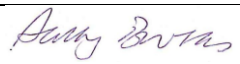
Standard Operating Procedures (SOP) for:			
Trial Data Management Systems			
SOP Number:	***38b***	Version Number:	***4.0***
Effective Date:	***16/5/16***	Review Date:	***16/5/18***

Author:	**Nick Allison, Data Systems Officer**
Author:	**Rachel Fay, Research Governance and GCP Manager**
Reviewer:	**M. Rickard, Research Governance and GCP Manager**

Authorisation:	
Name / Position:	**Sally Burtles, Director of Research Services and Business Development**
Signature:	
Date:	**27/4/16**

Background

The objective is to ensure that all trial data management systems are compliant with the Research Governance Framework. Clinical Trials of Medicinal Products (CTIMPs) computer systems must also comply with International Conference on Harmonisation (ICH) of Good Clinical Practice (GCP) Guideline to ensure that the 'data and results reported are credible and accurate and that the rights, integrity, and confidentiality of the trial subjects are protected.' (ICH GCP)

According to ICH-GCP, the sponsor should:

a. Ensure and document that the electronic data processing system(s) conforms to the sponsor 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 trial).
d. Maintain a security system that prevents unauthorized access to the data.
e. Maintain a list of the individuals who are authorised to make data changes.
f. Maintain adequate backups of the data.
g. Safeguard the blinding, if any (e.g. maintain the blinding during data entry and processing).' (ICH Topic E 6 (R1) Guideline for Good Clinical Practice 5.5.3 a)

Research data must be collected, recorded and managed in accordance with the Data Protection Act (1998) and QMUL and BH's Research Policies. Computer systems for CTIMPs sponsored by BH or QMUL must be set up and maintained in accordance with this SOP and in accordance with the trial's Database Management Plan (DMP) or equivalent document.

Purpose and Objective:

The purpose of this SOP is to outline the basic requirements in the selection, designing, testing, validation implementation and management of clinical research computer systems for trials that are sponsored by Bart's Health NHS Trust (BH) or Queen Mary University of London (QMUL).
The JRMO acknowledges that QMUL and BH CTUs and research groups already have clinical trial computer system SOPs and associated template documents. This document contains over-arching standard operating procedures that contain guiding principles for quality computer data management systems.
The JRMO acknowledges that information technology advances at considerable speed and so the intention is that this SOP provides details of good practices that may be used for trial data management systems in clinical research.
Any technical queries or terminology clarification should be directed to the CTSU in the JRMO.

Scope:

This SOP covers computerised data management systems and trial management systems (hardware and software) (e.g. statistical or other software, electronic participant diaries, coding of personal data, and software validation systems, apps and databases) for Clinical Trials of Medicinal Products (CTIMPs) that are sponsored by QMUL or BH. It is considered to be best practice and therefore is recommended by the JRMO to be used for non-CTIMP studies, where research data is being collected and analysed.
Suitable database may include but are not limited to commercially available and bespoke computer systems, the JRMO approved database 'Discovere' and other databases and computer systems used by clinical trials units (CTUs).

This SOP is intended for use by research teams involved in the creation or management of databases for clinical research, including clinical trials, and should act as a guide to the approach that is taken to the validation and documentation of older computer systems where original records may now be considered inadequate.
For broader research computer systems that may interface with CTIMP computer systems, for example computer systems used by QMUL or BH support departments and subcontractors, see SOP 38a - Computer Systems for CTIMPs. Of note, CTIMP computer systems for CTIMPs that have been contracted out (including support and maintenance) are inspectable by the regulators (MHRA).

Abbreviations:

AE	Adverse Event
ATMP	Advanced Therapy of Medicinal Product
BH	Bart's Health NHS Trust
CI	Chief Investigator
CRF	Case Report Form
CTIMP	Clinical Trial of an Investigational Medicinal Product
CTSU	Clinical Trials Systems Unit
eCRF	Electronic Case Report Form
DMP	Data Management Plan
GCP	Good Clinical Practice
ICT	Information and Communications Technology
ISF	Investigator Site File
JRMO	Joint Research Management Office
MHRA	Medicines and Healthcare products Regulatory Agency
Non-CTIMP	Clinical Trial with no investigational medicinal product i.e. non-drug trial
PI	Principal Investigator
QC	Quality Control
QMUL	Queen Mary University of London
SAE	Serious Adverse Event
SOP	Standard Operating Procedure
SUSAR	Suspected Unexpected Serious Adverse Reaction
TMF	Trial Master File
UAT	User Acceptance Testing

