



Computer System Validation for Clinical Trials:

Framework Standard Operating Procedure (F-SOP)

Author:	Tim Cross		
Version History:	0.1di DRAFT	Date:	24-April-2013
	0.2 DRAFT		12-June-2013
Current Version:	1.0		17-June-2013
Approved By:	ITIM	Date:	17-June-2013
Position:			
REVIEWED			
Initials:		Date:	

Document Filename: System Validation SOP 0.1.docx

Document Location: \\shrmedic\MEDIC\Shared\DNMED\School of medicine central administration\IT\Clinical Trials\Governance and MHRA

CONTENTS

Part 1 – Operating Procedure Definition and Scope	5
Procedure Flow Diagram	6
Part 2 – Framework Standard Operating Procedure (F-SOP)*	7
1 Documentation Management	7
1.1 Security	7
1.2 Standards	7
1.3 Review and Approval	7
1.4 Distribution	7
1.5 Access Control.....	7
1.6 Version Control	8
1.7 Change History	8
1.8 Archiving & Retention Policy.....	8
2 Software Development and Testing Including One-off Programs	8
2.1 Requirements Specification (Needs Analysis)	8
2.2 Functional Specification*	8
2.3 Design Specification*	9
2.4 Test Plan/Results.....	9
2.5 Testing Failures/Exception Handling.....	9
2.6 Change/Version Control*.....	10
2.7 User Manual and Training (development)*	10
2.8 Programming Standards*.....	10
2.9 Documentation Sign-Off and Retention.....	10
2.10 Release and Installation	11
3 System Set-up and Installation	11
3.1 System configuration	11
3.2 Set-up options.....	11
3.3 Installation test & documentation	11
4 User Acceptance Testing.....	11

4.1	Testing methodology	11
4.2	Testing Successes and failures	12
4.3	Documentation development and retention	12
4.4	Reporting and sign-off.....	12
4.5	Acceptance criteria for authorisation of a valid system for use	12
4.6	Formal acceptance of the system	12
4.7	Ongoing validation	12
5	Training	13
5.1	Training requirements for staff involved in the validation of computerised systems	13
5.2	Training records for computerised systems (may refer to a training SOP).....	13
6	Security	13
6.1	Password assignment and changes.....	13
6.2	Access authority levels and their review.....	13
6.3	Physical security	13
6.4	Virus checking and prevention.....	13
7	System Use and Maintenance	14
7.1	An SOP for each system	14
8	User Support	14
8.1	Support/help for problems	14
8.2	User Manuals and training (maintenance).....	14
9	Problem Management	14
9.1	Issue log.....	14
9.2	Monitoring and resolution	15
10	System Backup and Restoration	15
10.1	Routine backups.....	15
10.2	Backup log	15
10.3	Restoration of system and data	15
11	Business Continuity.....	15
11.1	System recovery in the event of a major disaster (may reference disaster recovery plan).....	15

12	Change Management.....	15
12.1	Documentation and maintenance of the system configuration	15
12.2	Documentation, prioritisation and authorisation of changes to validated systems	16
12.3	Development, testing, documentation and review of changes	16
12.4	Installation of changes and provision of training	16
13	Periodic Review.....	16
13.1	Revalidation requirements.....	16
13.2	Re-testing	16
	Appendix A – Validation Plan Template	17
	Appendix B - Requirements Specification Template	20
	Appendix C – Test Plan / Log Template	21
	Appendix D - Satisfactory Completion and Hand-over Template	22
	Appendix E – Installation Test Log	23
	Appendix F – User Acceptance Sign-Off Template	24
	Appendix G – Change Request Template	25
	Appendix H – Issue Log Template.....	26
	Appendix I – System Backup Process Template	27
	Appendix J – System Disaster Recovery Template	28

PART 1 – OPERATING PROCEDURE DEFINITION AND SCOPE

i. VALIDATION DEFINITION

Computer system validation is to “*demonstrate that a system, consisting of a controlled business process 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*¹.”

