SECURITY AND AUDITING CONFIGURATION FOR CLINICAL RESEARCH COMPUTER SYSTEMS

SOP Number: BTC-SOP-IT-002

SOP Version: 2.0

Click here to record your training for this SOP

	NAME	TITLE
Authors	David Carmichael Jana Kirwan	Research Systems Technical Developer Research Systems Technical Manager
Reviewers	Rachael Heys	Quality Assurance Manager
Authoriser*	Melanie Lewcock	Head of BTC Strategy

Release Date:	05/03/2024	**Implementation Date:**	05/04/2024

Review Due:	05/04/2026

Implementation plan

This Standard Operating Procedure (SOP) should be implemented within two weeks from Release Date for studies that are being set up.

For ongoing studies applicable sections of this SOP should be implemented as far as possible immediately after the implementation date, unless impractical for the circumstances e.g. too close to the end of study.

If unsure, the BTC Director and/or Quality Assurance Manager should advise.

Note to User:

It is your responsibility to ensure that you are using the latest approved version of this SOP. Please note that versions may be superseded before their planned review date.

THIS IS AN UNCONTROLLED VERSION WHEN PRINTED.

If you are reading this document in printed form, please check that the version number and date match the most recent SOP's details. Current versions of all Bristol Trials Centre (BTC) SOPs and accompanying documents are available on the BTC Teams QA channel.

Contents

1. INTRODUCTION and PURPOSE 3
2. SCOPE 3
3. DEFINITIONS 3
4. RESPONSIBILITIES 4
   4.1 Research Systems Technical Developer 4
   4.2 BTC Staff 4
   4.3 SOP author(s) or delegate 4
   4.4 SOP user 4
5. SPECIFIC PROCEDURES 5
   5.1 Security 5
   5.2 Auditing 6
6. SUPPORTING DOCUMENTS TO BE USED 6
7. CHANGE HISTORY 6

1. INTRODUCTION AND PURPOSE

As outlined in the International Conference on Harmonisation (ICH) E6 Good Clinical Practice (GCP) guidelines a system should "*maintain an audit trail, data trail, edit trail*" and "*maintain a security system that prevents unauthorised access to the data*".

GCP regulates specific requirements for computerised systems, specifically in Section 5.5.3: "when using electronic trial data handling and/or remote electronic trial data systems:

a) Ensure and document that the electronic data processing system(s) conforms to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e. validation).

b) Maintain SOPs for using these systems.

c) Ensure that the systems are designed to permit data changes in such a way that the data changes are documented, and that there is no deletion of entered data (i.e. maintain an audit trail, data trail, edit trail).

d) Maintain a security system that prevents unauthorised access to the data.

e) Maintain a list of the individuals who are authorised to make data changes.

f) Maintain adequate backup of the data.

g) Safeguard the blinding, if any (e.g. maintain the blinding during data entry and processing)."

The purpose of this SOP is to describe the standard procedures undertaken for ensuring adequate security and auditing measures are in place for all software and hardware systems which fall under the direct responsibility of the BTC for the explicit purpose of the capture, processing or reporting of clinical study data, in accordance with the requirements stated above.

2. SCOPE

This SOP describes the processes and steps required to ensure secure and audited software and hardware systems are in place for use within the BTC. It defines the security and auditing requirements for software and hardware systems used within the BTC for the purposes of collecting, storing or processing clinical study data.

This SOP is not expected to apply to any software or hardware systems outside of this remit, or any systems or components thereof which fall outside the direct responsibility of the BTC, for instance, systems configured and maintained by the University of Bristol or the UHBW.

The Chief Investigator (CI) must be made aware of this SOP and as a minimum, be signposted to the SOP by BTC.

NB: Throughout this document the terms 'research', 'trial', and 'study' will be used interchangeably to denote those projects which fall under the remit of the UK Policy Framework for Health and Social Care Research 2017.

3. DEFINITIONS

For definitions, acronyms and abbreviations relevant to IT please refer to the BTC-RES-IT-001 Definitions and Acronyms (IT) available on the BTC Teams QA channel. For all other definitions, acronyms and common abbreviations relevant to research projects and general management of

research refer to the BTC-RES-TM-001 Definitions and Acronyms, also available on the BTC Teams QA channel.

4. RESPONSIBILITIES

Any delegation of responsibilities should be formally agreed by all parties and clearly documented.

4.1 Research Systems Technical Developer

It is the responsibility of the Research Systems Technical Developer to:

- Implement adequate security and auditing mechanisms for software developed in-house
- Implement appropriate configuration of any software or hardware which falls within the scope of this document as defined above.

4.2 BTC Staff

It is the responsibility of all BTC Staff to:

- Adhere to any relevant BTC System specific procedures in addition to both University of Bristol and relevant NHS Trusts (e.g. University Hospitals Bristol and Weston NHS Foundation Trust (UHBW), North Bristol NHS Trust (NBT)) policies and general best practice guidelines when using software and hardware hosted by these organisations for work related activities. This includes:
    - ensuring passwords are of adequate complexity and are kept secure and not shared with colleagues;
    - informing the Research Systems Technical Developer where issues regarding security or auditing become evident;
    - applying caution when installing third party software and understanding such software may cause conflict with BTC systems.