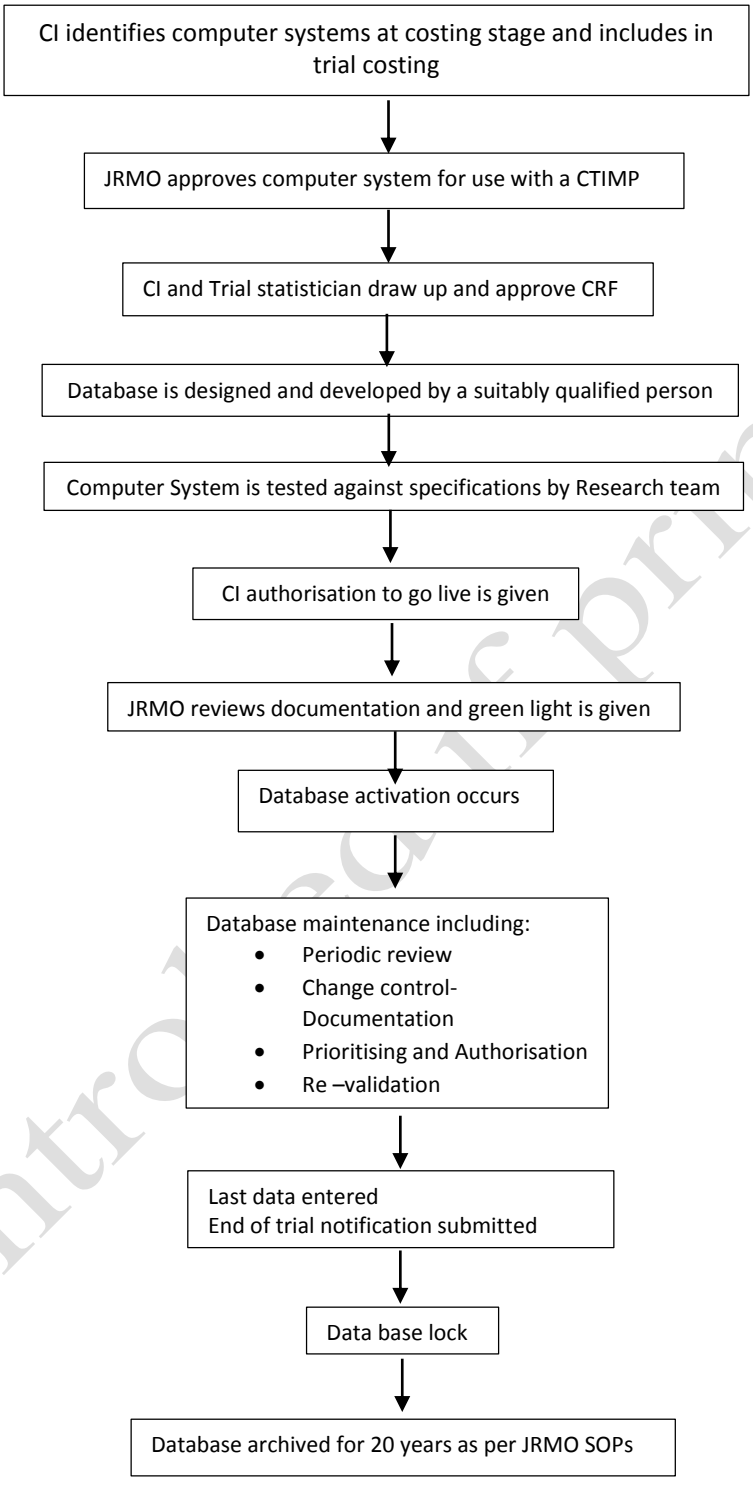
Definitions *(if needed):*

A clinical research computer system is defined as 'the set of hardware, software, procedures and people which together perform one or more of the capture, transmission, processing, analysis and reporting functions on clinical trial management of the clinical development program. [Gold A et al. CR-CSV Working party 2004]
Discovere: Discovere is a fully validated web-based tool for the building and publishing of eCRFs and research databases. It features role-based access, audit trials and query management. For further information see SOPs 901-906 Discovere specific SOPs, available from the Clinical Trials Systems Unit (CTSU). Contact details for the CTSU are on the JRMO website.
REDCap: 'Research Data Capture' is a free, secure, web-based application designed to support data capture for research studies. A centrally provisioned instance of REDCap in a secure High Value Data network zone is provided by QMUL IT. For further information on this system please contact its-research-support@qmul.ac.uk.

Relevant SOPs:

SOP 8 Site agreements for clinical trials
SOP 11 BH/QMUL Sponsorship of CTIMPs – Researchers Guide
SOP 18a Project closure: guidance for research staff of sponsored studies
SOP 20 Archiving for Research Projects
SOP 28 Monitoring
SOP 38a Computer Systems for CTIMPs
SOP 45 Essential documentation and Trial Master File (TMF)
SOP 47 Trial Committees for guidance on committees and charters.
SOPs 101- 106 Discovere specific SOPs.