ii. VALIDATION POLICY

All systems used within a clinical trial must have appropriate validation documentation in place, as outlined and referenced within this standard operating procedure. Where indicated the validation templates in this SOP must be used throughout the validation lifecycle.

iii. SCOPE OF VALIDATION POLICY AND F-SOP

This Framework Standard Operating Procedure (F-SOP) is to be used as a basis for the development of a SOP for all non-validated computerised systems that are used within a clinical trial setting. The Framework SOP should be adapted as appropriate for the development of a system validation SOP as appropriate to the clinical trial. The validation tasks outlined in the SOP must be done prospectively for all computer systems used in a clinical trial. A clinical research computerised system is defined as: “*The set of hardware, software, procedures and people which together perform one or more of the capture, transmissions, processing, analysis and reporting functions on clinical trial data management of the clinical development programme.*”

This F-SOP can also be used as a guide for other non-clinical trial computer systems that are being implemented to ensure the system being implemented is fit for purpose and appropriately controlled.

iv. RESPONSIBILITY FOR SYSTEM VALIDATION

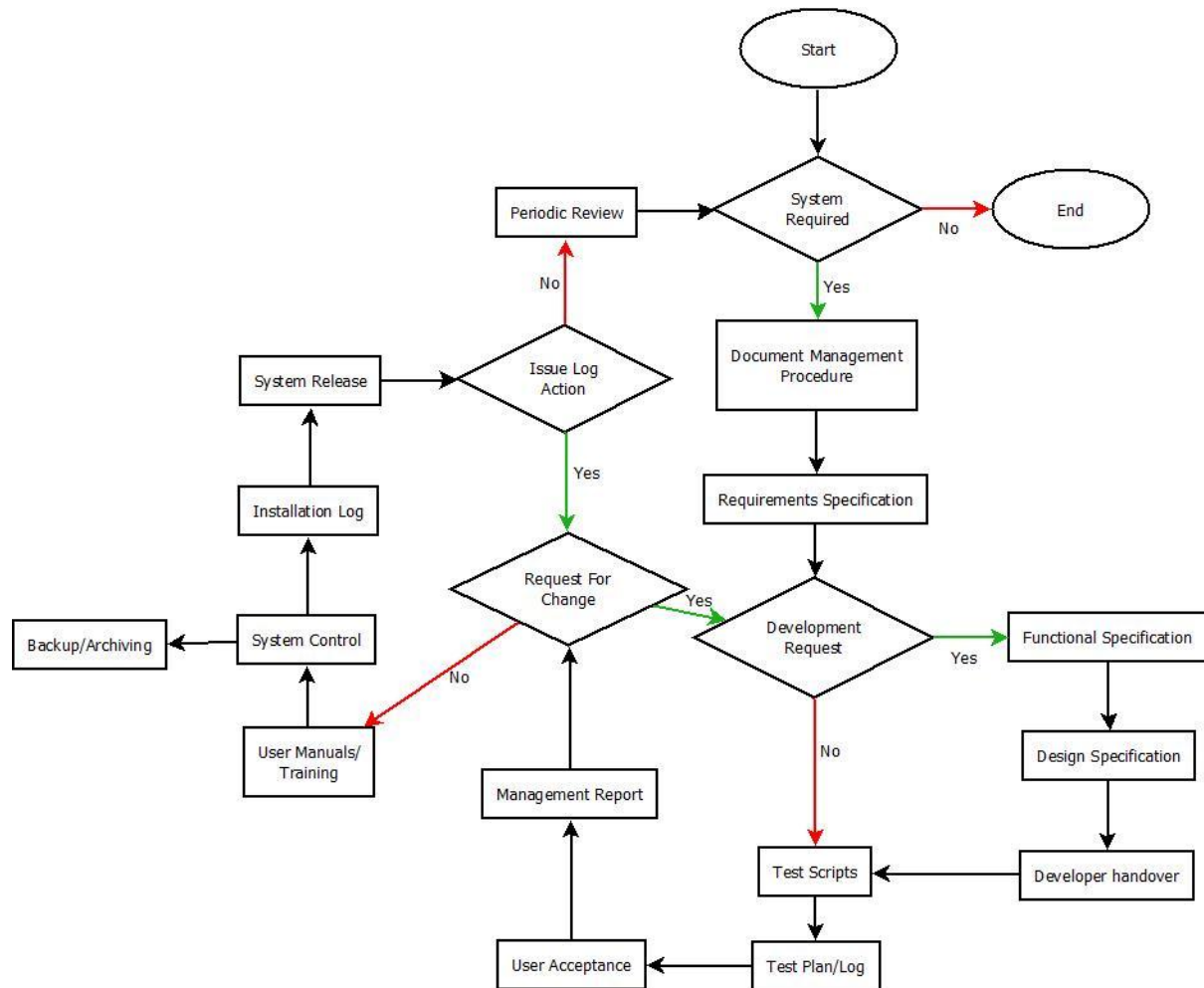
As part of the clinical trial setup procedure the Chief Investigator or nominated member of the trial team are required to have an interview with the Trial Unit Information Officer to discuss IT requirements in detail which will include advice on validation. For non-Clinical Trial Unit trials, IT requirements must be discussed with the Schools IT Manager. Further advice and support is available from the School IT Office throughout the process but it should be noted that “***the responsibility for validation lies with the owner and users of the business system***” which would usually be the Chief Investigator or nominated member of the trial staff.

