Queen Mary
University of London

Barts Health NHS
NHS Trust

Standard Operating Procedures (SOP) for:
Use of computerised equipment, software and systems in clinical research

SOP Number:	***38a***	Version Number:	***1.0***
Effective Date:	***21/3/16***	Review Date:	***21/8/17***

Author:	**Marie-Claire Rickard, GCP and Governance Manager**
Reviewer:	**Rachel Fay, GCP and Governance Manager**
Reviewer :	**Elizabeth Clough, Research Governance Operations Manager**

Authorisation:	
Name / Position	**Sally Burtles, Director of Research Services & Business Development**
Signature	Sally Burtles
Date	**15/3/16**

Purpose and Objective:

The EU Directive 2001/20/EC [4], EU Directive 2005/28/EC [5] and Annex 11 [6] defines the GCP technical requirements for data management including the necessity for computer systems to have data privacy, security system, and system descriptions. The Good Clinical Practice guide states that all computer systems used in clinical trials, in particular those that impact on the quality of the trial data and subject safety should be validated. Computer systems in clinical trials are typically used to control a process, process or store trial data.

The purpose of this SOP is to outline the overarching sponsor requirements for use of computer equipment and systems within its sponsored research projects (see scope). This includes: identifying and risk assessing which computer equipment, systems and software can be used in CTIMPs, which need validation and their oversight. There is separate and specific guidance on CTIMP *database* system validation (please see SOP 38b - Trial Data Management Systems including case report form (CRF) guidance and user acceptance testing and QC-sign-off processes). The objective of this SOP is to look beyond the trial database to ensure that computer systems used in CTIMPs are fit for purpose, such as those used by departments that support research, i.e. imaging departments and labs, subcontractors and research sites, as well as systems used by research teams. This is to ensure that all computer systems used in BH and QMUL sponsored CTIMPs consistently perform as intended in their operational environment, along with the trial database (as outlined in SOP 38b - Trial Data Management Systems) as part of holistic trial data integrity.

This SOP's objective is to ensure that all computerised systems used in BH and QMUL sponsored CTIMPs have been identified by the CI as part of site activation, not just the trial database. This includes guidance on the CI's oversight and awareness of computer systems, their risk assessment, documentation, and the validation required at site activation (for further information see SOP 46 – Site Selection, Initiation and Activation).

This SOP is a guide for Chief Investigators (CIs) and their research teams so that they can ensure that computer systems are fit for purpose during the CTIMPs data lifecycle. This SOP also provides a framework for researchers to assess which computer systems could impact upon trial data and patient safety and therefore will need a robust validation process.

For the purpose of this SOP 'CTIMPs' means all regulated clinical trials including: CTIMPs, ATMP and Clinical Trials of non-CE marked devices

Scope:

This SOP is relevant to all researchers who work on Queen Mary University of London (QMUL) and Barts Health NHS Trust (BH) sponsored CTIMPs, BH and QMUL support departments and their staff, service providers, central facilities and research sites that have computer systems that manage data of BH or QMUL sponsored CTIMPs. This includes computer systems such as laboratory IT systems, image analysis software etc. as well as delegated members of research teams that are involved in CTIMPs.

The scope of this SOP applies to all computer systems used in BH/QMUL sponsored Clinical Trials of Medicinal Products (CTIMPs), Advanced Therapy Medicinal Products (ATMPs), Clinical Trials of non-CE marked Medical

Devices. This SOP particularly applies to computer systems that impact on the quality of the trial data and subject safety. The principles of this SOP are considered best practice but are not mandatory for non-CTIMPs and CTIMPs that are hosted at BH.

Abbreviations:

BH	Barts Health NHS Trust
JRMO	Joint Research Management Office
QMUL	Queen Mary University of London
CTIMP	Clinical Trial of a Medicinal Product
ATMP	Advanced Therapy Medicinal Products

Definitions *(if needed)*

Data Integrity: The extent to which the data is maintained, complete, consistent and accurate throughout the data lifecycle.

Data Lifecycle: All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, retention, archiving / retrieval and destruction.

Data Governance: All of the arrangements to ensure that data, irrespective of the format in which it is generated, is recorded processed and retained and used to ensure a complete, consistent and accurate record through the data lifecycle. This includes the processes and systems (including computer systems validation), ownership, monitoring and audit, environment and training.

Computer system validation (CSV): Is the process of establishing documented evidence that a computerised system will consistently perform as intended in its operational environment.