Flow Chart



SOP text		
	Responsibility	Activity
1.	Chief Investigator (CI)	**Include the Clinical Research Computer System and Trial Data Management in the Costing of the Trial.** When the trial is at funding application stage the CI must include the cost of the clinical trial computer management system.
2.	Chief Investigator (CI)	**Selecting a Clinical Research Computer System for the Trial.** With regard to the type of database to be used, Microsoft Excel or Access will not be accepted by the JRMO for BH or QMUL Sponsored CTIMPs as they do not meet the requirements of this SOP or GCP. If a CI wishes to use Discovere, or needs further guidance on the database selection, they may approach a member of the Clinical Trials Systems Unit (CTSU). Contact details for the CTSU can be found on the JRMO website or via the GCP Manager. To provide a quote for Discovere the CTSU will need to know the required size (number of fields and complexity) of the CRF and whether the trial will use eCRF or paper CRF. Use of any other software should be discussed at Application stage. Vendor assessment should be performed (as per SOP 40) on any unknown vendors. Any proposed clinical research computer systems must have the capability to: • Store data as defined by the case report forms (CRFs) for the number of participants and visits that are defined in the protocol. • Identify each participant by a unique identifying ID. • Distinguish between data that is missing or incomplete and data that is unknown, e.g. 'NK' or '00' and NK_NOV_2015 • Safe-guard the trial blinding where this is applicable to the protocol. • Ensure data can be stored and exported without alteration. • Provide consistent and accurate downloads for analyses. • Provide consistent data coding (e.g. MedDRA coding or other convention that is relevant for the trial). • Prevent duplicate patient entries from being created. E.g. two patient records being created for patient number 0003. Additionally CI must ensure that a selected system has the ability to ensure that: • The code that links the participants' names with their ID should be kept secure and separate from the data used for analysis, unless written confirmation from the GCP manager is given to allow identifying ID to be stored on the database. • The database protects against unintentional un-blinding but should support, where appropriately approved, any trial unblinding procedures. • The database has a system that ensures data quality, for example that warns the user where there is inconsistent or out of range data for the protocol. It is advisable that such system either 'refuses' or 'flags' data that is out of range to the user so that they can clarify data inconsistencies against the source data or their clinical/safety relevance with the PI (or suitably qualified and delegated medical member of the research team). • The system must contain a clear method of version control, including details of what has been changed for each version and when it is 'live'. (See Trial Database: Requirements and Specification template). • The ability to archive the data for 20-years (30-years if the trial is an ATMP) following the end of trial (See SOP 20 - Archiving for Research Projects). • An audit trail to include functions such as modifications/corrections/deletions to data that has been entered. All original data entry records and master and any changes alterations, additions, deletions or modifications are to be retained accurately and comprehensively within the retrievable audit trial. (See Trial Database: Requirements and Specification). • Any linked component must be immutably linked to the computer systems security (see section 4 for security requirements) Before commissioning a database for their CTIMP, the CI must consider the following computer security issues: • Physical location of the servers: Servers holding the data for CTIMPs should be in a secure area where physical access is restricted to authorised personnel only. Physical servers must be within the European Union. The server room must be temperature controlled using a calibrated system, have redundant power supplies, rodent control measures, and have fire suppression systems in place.

		• Backup: Data should only be stored on devices that are backed up in a secure and timely manner. Daily back-up is the ideal, to ensure minimal data loss. The back-up should be to a remote or removable storage, i.e. a disk that is held in a secure fire-proof place. • The process of restoring from backup should be tested regularly and logs kept of this procedure. • Ensure any access to the system and any password assignment is in accordance with the QMUL / BH Regulations and Acceptable Use including: QMUL / BH Systems Password. Ideally, the system should be capable of enforcing regular changes of passwords. • Ensure system is complaint with the QMUL/BH anti-virus policy and the approved QMUL/BH antivirus software is installed on the systems being used. For security testing and validation requirements for proposed computer systems see Trial Database: Requirements and Specification template. Additional considerations • The computer systems/machines that are to be used to enter or access trial data i.e. laptops and PCs should have up-to-date operating system patches installed with appropriate security software (e.g. antivirus/spyware, firewalls) (See Trial Database: Requirements and Specification template). • Documented validation process that is signed off by the developer/designer, the chief investigator (CI), the trial delegated Statistician, and by a qualified person who is independent from the developer/designer (this may be a person from the CTSU). • Documented release of the database for use in the 'live environment'. All data transfer with identifiable personal data will be encrypted prior to transmission or transfer (e.g. before being burnt on to a CD) or uploaded to interfacing computer system (see SOP 38a – Computer Systems for guidance on interfacing trial databases with other computer systems). Unless the CI has dedicated support of data programmer/data system specific personnel and can provide evidence that their preferred system meets the minimum standards expected in this SOP then the JRMO's preferred system will be Discovere. It is the CI's responsibility to ensure that adequate funding provision is made for the personnel and time to validate all computer systems including the trial database. This should include the cost of their time to support the computer system's set-up in this SOP including review and authorisation.
3.	Chief Investigator (CI)	**Security** The database must have security that prevents unauthorised access to the data. This should include role based access, whereby some people will be delegated the role of design, others to enter data, others to approve and others to change data. Each user should have an individual account with a login using username and password. A record should be kept of authorised users and when access was granted or revoked. Once a user leaves the trial and is removed from the delegation log their access to the database (and other computerised systems related to the trial) should be revoked. All systems must be stored on a secure server with user restricted access.
4.	CTSU and GCP manager	**Assess selected system for compliance with the SOP.** Discuss proposed system with CI and team and assess compliance with this SOP. Inform CI of suitability and/or flag potential issues.
5.	Chief Investigator (CI)	**Once funding has been awarded, confirm suitability of software and funding with JRMO.** Once a protocol has been drafted, and if Discovere will be used, an initial meeting between the trial team and the CTSU will be held to discuss the steps for database design and build. This process will follow the Discovere SOP's. If a system is to be used that is new to the trials team, evidence of the system's suitability should be presented to the GCP Manager and CTSU. The CI must provide the documentation to the Sponsor to prove that the database meets all of the requirements in this SOP and ICH-GCP before Provisional Sponsorship approval is given (CTIMPs only). If an existing system is to be used, GCP manger should be informed and allowed time to check suitability of the system. The CI must receive written confirmation from the JRMO that the system is acceptable.