v. SOP OWNER AND APPROVAL

The Computer System Validation SOP is owned by the IT & Information Management Working Group a sub group of the Clinical Trials Management Group who is responsible for the development of the SOP, subsequent review and implementation of any SOP changes.

¹ *Computerised Systems Validation in Clinical Research, A Practical Guide, 2nd Edition (CR-CSV Working Party, Association for Clinical Data Management) 2004. Used throughout and indicated by italicised text in quotes.*

CLINICAL TRIAL SYSTEM VALIDATION PROCEDURE FLOW DIAGRAM



PART 2 – FRAMEWORK STANDARD OPERATING PROCEDURE (F-SOP)*

1 DOCUMENTATION MANAGEMENT

This section describes the procedure for the security, development and management of any System Validation documentation, including this SOP, its appendices and documentation referenced within.

The Chief Investigator or nominated/delegated authority is responsible for document management.

If a Clinical Trial Unit has its own SOP on document management then this should be used as an alternative to this section.

1.1 SECURITY

1.1.a System Validation SOP

This SOP documentation must be stored on the University network for the purposes of editing and amending, within a secure folder accessible by document authors only. The full path to the current document version must be included in the SOP cover-sheet. A document management system (such as Q-Pulse) can be used as an alternative storage and control mechanism.

1.1.b Other Validation Documentation

Any documentation completed as part of the System Validation Plan must be kept secure within the Trial Master File and adheres to access control mechanisms in place.

1.2 STANDARDS

Documentation standards will be developed and applied generically via the IT & Information Management Working Group (ITIM) which is a sub group of the Clinical Trials Management Group where applicable.

1.3 REVIEW AND APPROVAL

The System Validation documentation, including this SOP, its appendices and documentation referenced within will be reviewed periodically by the ITIM Group and will be signed off by the Chair of the Group upon any change to the documentation.

1.4 DISTRIBUTION

The SOP will be made available to nominated trial staff through the University network.

Any validation documentation completed must be kept securely within the Trial Master File (TMF), whether electronic or paper format, and distributed in accordance to the trial procedures in place.

1.5 ACCESS CONTROL

Access to the validation documentation should be kept secure in accordance to any procedures currently in place for the TMF.

1.6 VERSION CONTROL

Any changes to this SOP will be clearly indicated by the version number on the SOP cover sheet and document filename.

Any changes to completed validation documentation as referenced in this SOP must be clearly indicated by incrementing the version number, date and author at the top of each document using the templates provided in the appendices.

1.7 CHANGE HISTORY

Any changes to completed validation documentation as referenced in this SOP must be fully auditable. Any previous version of the documentation must be stored and indicated by the version number at the top of the document template and by the document filename and stored securely on the University network. Alternatively an approved document management system can be used (such as QPulse) which retains historical information, maintains version control and imbeds electronic signatures.