Relevant SOP s

SOP 11A - BH/QMUL Sponsorship of CTIMPs, ATMPs and Clinical Trials of non-CE marked Medicinal Devices – Process for Researchers
SOP 11B - BH/QMUL Sponsorship of CTIMPs, ATMPs and Clinical Trials of non-CE marked Medicinal Devices – For JRMO Staff Sponsor
SOP 38b - Trials data management systems and associated documents
SOP 40 - Vendor Assessment
SOP 46 - Site Selection, Initiation and Activation

SOP Text

	Responsibility	Activity
1.	Chief Investigator	**At the protocol design stage the CI should ensure that all computerised systems that will be used for the CTIMP are identified, risk assessed and validated where appropriate.** The CI and team should identify the computerised systems they will be using in their CTIMPs either within the protocol or in a data management SOP/plan and ensure Sponsor authorisation. These may include but are not limited to: • Pharmacovigilance systems • eCRF systems • Databases (including electronic edit checks, statistical analysis) • Electronic data transfer (e.g. laboratory data or Imaging data to a central database) • Randomisation systems • Unblinding systems • IMP Management systems • Specialist imaging software (e.g. cameras, scanners of all types) • Data input devices i.e. apps, electronic prescribing systems that may be stand alone. • Laboratory computer systems. These computer systems must be declared by the GCP Manager as part of the 'greenlight to activate sites' process. (See SOP 11A- Sponsorship of CTIMPs – Researchers Guide) CIs should note that software and web applications may be considered a clinical

		device and should seek advice regarding their use in trials with the GCP Manager and the BH clinical physics department (see JRMO website for contact details) for a risk assessment.
2.	Chief Investigator	**At the protocol design stage the CI should ensure that all computerised systems that will be used for the CTIMP are identified, risk assessed and validated where appropriate.** The CI and team should identify the computerised systems they will be using in their CTIMPs either within the protocol or in a data management SOP/plan and ensure Sponsor authorisation. These may include but are not limited to: • Pharmacovigilance systems • eCRF systems • Databases (including electronic edit checks, statistical analysis) • Electronic data transfer (e.g. laboratory data or Imaging data to a central database) • Randomisation systems • Unblinding systems • IMP Management systems • Specialist imaging software (e.g. cameras, scanners of all types) • Data input devices i.e. apps, electronic prescribing systems that may be stand alone. • Laboratory computer systems**.** These computer systems must be declared by the GCP Manager as part of the 'greenlight to activate sites' process. (See SOP 11A- Sponsorship of CTIMPs – Researchers Guide) CIs should note that software and web applications may be considered a clinical device and should seek advice regarding their use in trials with the GCP Manager and the BH clinical physics department (see JRMO website for contact details) for a risk assessment.
3.	Chief Investigator	**Ensure that there is oversight of all Computer Systems used in the trial** Computer systems used in research come in various guises but include: Cloud storage, IT programs, computer synchronisation process, IT interfaces between computer systems, and IT infrastructures/platforms/software as a service. These could be 'off the shelf' i.e. purchased through NHS or QMUL procurement processes, customised for the trial or bespoke to the trial or provided centrally. When used in a CTIMP, each computerised systems needs to be assessed as below.
4.	Chief Investigator	**For CTIMPs, ATMPs and MHRA regulated Medical Devices** Selection of CTIMP trial databases: Microsoft Excel and Access database are not permitted by the JRMO as Sponsor (see point 9 for guidance on non-CTIMP databases and SOP 38b – Trials data management systems). All other computerised systems should be assessed and deemed fit for purpose. This should be achieved by validation and testing. All aspects of this process should be documented but must include: • Specifications • Testing against specifications (traceability – is the data accurate, reliable, have integrity, available and authentic) • Approval and release of the computer system • Change control See SOP 38b – Trials data management systems and associated documents for guidance and templates.