6.	Chief Investigator (CI)	**It is the Chief Investigator's (CI) responsibility to ensure that all chosen clinical research computerised data systems comply with this SOP, with ICH GCP and the relevant UK Statutory Instruments.** Full consideration must be made of data management at all stages of the trial, from protocol design and trial set-up; once the trial is active; when analysing the results and upon closure of the trial. It is the CI's responsibility to ensure that there are plans for data management in all of the following documents: • The protocol. With reference to the JRMO template protocol guidance on databases and computer systems the CI must write a protocol with information on the description of the procedures for data collection. This must include what data must be collected to assess all the trial end points(s) both primary and secondary. It may be necessary in the protocol to indicate that detailed data management, including computer systems and database are outlined in a data management plan (DMP). • Case Report Forms (CRFs) – see Associated Document 1 CRF design guidance. • In the design and build documentation of computerised data management systems– see Data Management Plan template. • In a data management plan (DMP) (see Data Management Plan template). • Storage and archiving the data and CRFs plan/document – see SOP 20 Archiving for Research Projects. • Within the research site agreements, where sites are delegated data management by the CI (see SOP 8 - Site agreements for clinical trials). Data management should also be considered when assessing levels of monitoring of the trial and on-going oversight (see SOP 28 – Monitoring and associated documents) Where the CI has delegated database development or testing to other research personnel or an external vendor, they must be either listed on the delegation log in the trial master file (TMF) or contracted following a full vendor assessment.
7.	Chief Investigator (CI)	**Ensure that the Database Developer is appropriately qualified.** The CI must provide the JRMO, as sponsor confirmation that the database developer is suitably qualified to build the CTIMP database. ICH GCP states that: "5.5.1 The sponsor should utilize appropriately qualified individuals to supervise the overall conduct of the trial, *to handle the data, to verify the data*, to conduct the statistical analyses, and to prepare the trial reports". JRMO Staff responsible for Discovere will be appropriately trained and qualified. Evidence of this will be retained in staff training folders (see SOP 34b JRMO Staff training and Induction). (The delegation of the Statistician is the responsibility of the Chief Investigator and is outlined in Sponsor SOP 11a – Sponsorship of CTIMPs).
8.	Chief Investigator (CI)	**Design and Development:** **The CI is responsible for designing the trial Case Report Forms (CRFs) and for writing the database specifications.** A case report form (CRF) must be designed to record all information required by the protocol on each trial subject and will contribute to the data that will be analysed in order to answer the protocol aims and objectives. The Chief Investigator (CI), in accordance with GCP, "should ensure the accuracy, completeness, legibility and timeliness of the data reported in the Case Report Forms (CRFs) and in all required reports" (4.9.1, ICH-GCP). Where the CI has delegated these duties to other research personnel, they must be listed on the delegation log in the trial master file (TMF). The CI must ensure that data required by the protocol are reported accurately on CRFs and that they are consistent with the source documents e.g. medical notes scans or SAE forms (see Associated Document 2 Good Documentation Practice). The CRFs must be designed to capture the required trial data across all research sites and for every participant consented to take part in the trial and including screening fails.