1.8 ARCHIVING & RETENTION POLICY

All validation documentation must be retained in accordance with the University Standard Operating Procedure for Archiving records from clinical trials of investigational medicinal products.

2 SOFTWARE DEVELOPMENT AND TESTING INCLUDING ONE-OFF PROGRAMS

This section describes the procedure for producing documentary evidence to verify that any software (including database) developed or used for a clinical trial has been specified, designed, tested and signed off prior to the implementation.

The Chief Investigator or nominated/delegated authority is responsible for software development and testing.

* Indicates requirement applicable to bespoke software or database development only. Everything else is applicable to ALL computer systems as defined in Part I.

2.1 REQUIREMENTS SPECIFICATION (NEEDS ANALYSIS)

- Complete Appendix B1 : Requirements Specification and Appendix B2 : Needs Analysis
- Print and sign by the Chief Investigator or nominee.
- Ensure the Requirements Specification is stored in the Trial Master File and referenced in the Validation Plan (Appendix A).

2.2 FUNCTIONAL SPECIFICATION*

Functional specification documentation should include detail on how the requirements outlined in the Requirements Specification (2.1) will be achieved. Specification will be from the end-user perspective and may include workflow diagrams, screen mock-ups and full description of all features required and how they are to be used by the end-user.

Include how the end-user will be required to use the software (data entry), any data validation rules required, data output requirements and reports.

- Refer to the University Data Management SOP
- Ensure a full and detailed functional specification (user-driven) has been completed for any bespoke software or database development.
- Print and sign by the Chief Investigator or nominee.
- Ensure the Functional Specification is stored in the Trial Master File and referenced in the Validation Plan (Appendix A).

2.3 DESIGN SPECIFICATION*

Design specification documentation should include more technical detail including what application development model should be adopted, any data-flow processes including database structure, key deliverables and source-code documentation.

Include how the software/database should be delivered and how any design changes should be managed.

- Ensure a full and detailed design specification has been completed for any bespoke software or database development.
- The design specification must be completed by a qualified vendor/developer.
- The design specification should outline how it meets the requirements specified.
- The design specification should be printed and signed by the Chief Investigator or nominee as well as the vendor/developer as part of the design qualification
- The design specification should state how change requests are implemented and managed post design sign-off.
- A formal handover letter should be produced by the developer/vendor and signed by the Chief Investigator indicating that the design meets user specification and is ready for testing.
- Ensure the Design Specification is stored in the Trial Master File and referenced in the Validation Plan (Appendix A).

2.4 TEST PLAN/RESULTS

The software or database development, or any off-shelf system (such as SPSS, Microsoft Access etc.) must be fully tested by the end-user against the requirements, functional and design specifications, to ensure any data input and output produces the required result. The test should be conducted on the client hardware/software that is to be used in the trial, for instance, an iPad or correct version of Internet Explorer. Each screen should be tested with expected values and any data entry validation rules should be tested. Any system or data errors should be noted and re-tested until all tests are satisfactory.

For incremental or iterative system development, a Test Plan should be provided for every software release, patch or additional module within the development lifecycle. Refer to **Section 4: User Acceptance Testing** for the procedure for releasing development and test systems to a production environment.

2.5 TESTING FAILURES/EXCEPTION HANDLING

- Record all test results and outcomes and specify if the test was a success or fail.
- Record any testing failures and action required in the Test Plan (Appendix C).

- Re-test any function that failed and record in the Test Plan and record any further action if necessary.
- 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.

2.6 CHANGE/VERSION CONTROL*

- Complete the document control header for each document produced including author, version (incremental), approved by Initials and date, reviewed by initials and date. Previous version must be archived in accordance with the University Standard Operating Procedure for Archiving records from clinical trials of investigational medicinal products 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.
- Document any change request in a Change Request Log (Appendix G, see also Section 12 of this SOP).
- Software changes must be documented by the developer in the programme source code.