5.	Chief Investigator	**Consider and document the risk of each computer system.** • The CI should ensure that appropriate controls are in place to support and safeguard their data at all stages in the data lifecycle. This includes when delegating or subcontracting aspects of their trial management to other parties i.e. departments, labs, central facilities and sites. • Ensure that departments and organisations have systems in place that are designed to provide an acceptable state of control of the data, based upon the data integrity risk of the computer system. • The CI should consider that the governance and control of the computer system is commensurate with the significance of the computer system to the data integrity. • Where a computer system is critical to the data integrity and patient safety, ensure that the resource and governance of the computer system is robust before the computer system is used. • The risk assessment of the computer system should be documented.
6.	Chief Investigator	**The computer systems used in research must be 'fit for purpose' i.e. validated (ICH GCP 5.5.3 [a])** To ensure research data integrity, computer systems need to be validated and processes put in place to ensure quality of the data. The computer systems need to be reviewed to ensure that they are trustworthy and reliable. Therefore, all Chief Investigators should note that a computer systems vendor is likely to have performed 'functional verification and activities.' Therefore, it is the CI's responsibility to ensure that the purchased system has demonstrated its fitness for its intended use. This should include performance, configuration, SOPs and staff training. **Minimum requirements for outsourced computer systems** Vendor assessment should be performed for all computerised system providers that are either unknown or a preferred supplier to the Sponsor and key stakeholders. Please see and follow SOP 40 – Vendor Assessments for vendor assessment definitions and procedures. **See SOP 40 - Vendor assessment and SOP 38b – Trials data management systems for further guidance.**
7.	Chief Investigator	**Computer System Assessment at each Research Site and Subcontractor or Service Provider:** As part of site selection and feasibility (see SOP 46 – Site Selection, Initiation and Activation for further guidance) the CI and team must clearly identify and document each research site's computerised systems which will be utilised during the study. Request the PI to provide details of local computer systems. Examples of which local computerised systems need to be identified can be found in Appendix A – section 2. Once the details of the local computer systems have been collected the CI should assess whether the systems can be used within the trial. The decision whether or not the local site computer system can be used, or whether it will be used as source data should be documented as part of site activation. Particular attention should be paid to pharmacy electronic prescribing system, systems used to transfer data/images between sites or locations and electronic health record/patient record systems. The CI must ensure that the PI or subcontractor has provided evidence that their local computer systems have been validated and that they are fit for purpose. This process of scoping and assessing local computer systems should be made before site activation or before sending CTIMP work to a sub-contractor i.e. lab or central imaging centre. Systems used for standard clinical care within NHS sites can be deemed as low

		risk and trustworthy. However a minimal amount of information should still be collected i.e. name of the computer system and department/key worker responsible for their governance and maintenance.
8.	PI	**Computer Systems used to transfer data should be tested and validated, for example computer systems that transfer scans between sites.** Any system being used to transfer data or images must be tested prior to its use e.g. transfer of de-identified images for central review. This testing must be part of site initiation, see SOP 46 – Site Selection, Initiation and Activation. Any identifiable data must be encrypted before transfer.
9.	Chief Investigator	**For Non CTIMPs** This SOP should apply in a proportionate manner to non-CTIMPs, based upon the type and size of a study. An assessment of the computer systems should be performed and documented by the CI considering: • Size of study • Type of study (interventional, questionnaire) • What the data will be used for (publication, changing practice, student project). • Risk a computer system has to patient safety and data integrity • Risk to project of low level audit trail and data management Where deemed appropriate and the risks to the data integrity have been risk assessed by the CI, Microsoft Excel and Access may be used for non-CTIMP studies.

Change Control

Not Applicable New SOP.

List of appendices *(this is embedded text such as template wording)*

	Appendix name
Appendix A	**CTIMP Computer Systems Survey, including Support Department i.e. imaging departments/labs/pharmacy/ subcontractors/research sites**
Appendix B	**Process Flow chart**

Appendix A

CTIMP Computer Systems Survey, including Support Department i.e. imaging departments/labs/pharmacy/ subcontractors/research sites

1. Introduction: Purpose of this document, scope, created by, additional information
To identify, risk assess and document which computer systems need to have systems validation. (See SOP 38b – Trials data management systems associated docs for validation templates and guidance)
List here: sites, support departments, teams, subcontractors, service providers who have computer systems that may impact on CTIMP data integrity or patient safety

2. Details of the Computer System
    - What software/app/computer system are being used? Consider imaging departments, pharmacy, support department, Health records.
    - Are the computer systems critical for the assurance of patient safety, data integrity or for the CTIMP end points?
    - Is it used to transfer data between sites? What process is in place to assure participants' data protection (i.e. anonymisation of data)?
    - If an external party i.e. subcontractor or lab, how have they assured GCP compliance of the computer system as part of the subcontract?

- Who purchased the computer system/equipment/software/app and for what purpose?
- Is it an NHS computer system used in clinical practice? (If so it is deemed low risk but oversight is still required).
- If not purchased for this CTIMP, is it fit for purpose? Does it need to be tested against a specification?
- What version?
- How is the computer system hosted? I.e. is the system on a secure network?
- Who is the custodian of the computer system?
- When was the computer system implemented?
- Are there any relevant policies, manuals or SOPs for the computer system?
- If the system is maintained by BH or QMUL IT, who is responsible for the system? Include what network it is on where servers, Reference to ICT SOP