		Case Report Forms are not source data but a tool for recording source data. However, if source data is recorded *directly into a CRF* i.e. when the research nurse records the telephone interview answers directly into the case report forms, **the decision to use the CRF as source data must be documented** before the trial starts**.** The documentation of the decision should be included in the TMF and in the source data list in each Investigator Site File (ISF) so that it can be appropriately monitored at sites (see SOP 11a – Sponsorship of CTIMPs – Guide for Researcher for information required before the trial starts and SOP 28 –Monitoring). It is advisable that the CI designs the CRFs after the protocol has received provisional sponsorship approval. The protocol may be amended during the REC and MHRA approval process but by designing the CRFs and database at this stage, i.e. in parallel with regulatory approval, as it may save delays in receiving 'greenlight to activate the site' from the GCP Manager.
9.	Chief Investigator (CI)	**Mandatory CRF/databases pages** Every CRF & database must have pages/areas to catch the following information: • AEs/SAEs/SUSARs safety information, • Concomitant medications • Inclusion & Exclusion Criteria Review • Eligibility and PI signature • Participant Status (i.e. screen-fail, withdrawn, enrolled) • PI signoff (confirming that the data in the CRF is accurate and complete at a site level) • Dates of all visits / interactions with the participant must be recorded. • CI signoff as part of data lock and oversight • Trial Completion • IMP Administration & compliance • Randomisation (if applicable) The following pages are optional but should be considered by the CI: • Medical History (Smoking and Alcohol History if applicable) • Physical Examination • Post Randomisation • Laboratory • Physical Examination • Unscheduled Visits • IMP batch no. and Expiry date The CRFs must have an authorisation section for the Principal Investigator to authorise each CRF at their site. For specific guidance on CRF design and structure see associated document 1 for CRF Design and Structure Guidance.
10.	Trial Statistician	**Statistician approves the CRFs.** This ensures that the CRFs contain the data points required for the statistical analysis plan.
11.	Chief Investigator (CI)	**CI approves the CRFs.** The CI must confirm that the CRFs match the protocol and that they collect sufficient information to answer the research questions. The CRFs must record all visits, participant interactions, procedure and intervention dates. The CRF should then be used to create eCRF(s) and/or a database specification (if paper XRF to be used) document. A template specification document can be found associated with Discovere SOPs.
12.	Chief Investigator (CI)	**Database and Computer System Documentation Management.** The CI or their delegated individual is responsible for the computer system documentation management, including testing and validation documentation. Every test and QC check should be recorded each time it is carried out. Evidence of the testing must be retained in the TMF.

		The CI must ensure that records relating to the various systems are readily available, well organised, and key staff are prepared to present, discuss and review the detail, as necessary with any monitor, auditor or inspector. The computer System documentation (including software) should be correct and updated. All Requirements and Specification documentation (see Requirements and specifications template) must be retained in accordance with QMUL and BH's Archiving SOP – 20, for 20-years (30-years for ATMPs).
13.	Chief Investigator (CI)	**Database/Software Design Specification.** The CI must ensure a full and detailed design specification has been completed prior to any bespoke software or database development**.** A detailed and complete specification must be written from the end-user perspective for all bespoke software and databases. It may include workflow diagrams and screen mock-ups. The design specification documentation should contain full system details including: • Full descriptions of all features required and how they are to be used by the end-user. • Outline how the computer system meets the requirements specified. • What application development model will be adopted (if applicable). • Any data-flow processes including database structure. • How the system will be delivered. • How CRF change requests are implemented and managed post design sign-Off, or they must be included in the DMP. • How system design changes will be managed. • Details on what the requirements of the trial computer system are. • Key deliverables and source-code documentation. • How the end-user will be required to use the software i.e. data entry. • What data validation rules will be required. • Data output requirements and reports. • User access control methods. • Measures in place for resilience including backups and data recovery. • Data encryption states at rest, in transport, at backup and in archive. The design specification should be printed and signed by the Chief Investigator and Statistician as well as the vendor/developer as part of the design qualification. Ensure the Design Specification is stored in the TMF and referenced in the Requirements and Specification document (see template associated to this SOP) or equivalent document. Document a physical and IT security protocol outlining how the system secured against unauthorised access, theft or attack.
14.	Database designer (CTSU or trial team based)	**Including Programming Standards within specification documents.** Source code development standards should be detailed within System specifications to ensure the quality and consistency of software code. This should be stated prior to system development and used consistently throughout the development cycle. The CI must agree source code standards and ensure this is specified in the design specification document. Source code must be well documented (including source code comments), maintain header information such as author, version, date and any explanatory coding notes.
15.	Database designer (CTSU or trial team based)	**Once the database specifications have been signed off by the CI and statistician, database build can commence.** The database and eCRF(s) must be built in line with specifications (provided by the trial team, and signed off by the Chief Investigator and trial statistician).
16.	Database designer (CTSU or	There should be written documentation from the developer/vendor indicating that the design meets user specification and is ready for testing.

	trial team based)	
17.	Database designer (CTSU or trial team based)	**Implementation System in compliance with specification.** Record any installation observations and tests conducted to evidence the system has been installed successfully. Maintain an Access Control List of who needs access to the system being validated including review dates. Ensure the Access Control List is stored in the Trial Master File and referenced in the Requirements and Specification documents. Follow guidelines from the supplier or vendor of the computer system that is being validated to ensure all appropriate set-up options have been completed as appropriate to the required use. Consider most appropriate delivery of the CI's software such as workstation installation via Networked Applications (user-authenticated installation), or direct installation. Ensure the host computer system (e.g. workstation or server) meets the system configuration requirements for the system being validated, including server/workstation operating system processor and memory specifications. Ensure any system dependencies specified are pre-installed and available on the host computer system.
18.	Database designer (CTSU or trial team based)	**Validation and Testing** **Training Requirements for Staff Involved in the Validation of Computerised Systems.** All staff involved in the validation of computer systems must be appropriately trained (including on the system software and trial). A statement on the qualifications and training background of personnel engaged in testing and validation of computerised systems, including consultants and sub-contractors must be prepared and maintained. Delegation logs and training logs should be maintained. Testing should be performed by a person independent to the main computer programmer and should include a member of the research team.
19.	CI or delegate	**Validate the database/computer system.** The database and all other computer systems used in the trial, must be validated to "demonstrate that [the] system, consisting of business procedures which has attributes of People and procedures, Hardware and Software, is fit for purpose, performs consistently, and that changes are effectively controlled […] Validation applies to all systems that may impact on the integrity and quality of clinical data"[i]. The responsibility for validation lies with the Chief Investigator, or delegated individual, as the 'owner and user' of the computer system. Validation involves checking that the program as implemented meets the expectations of the Chief Investigator and to check that database matches the specifications and the documented descriptions. Validation must be done prior to go live of any system used in a CTIMP. If any modifications are made to the database during its lifecycle these should be tested and validated. Where it is necessary, the database specification and associated documents and the testing regime should be updated.
20.	CI	**The Scope of the Computer System Validation and Tests.** The CI is responsible for the assessment of which elements of the computer systems need to be validated and to what extent, to ensure the quality of their trial data. Consideration should be given to the three different elements involved: • Process control systems, • Data processing systems, (including data collection/capture) • Data record/storage systems. Additionally, the 'interfaces' or links between these may need validation. The Data Management Plan and/or testing and validation plans should consider the three types of computer application systems and the 'interfacing systems'.