2.7 USER MANUAL AND TRAINING (DEVELOPMENT)*

- A User Manual or user guide must be produced in order to provide end-users with appropriate guidance on how to use the system developed. A new version of the User Manual should be produced after any major software change.
- Ensure the User Manual is stored in the Trial Master File and referenced in the Validation Plan (Appendix A).
- Ensure electronic copies are stored securely on the University network ensuring filenames include the relevant version number.
- If applicable, archive previous version.

2.8 PROGRAMMING STANDARDS*

Source code development standards should be specified to ensure the quality and consistency of software code. This should be stated during the design specification and used consistently throughout the development cycle.

- 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.

2.9 DOCUMENTATION SIGN-OFF AND RETENTION

- Upon satisfactory user-testing, ensure that a satisfactory completion hand-over document has been signed and filed with the validation documentation. This should be signed and dated by the Chief Investigator and the Developer. Complete Appendix D - Satisfactory Completion & Hand-over template.
- Ensure all validation documentation is signed by the Chief Investigator and stored in the Trial Master File.
- Ensure all versions of the validation documentation, both hard and soft copies, are retained in accordance with the University archiving policy.

2.10 RELEASE AND INSTALLATION

- A system release date must be agreed between the end-user and developer/software provider and documented in the Validation Plan.
- Post install checks must be made and documented to verify successful installations – see Section 3 below.

3 SYSTEM SET-UP AND INSTALLATION

The Chief Investigator or nominated/delegated authority is responsible for system set-up and installation.

3.1 SYSTEM CONFIGURATION

- 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.
- If system is delivered via a web browser ensure supplier recommended web browser version (e.g. Internet Explorer, Firefox, Chrome) is available and installed correctly for its use.
- Check whether appropriate system user rights are available to ensure successful installation. Workstation Administrator rights may be required for software installation onto client PC's.

3.2 SET-UP OPTIONS

- Follow guidelines from the supplier or vendor of the computer system being validated to ensure all appropriate set-up options have been completed as appropriate to the required use.
- Consider most appropriate delivery of client software such as workstation installation via Networked Applications (user-authenticated installation), or direct installation.

3.3 INSTALLATION TEST & DOCUMENTATION

- Complete the Installation Test Plan (Appendix C) and record any installation observations and tests conducted to evidence the system has been installed successfully.

4 USER ACCEPTANCE TESTING

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.

The Chief Investigator or nominated/delegated authority is responsible for user acceptance testing.

4.1 TESTING METHODOLOGY

- 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 patient' which can then be entered onto the system including expected data outputs. Different scenarios should be tested.
- Test scripts should also include boundary values or incorrect values to ensure any form or rule-based input validation works as expected.

4.2 TESTING SUCCESSES AND FAILURES

- Record all testing successes and failures in the Test Plan (Appendix C) including any remedial action required.
- Any test failures must be re-tested following the completion of the remedial action.

4.3 DOCUMENTATION DEVELOPMENT AND RETENTION

- Print and sign all User Acceptance Test documentation by the Chief Investigator or nominee.
- Ensure the User Acceptance Test documentation is stored in the Trial Master File and referenced in the Validation Plan (Appendix A).
- Refer to Section 1 for applicable document management procedures..
- If applicable, archive previous version.
- 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.

4.4 REPORTING AND SIGN-OFF

- Produce a brief management report including the outcome of the user acceptance tests conducted and the system fit for purpose for the given Clinical Trial. The Report must be stored in the Trial Master File and referenced in the Validation Plan (Appendix A).

4.5 ACCEPTANCE CRITERIA FOR AUTHORISATION OF A VALID SYSTEM FOR USE

- Ensure all criteria outlined in the requirement specification document (Appendix B) have been met by the provided system.
- Ensure all test scripts have been satisfactory completed.

4.6 FORMAL ACCEPTANCE OF THE SYSTEM

- Complete the User Acceptance Sign-Off template (Appendix F) which must be stored in the Trial Master File and referenced in the Validation Plan (Appendix A).