4.3 SOP author(s) or delegate

It is the responsibility of the SOP author(s) (or an appropriately qualified/trained delegate) to:

- Generate, finalise and revise the SOP in accordance with the BTC-SOP-QM-001 Development and Management of SOPs.
- Ensure that the SOP remains fit for purpose.
- Provide relevant training and education materials to ensure that staff are aware of their responsibilities in relation to SOP content and management.

4.4 SOP user

It is the responsibility of the SOP user to:

- Ensure compliance with this document.
- Review procedures during use of the SOP and inform the QA manager of any changes required using the Change Request log on the BTC Teams QA channel.
- Undertake training on all aspects of this SOP and record training on the BTC Teams QA channel.

5. SPECIFIC PROCEDURES

5.1 Security

The Research Systems Technical Developer will follow the steps detailed below in order to ensure both the confidentiality and integrity of clinical study data collected, stored or processed on BTC systems.

a) For systems collecting and processing clinical study data an appropriate authentication and authorisation scheme must be available in both in-house developments and applications sourced from a third party. Such schemes must allow the assignment of appropriate rights to individual user accounts.

b) Only users authorised by an appropriate representative within the study team will be granted access to systems or data for use with the associated clinical study. Users and their individual access rights should correspond to the user role and their tasks as defined within the related study delegation log, where applicable.

c) Where applicable, an appropriate password policy must be maintained and enforced to protect any system storing or processing clinical study data. This policy will enforce 'best practice' password guidelines, such as minimum password length and password complexity. In certain cases this policy will be set by another organisation rather than within the BTC.

d) An ethos of 'least privilege' will be adopted, ensuring any access rights granted to a user of a clinical study system or associated data is the minimum they need to perform a task and no more.

e) Where data is extracted from a clinical study system for the purposes of reporting or analysis such data will exclude patient identifiable data unless such data are needed to complete the task. Where extracted data does contain patient identifiable or other sensitive information it must be stored in a secure location, subject to conditions in point b.

f) In order to protect sensitive clinical data an appropriate encryption mechanism must be used, where appropriate, when transmitting data across a computer network.

g) Security tools will be installed and appropriately configured on database and web-servers, such tools must include at a minimum Anti-virus and Firewall components.

h) Servers must be configured appropriately only for the role(s) they were commissioned for in order to reduce their vulnerability to intrusion. This configuration will be performed with reference to best practice guides for the system in question.

i) Patches and updates addressing security vulnerabilities will be applied as soon as reasonably practicable and at a suitable time to minimise disruption to the system.

j) Software Engineering and Code Security best practices must be observed during the development of clinical study systems in order to reduce the likelihood of malicious exploitation of potential security vulnerabilities.

k) Hardware systems which are used to store and process clinical study data must be physically protected in order to ensure that only authorized people have physical access to these systems. Hardware will be sited within a locked room, or if such a location is unavailable, secured within a lockable rack cabinet. Access to this room or cabinet must be made available only to designated members of staff with a legitimate reason to access areas containing these hardware systems.

5.2 Auditing

Software systems collecting and processing clinical study data, either bespoke developments or sourced from a third party, are expected to have comprehensive auditing mechanisms in place in order to track changes to data which occur within that application.

The level of auditing functionality required will depend on the nature of the study. A risk assessment should be carried out to determine the correct level of auditing required and should be documented in the database functional specification.

For any trial, auditing must capture any changes to data i.e. the insertion, editing or deletion of data will be recorded. Audited data must also include who was responsible for the change, when the change occurred and the value of the data item prior to the change.

The risk assessment will determine if the following auditing functionality is also required:

- Recording the reason for data changed. This could be for all data items or for a specified subset of data items.
- Enforcing that any data changes must be approved by the investigator or user with assigned privileges. This could be for all data items or for a specified subset of data items.
- Recording the history of any changes made prior to the form being saved. This is most likely to be required for CTIMPs where electronic case report forms (eCRFs) are the primary source of data and the data is not first collected on a paper CRF.

Software systems employed only for the reporting or analysis of clinical study data, such as statistical packages, Microsoft Access etc, do not require such an auditing mechanism, as the original source data held in the database cannot be altered via these systems.

6. SUPPORTING DOCUMENTS TO BE USED

Number	Title
BTC-RES-IT-001	Definitions and Acronyms (IT)
BTC-RES-IT-002	Website References – IT SOPs
BTC-RES-TM-001	Definitions, acronyms and abbreviations relevant to research projects and management of research
BTC-SOP-QM-001	Development and Management of SOPs

7. CHANGE HISTORY

Previous version and date	New version and date	Summary of review
NIL		New document
V1, 28 Jul 2021	No change	SOP was reviewed and required no change; review date was amended but the SOP version number and date were not changed
V1, 28 Jul 2021	V2, 05 03 2024	Updates to roles and general grammatical corrections.