		The CI should be able to demonstrate through the validation evidence that they have a high level of confidence in the integrity of both the processes executed within the controlling computer system and in those processes controlled by the computer system within the prescribed operating environment.
21.	CI	**Testing Methodology and creation of test scripts.** User acceptance testing must be carried out by the end-users of the system being validated with the aim that the system meets the user requirements and specification. This should be undertaken prior to a system moving from a development environment to a production environment. Ensure testing is done on a system other than the live/production system. The test system must be as identical to the live/production system as possible but must be separate to ensure there is no contamination of live data with test data. Detailed test scripts must be written to include test data and expected results. For example, document the input variables of a 'dummy participant' which can then be entered onto the system including expected data outputs. Different scenarios should be tested. Test scripts should be developed, formally documented and used to demonstrate that the computer system has been installed and operating according to the specification and is fit for purpose. Test scripts should also include boundary values or incorrect values to ensure any form or rule-based input validation works as expected. (See Associated Document 3 UAT). These scripts should include scope for re-testing any function which fails, actions taken to correct (and changed in the specifications if necessary). For incremental or iterative system development, a test plan should be provided for every software release, patch or additional module within the development lifecycle. This may include testing the transferring/importing/exporting data (see section and see SOP 38a – Computer Systems, for guidance). Each screen should be tested with expected values and any data entry validation rules should be tested. Following QC checks the database/eCRF must be tested by further independent staff.
22.	CI	**Testing Successes and Failures, Handling Exceptions.** All system or data errors should be noted and sent back to the Computer Programmer and re-tested by the user until all tests are completed satisfactorily. Record all testing successes and failures in the Test Plan including any remedial action required. Any test failures must be re-tested following the completion of the remedial action to ensure they are fit for purpose. Record any testing failures and action required in the Test Script/ DPM's Test Plan. Record any system exception messages in the Test Plan and record any further action required ensuring every scenario is re-tested. Ensure appropriate exception handling is controlled in the application to enable end-user to record any system errors during testing, or use automatic exception notifications. Ensure all test scripts have been satisfactory completed.
23.	CI	**System Configuration and Management.** The test should be conducted on the CI's hardware/software that is to be used in the trial, for instance, a tablet or correct version of Internet Explorer. If the system is delivered via a web browser ensure supplier recommended web browser version (e.g. Internet Explorer, Firefox, and Chrome) is available and installed correctly for its use. Checks should be performed to ensure appropriate system user rights are available to ensure successful installation.
24.	CI	**Documentation Development and Retention.** Print and sign all User Acceptance Test documentation authorisations by the Chief Investigator. Ensure the User Acceptance Test documentation is stored in the Trial Master File.