4.7 ONGOING VALIDATION

- Register and document any change requests by completing Appendix G Request for Change template to assess change requests and gain authorisation for the implementation of the change request.
- Re-validate any component of the system affected by the change request in a test environment.

5 TRAINING

A clinical trial may refer to their own Training SOP if appropriate.

The Chief Investigator or nominated/delegated authority is responsible for Training.

5.1 TRAINING REQUIREMENTS FOR STAFF INVOLVED IN THE VALIDATION OF COMPUTERISED SYSTEMS

- All staff involved in the validation of computer systems must be appropriately trained.

5.2 TRAINING RECORDS FOR COMPUTERISED SYSTEMS (MAY REFER TO A TRAINING SOP)

- All end-users must be appropriately trained in the computer system being validated
- All end-users must have training recorded in the training plan

6 SECURITY

The Chief Investigator or nominated/delegated authority is responsible for ensuring the system has an appropriate level of security in place.

6.1 PASSWORD ASSIGNMENT AND CHANGES

Ensure any access to the system and any password assignment is in accordance with the University's Regulations and Acceptable Use including:

- University IT Systems Password Policy (Schedule 7:
<http://www.cardiff.ac.uk/insrv/resources/regulationsandstrategy/insrvregulationsjuly2012.pdf>)
- University Permission to Connect to the IT Network Policy:
<http://www.cardiff.ac.uk/insrv/aboutus/regulations/index.html>

6.2 ACCESS AUTHORITY LEVELS AND THEIR REVIEW

- 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 Validation Plan (Appendix A).

6.3 PHYSICAL SECURITY

- Ensure any host system is secured appropriately (including workstations and servers) to prevent unauthorised access.
- Document a physical security protocol outlining how the system secured against unauthorised access or theft. Store this document in the Trial Master File and ensure it is referenced in the Validation Plan (Appendix A).

6.4 VIRUS CHECKING AND PREVENTION

- Ensure system is compliant with the University's anti-virus policy and the approved University's antivirus software is installed on the systems being used:
<http://www.cf.ac.uk/insrv/it/antivirus/index.html>
- Refer to the Information Services Regulations and Acceptable Use policies:
<http://www.cardiff.ac.uk/insrv/aboutus/regulations/>

7 SYSTEM USE AND MAINTENANCE

Clinical Trial Units should adapt this section according to local procedures.

The Chief Investigator or nominated/delegated authority is responsible for System Use and Maintenance

7.1 AN SOP FOR EACH SYSTEM

- Create a System Use and Maintenance SOP and include any maintenance or support contract for software and host systems.
- 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 Validation Plan (Appendix A).

8 USER SUPPORT

The Chief Investigator or nominated/delegated authority is responsible for user support.

8.1 SUPPORT/HELP FOR 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 Issue Log (Appendix H) including any support reference number, remedial action and date resolved.

8.2 USER MANUALS AND TRAINING (MAINTENANCE)

- Reference any user manuals and training material in the Validation Plan (Appendix A).
- Ensure any future releases of the computer system being implemented have up to date user manuals.

9 PROBLEM MANAGEMENT

The Chief Investigator or nominated/delegated authority is responsible for problem management

9.1 ISSUE LOG

- An Issue Log (Appendix H) must be maintained for each system being validated throughout the period of the Clinical Trial.
- Ensure the Issue Log is stored in the Trial Master File and referenced in the Validation Plan (Appendix A).

9.2 MONITORING AND RESOLUTION

- A nominated member of staff must be responsible for maintaining the Issue Log and ensure the Log is kept up to date and any resolutions noted including resolution date.
- Nominee must be named on the Issue Log (Appendix H) under 'Issue Log Owner'.

10 SYSTEM BACKUP AND RESTORATION

The Chief Investigator or nominated/delegated authority is responsible to ensure that an appropriate level of system backup and restoration procedures are in place.

10.1 ROUTINE BACKUPS

For data stored on systems other than the University shared drive (which is routinely backed up).

- Complete the System Backup Process template (Appendix I) and store this document in the Trial Master File and ensure it is referenced in the Validation Plan (Appendix A).