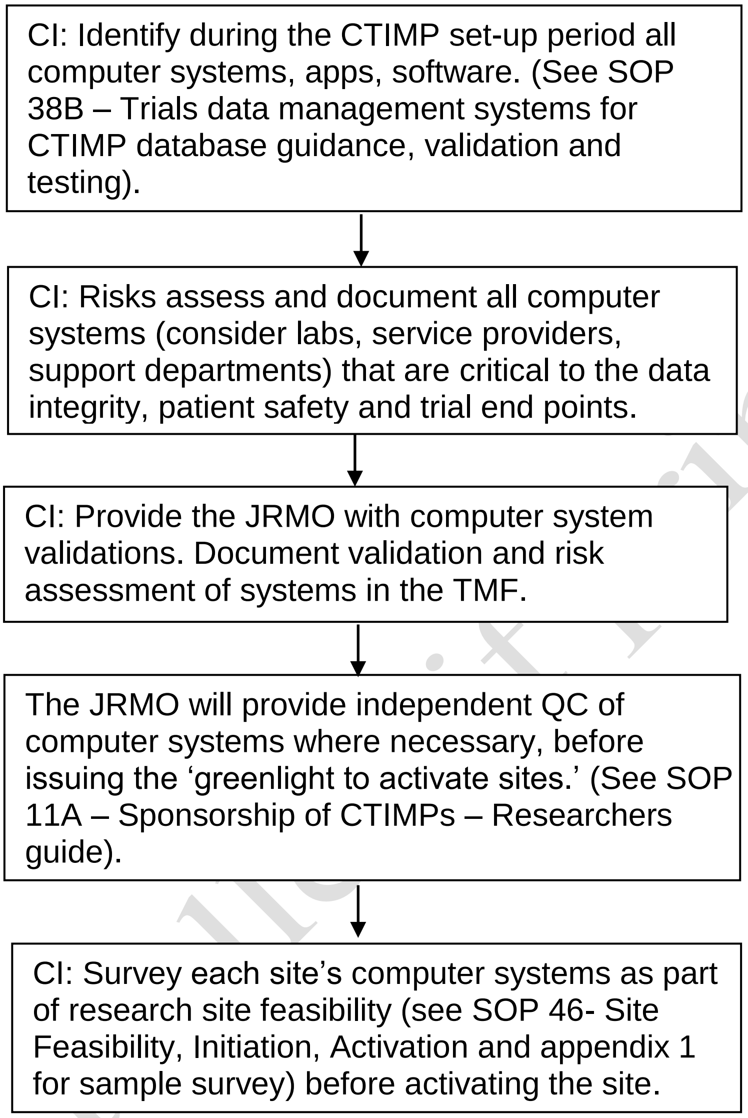
3. Security of system
   - Who has access to the computer system?
   - Detail the process of how is access is granted? I.e. username and passwords?
   - Who allocates roles?

4. Training evidence for computer system users
   - How are personnel trained in the computer system?
   - How is this training documented and where are user training records kept?

5. Access to the Computer System by Regulators
   - Will Clinical Trial Monitors/Auditors/Inspectors have access to the computer system? If yes, what should be done to enable this? (Consider patient healthcare records that need to be monitored as source data).
   - Will Clinical Trial Monitors/Auditors/Inspectors only have access Trial specific patient records?
   - Is there a clear process for gaining and using the computer systems for Clinical Trial Monitors/Auditors/Inspectors? I.e. a manual to use once on site?
   - Who arranges access to the computer systems? (Name and contact details)

6. Backup systems for Clinical Records System (CRS), disaster recovery- IT SOPS/policies
   - Provide details of the back-up systems, including frequency (SOP, manual, policy)
   - Provide details of the disaster recovery process (SOP, manual, policy)
7. Computer System Audit trails
   - Description on included?
   - Who is in control
   - Who can see it?
8. Computer System Approval Process
   - What is the approval / authorisation process? I.e. what do authorisation signatures confirm has been done?
9. Computer System validation
   - Has the computer system been validated and tested?
   - The CI will need to be supplied with documentation of the validation and testing.
   - Who validated the software? Software provider details.
   - Or was it validated by the research site/service provider/department?
10. Change control systems
    - What systems are in place for governing any change to the computer system? (SOP, manual, policy)
    - Who is responsible for change control authorisation/QC?
11. Archiving:
    - How long is clinical trial data kept for archiving?
    - Where is the data archived?
    - What is the process for archiving the data?
    - Who is the archivist (name and role) responsible for archival of the computer system?

Appendix B Process Flow Chart



CI: Identify during the CTIMP set-up period all computer systems, apps, software. (See SOP 38B – Trials data management systems for CTIMP database guidance, validation and testing).

CI: Risks assess and document all computer systems (consider labs, service providers, support departments) that are critical to the data integrity, patient safety and trial end points.

CI: Provide the JRMO with computer system validations. Document validation and risk assessment of systems in the TMF.

The JRMO will provide independent QC of computer systems where necessary, before issuing the ‘greenlight to activate sites.’ (See SOP 11A – Sponsorship of CTIMPs – Researchers guide).

CI: Survey each site’s computer systems as part of research site feasibility (see SOP 46- Site Feasibility, Initiation, Activation and appendix 1 for sample survey) before activating the site.