		Complete the document control header for each document completed including author, version (incremental) and date, approved by Initials and date, reviewed by initials and date.
25.	Trial delegated Statistician	**Approval & Release Process for the Clinical Research Computer System Statistical review and approval of the CRF and Clinical Research Computer System.** The statistician's final approval of both the database and CRF must be documented and kept in the Trial Master File (TMF).
26.	CI	**Approve that the database has passed functional testing and has been validated.** The CI's final approval of the final database and CRF must be documented and kept in the Trial Master File (TMF). CI and statistician to sign off final build using template associated to this SOP.
27.	CTSU/QMUL ICT	**Once CI and Statistician sign-off is received the CTSU will review documentation.** If the database/eCRF is Discovere (i.e. CTSU Built and managed) the database documentation will be sent to QM ICT for review. The CTSU/QMUL ICT should be sent: • Signed Specifications • Test plan and completed scripts (including change documents if applicable) • CI and Statistician final approval The CTSU/QMUL ICT will check that all required documents are present, completed and covers all aspects needed. This should ensure checking that the version is clearly documented. CTSU/QMUL ICT will email the relevant GCP manager to confirm CI, Statistician and CSTU sign off.
28.	Chief Investigator	**Formal Acceptance of the System.** CTSU review of the computer system should be documented in writing and stored in the Trial Master File.
29.	GCP manager	**GCP Team - 'Green light Process'.** GCP manager will include 'Go Live' to the trial, which includes the computer system, in green light report and the 'green light to activate sites' email (see SOP 11b on sponsorship for guidance).
30.	Chief Investigator	**Training and Training Records for Computerised Systems.** Prior to any staff (co-ordination, site or JRMO) being given access to the database or eCRF, training should be given. The Chief Investigator or nominated/delegated authority is responsible for computer system training. A clinical trial may refer to a trial specific training SOP if appropriate. All end-users must be appropriately trained in the computer system being used. A central training log must be held in the TMF.
31.	Chief Investigator	**A system or procedure should be in place to manage site users.** A dedicated person should be identified to provide site and user support. A documented system or procedure should be in place, identifying who can approve new uses and their roles and who will add new users. Site management includes adding/removing users to studies and adding/removing sites.
32.	CI or delegate	**User Manuals and Training (maintenance).** Reference any user manuals and training material in the Requirements and Specification Plan. Ensure any future releases of the computer system being implemented have up to date Requirements and Specification Plan.
33.	Chief Investigator or delegate	**Clinical Research Computer System on-going use and maintenance.** (Computer System Data Management Plans/Data SOPs) The Chief Investigator or nominated/delegated authority is responsible for the computer system use and maintenance and for the creation and maintenance of the Data Management Plan (DMP) or trial specific computer systems SOPs. Creation of a DMP for each studies is mandatory for all new studies.
34.	Chief Investigator or delegate	**Each CTIMP should have a Computer System SOP/specifications for each system/database.** Create a Specifications and include any maintenance or support contract for software and host systems.

		The specification may include: • Include a statement of support from the developer or vendor including any service level agreement. • Store this document in the Trial Master File and ensure it is referenced in the Requirements and Specification plan • There should be additional procedures for critical data entry, requiring a second QC check, for example checking data that is required for primary endpoints. A second authorised person with access may verify the data entry is accurate based upon the source data. This information should be recorded in the specification. • The Chief Investigator or nominated/delegated authority is responsible for problem management. The specifications will refer to the procedures to be used to develop the database and manage the data and include instructions to the research team in the database's use and change control.
35.	CI or delegate	**Routine Backups.** For data stored on systems other than the QMUL or BH shared drive (which is routinely backed up), documentation detailing the back-up process (including details of location where relevant) should be kept and stored in the Trial Master File and ensure it is referenced in the specification document . The frequency of the backups is dependent upon the risk assessment of the loss of data. In order to guarantee the availability of the data copies should be made so that if necessary it is possible to re-construct CTIMP data documentation, including audit trial records for an MHRA inspection.
36.	CI or delegate	**Restoration of System Data.** A 'restore procedure' must be documented and referenced in the DPM. The restore procedure may be part of an established SOP or disaster recovery plan, if so ensure it is referenced in the Requirements and Specification Plan. The Chief Investigator or nominated/delegated authority is responsible to ensure that an appropriate level of system backup and restoration procedures are in place. Measures should be in place to ensure validated recovery of original data following back up, media transfer, transcription or system failure.
37.	CI or delegate	**User Support.** The Chief Investigator or nominated/delegated authority is responsible for user support. The Chief Investigator or nominated/delegated authority is responsible to ensure an appropriate business continuity procedure is in place (i.e. a plan should be in place in case the database or system In unavailable for any reason.
38.	CI or delegate	**Support and assistance with database / computer system problems.** Document the procedure for obtaining support in event of system issues and failures. Include support contact information. Record any issues or failures in the computer system version log (or equivalent) including any support reference number, remedial action and date resolved.
39.	Database designer (CTSU or trial team based)	**Change Control** **A process for change control must be present for the duration of the trial.** Each version of the CRF/E-CRF/database/computer system must be version controlled to ensure there is a clear audit trial of the change control following testing modifications. Complete the document control footer/header/filename for each document produced including author, version (incremental), 'approved by' (Initials and date), and 'reviewed by' (initials and date). Previous versions must be in included in the TMF to ensure traceability and historical information preservation. Software code must have appropriate version control, preferably through an automated version control repository, or via the source code. There are several instances where a change to the system or database may be needed. These include an amendment to the protocol which calls for a change to the database, an upgrade to the system or an error being highlighted. Any change (however small) to a database /eCRF is a new version. Each time a change is needed a review should be held to determine the effects of this change on the existing data.

