studies sponsored by University of Dundee (UoD) and/or NHS Tayside (NHST).

This policy should be read in conjunction with TASC Data Management SOPs.

3. Research Data and Computerised Systems

Research data should be collected, recorded and managed in accordance with current Data Protection Legislation and UoD and NHST policies. In addition, data for all trials involving the participation of human subjects must be handled according to the principles of Good Clinical Practice (GCP). It should be noted that achieving GCP standards is a legal requirement for Clinical Trials of Investigational Medicinal Products (CTIMPs).

Computerised systems used for the capture, processing, manipulation, reporting and storage of data should be developed, validated and maintained in a manner which ensures the validity, integrity and security of the data.

Computerised systems may be:
i) Bespoke.

ii) Multifunctional software packages which are not specifically designed for clinical trials, but which can be customised to do so with some caveats, e.g. Microsoft Excel (refer to relevant TASC SOP).

iii) Off-the-shelf packages which are specifically designed to collect clinical trial data and which require trial-specific configuration, e.g. Castor EDC (refer to relevant TASC SOP).
Research staff should follow UoD and NHST procurement procedures before purchase of software packages and the CI should contact TASC Legal to prepare an appropriate collaboration or service agreement if any of these activities are outsourced to a third party.

The level of software validation required will be dependent upon the system and nature thereof, e.g. bespoke systems will require more comprehensive validation than generic off-the-shelf packages since they will have been validated prior to release for sale, e.g. Excel. However, the trial-specific configuration will require validation along with confirmation that it meets the required specification.

4. System User Requirement Specification (URS)

A URS should be prepared for the intended system and should describe the requirements of the end user. The URS should include risk-based consideration regarding the intended use of the system and its potential to affect human subjects and/or the reliability of results. Typical requirements for a URS may include:

- Functionality
- Interface
- Performance
- Security
- Maintenance
- Regulatory
- Data migration

5. System installation and validation

5.1 Installation

Core system installation for hardware and software packages should be documented and carried out by specialist IT personnel. Web-based systems require compatibility with internet browsers.

5.2 Validation

Validation of the core system must be carried out according to a Validation Plan and documented.

5.3 Functional Testing and UAT of trial-specific configuration

Prior to use, the trial-specific configuration of the computerised system must undergo documented functional testing and UAT to demonstrate that it is fit for purpose and performs consistently for the intended purpose as per the URS. Test results must be documented along with a summary report.

The "Go Live" date and version numbers for any computerised system must be recorded.

6. Data Collection and Handling

6.1 The collecting, processing, reviewing, reporting and archiving of data must be carried out in a traceable manner from start to finish of the trial, with a record of who carried out each procedure.

6.2 There must be no deletion or over writing of data. Data changes must be documented (by audit or edit trail) to confirm the integrity of data after any modifications.

6.3 Regular, routine quality control checks and reviews of the data must be carried out as required and documented.

6.4 Image acquisition systems that have in-built data capture and storage (e.g. ECHO machines) should be maintained by regular servicing to ensure accuracy of measurements.

7. System and data security

7.1 Server security

Servers holding data for clinical studies must be located in secure data centres where physical access is restricted to authorised personnel. The server room should be temperature controlled, have an Uninterruptible Power Supply (UPS) and fire protection measures in place. Each computerised system should have documentation to explain where its corresponding server is situated and who is responsible for its maintenance.

7.2 Data security

All persons dealing with personal data are responsible for ensuring the security and safety of these data. Data used for analysis must be anonymised.

Systems used for entry of, storage of and access to study data must have up-to-date operating system patches installed together with appropriate security software (e.g. antivirus, anti-spyware and firewall).

Access to data must be limited to authorised personnel and each user must have an individual login account. Accounts must never be shared and users should not log in to provide access to another user. There may be role-dependant access rights granted to other personnel, e.g. study monitors, auditors or regulatory inspectors who need access.

Workstations must not be left unattended without locking the desktop computer first.

8. Back-up and Disaster Recovery

Electronic data must be stored on devices that are backed up in a secure and timely manner. Data shall be backed up to remote and/or removable disk storage, the latter of which should be locked in a secure fire safe cabinet. The process of restoring from back-up should be tested

periodically and results recorded. Specialist IT assistance may be required to enable successful back-ups.

9. Change Control

Guidelines for a Change Control Management procedure must be written for each computerised system as applicable. If there are any changes to the computerised system or its study - specific configuration after release (i.e. to correct an error or a modification to functionality), the changes must be validated and documented with version control in place. The reason why study-specific changes are required and approval to make the changes to the system should be documented.

DOCUMENT HISTORY

History prior to 2021 is in the archived Policies available from TASC Quality Assurance Dept.

Version Number:	**Reviewed By (Job Title):**	**Effective Date:**	**Details of editions made:**
3	Marcus Achison (TCTU Database Manager)	24/09/2022	Change of author.
4	Marcus Achison (TCTU Database Manager)	24/09/2024	Reference to OpenClinica in 3(iii) removed as OC is no longer used.

APPROVALS

Approved by:	**Date:**
Professor Linda Martindale, Dean, School of Health Sciences, University of Dundee, on behalf of TASC Research Governance and Oversight Committee	17 Sept 2024
Approved by:	**Date:**
Professor Russell Petty, R&D Director, NHS Tayside	16 Sept 2024