40.	Database designer (CTSU or trial team based)	**Create and maintain a Change control log.** A Version Control log must be maintained for each system being validated and throughout the period of the Clinical Trial. The Chief Investigator or nominated/delegated authority is responsible for change management of the clinical trial computer systems. Ensure the Computer System Change log (see template Database Change Control Form associated with this SOP) is stored in the Trial Master File and referenced in the Requirements and Specification Plan. Any changes to the completed Requirements and Specification documentation must be fully auditable. Any previous version of the documentation must be stored and indicated as superseded.
41.	CI or delegate	**Documentation, Prioritisation and Authorisation of Changes to Validated Systems** The reasons for changes to the research trial computer system should be documented. For example, email correspondence or a 'change request form'. The CI and programme developer can then assess whether the change is necessary, whether it is required across all systems/sites and that the appropriate person is authorised to implement the changes. This may depend upon the complexity and scope of a change i.e. minor corrections may not need a thorough 'impact risk assessment'. Before changes are made, there should be formal change control procedures in the following areas: • Records of details of the proposed change(s) and reasons for them (e.g. an improvement to the system, correction to an error, fixing a deviation, following a protocol amendment, hardware or software updates). • Status of the computer system and controls in place prior to implementing change. • Review changes and approval/rejection process and documentation. • Method of indicating the status of the change in the documentation i.e. pending, in progress, implemented. • Method of assessing the impact of the change. Interface of change control procedures with configuration systems i.e. how will the changes impact interfacing computer systems? Any approved change request must be reflected in the Requirements Specification, Design Specification and any other relevant validation documentation. Amend these documents according to version control/change control log.
42.	CI or delegate	**Re-validation should occur.** Each change to the database must lead to a new round of validation and UAT, however the extent of UAT or testing needed should be assessed and proportionate. The change management should accommodate enhancement of the system i.e. to change the specification that were not identified before the trial started. Re-validate any component of the system affected by the change request in a test environment. Save redundant source code and documentation in the TMF. Ensure that following has been completed: • All errors/failures have been followed up to resolution • Same type of tests but applied after integrating the modules. • If the program is purchased, then validation proof needs to have been assessed by the CI's team.
43.	Database designer (CTSU or trial team based)	**Rerelease and Installation.** A system release date must be agreed between the end-users and documented in the Requirements and Specification Plan. Post install checks must be made and documented to verify successful installations
44.	Chief Investigator	**Installation of Changes and Provision of Training.** Inform end-users of the proposed change and provide training and amend any user guidance documentation as appropriate.

		Announce an install date to end users for the implementation of the change. Make them aware of any scheduled down time, and install the required change following the validation procedure outlined in this document.
45.	Chief Investigator	**Depending on length and size of trial a periodic review may be needed.** The Chief Investigator or nominated/delegated authority is responsible for assessing the needed for a periodic review of the research trial computerised system. They should ensure, conduct and document a periodic review to ensure the system documentation is up to date and the validated system is functioning according to the specification: • Review of computer system version log to evaluate any reoccurring issues or major problems. • Review user training and training records. • Review DPM and computer systems SOPs and ensure all documentation is up to date. Periodic review of the computer system is often included in a trial committee's remit/charter, so that the database is reviewed periodically. See SOP 47 – Trial Committees for guidance on committees and charters. Documentation to evidence this review should be kept in the TMF.
46.	Chief Investigator	**End of Trial** **The Chief Investigator is responsible for ensuring end of trial procedures are completed as per DMP and SOP 18a - Project closure: guidance for research staff of sponsored studies.** Data lock procedures should be fully documented in the DMP. Data lock procedures should ensure that the data set used for analysis is clearly identified. This should be retained separately from the live database to allow reproducible analyses. It is a controlled procedure that freezes the data in a particular format securing the trial data and preventing further changes. There is a requirement to ensure all the trial data have been received, verified, fully coded and cleaned for analysis with all queries resolved before locking the database for further analyses. Unlocking of the database should be strictly controlled and documented in the DMP.
47.	Trial Statistician	**Database lock.** The designated statistician should receive a full and dated download of the database or computer systems, with a complete and accurate dataset used for analysis.
48.	Chief Investigator or delegate	**Database should be archived and retained for 20 years.** Once the data lock has occurred and clinical study report is submitted the database should be archived.

Change Control

This section outlines changed from SOP 38 version 3.0 to SOP 38b version 4.0.

Section Changed	Summary and description of change
All	Migrated to New template
All	Full update of all sections and requirements

List of Associated Documents *(these are standalone documents)*

Document	Document name
Associated Document 1	CRF design and structure Guidance
Associated Document 2	Good Documentation Practice
Associated Document 3	Guidance on UAT

List of templates

Templates
Sign Off Final Build Form
DMP
Requirement and specification
Database Change Control Form

References

[i] Gold A, Wells H, Tucker J, et al, *Computerised System Validation in Clinical Research*, *A Practical Guide,* 2nd Edition (CR-CSV Working Party, Association for Clinical Data Management) 2004.

Relevant recent guidance is also provided in ISO/IEC17799:2000 on Information Technology – "Code of practice for information security management" and also in the pre-amble to FDA's 21 CFR Part 11.

Good practices for computerised systems in regulated 'GXP' environments, pharmaceutical, inspection convention pharmaceutical inspection co-operation scheme, PI 011-3 25 September 2007.

In the drafting of the document, the JRMO referenced Cardiff University School of Medicine's Framework Standard Operating Procedure (F-SOP) 'Computer System Validation for Clinical Trials.