10.2 BACKUP LOG

For data stored on systems other than the University shared drive (which is routinely backed up).

- Maintain a backup log to include who and when backups are undertaken. This may be provided by electronic and automated backup logs.

10.3 RESTORATION OF SYSTEM AND DATA

- A restore procedure must be documented and referenced in the Validation Plan (Appendix A).
- The restore procedure may be part of an established SOP or disaster recovery plan, if so ensure it is referenced in the Validation Plan.

11 BUSINESS CONTINUITY

The Chief Investigator or nominated/delegated authority is responsible to ensure an appropriate business continuity procedure is in place.

11.1 SYSTEM RECOVERY IN THE EVENT OF A MAJOR DISASTER (MAY REFERENCE DISASTER RECOVERY PLAN)

- Ensure a disaster recovery plan exists for every system validated. Use Appendix J - System Disaster Recovery Template if one does not currently exist.
- Any disaster recovery document must be securely located with appropriate access control.
- Ensure the disaster recovery plan is referenced in the Validation Plan (Appendix A).

12 CHANGE MANAGEMENT

The Chief Investigator or nominated/delegated authority is responsible for change management.

12.1 DOCUMENTATION AND MAINTENANCE OF THE SYSTEM CONFIGURATION

- Any approved change request must be reflected in the Requirements Specification, Design Specification and any other relevant validation documentation. Amend these documents according to document control mechanisms (see section 4.3).

12.2 DOCUMENTATION, PRIORITISATION AND AUTHORISATION OF CHANGES TO VALIDATED SYSTEMS

- Register and document any change requests by completing Appendix G Request for Change template to assess change request and gain authorisation for the implementation of the change request.

12.3 DEVELOPMENT, TESTING, DOCUMENTATION AND REVIEW OF CHANGES

- Re-validate any component of the system affected by the change request in a test environment.
- Archive redundant source code and documentation.

12.4 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 and install the required change following the validation procedure outlined in this document.

13 PERIODIC REVIEW

The Chief Investigator or nominated/delegated authority is responsible for periodic review

13.1 REVALIDATION REQUIREMENTS

- Conduct and document a Periodic Review to ensure the system documentation is up to date and the validated system is functioning according to the Requirements Specification. The Validation Plan (Appendix A) should state who is responsible for the Periodic Review (business owner) and the frequency.
- Review of Issue Log to evaluate any reoccurring issues or major problems.
- Review user training and training records.
- Review Validation SOP and Validation Plan (Appendix A) and ensure all documentation is up to date.

13.2 RE-TESTING

- Reviewer should conduct and document an assessment of any risk identified by the periodic review and revalidate the system if necessary.

*SOP headings and titles were adapted from *Computerised Systems Validation in Clinical Research, A Practical Guide, 2nd Edition* (CR-CSV Working Party, Association for Clinical Data Management) 2004, Appendix 4.

APPENDIX A – VALIDATION PLAN TEMPLATE

Author:	Tim Cross		
Current Version:	0.1	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:

NAME OF COMPUTERISED SYSTEM:

**Bespoke Software / Database development only*

Validation Documentation	Date Completed	Document Location
Requirements Specification (Section 2.1, Appendix B)		
Functional Specification* (Section 2.2)		
Design Specification* (Section 2.3)		
Test Scripts (Section 4.1)		
Test Plan/Log (Sections 2.4, 4, Appendix C)		
Satisfactory Completion & Hand-over* (Appendix D)		
User Acceptance Sign-Off (Section 4.6, Appendix F)		
Produce Management Report (Section 4.4)		

Validation Documentation	Date Completed	Document Location
Request for Change (Sections 4.7, 12.2, Appendix G)		
Access Control List (Section 6.2)		
Physical Security of the System Protocol (Section 6.3)		
Create System Use and Maintenance SOP (Section 7.1)		
Issue Log (Sections 8.1, 9.1-9.2, Appendix H)		
User Manuals / Training Material (Section 8.2)		
System Backup Process (Section 10.1, Appendix I)		
Backup Log (Section 10.2)		
Restore Procedure (Section 10.3)		
Disaster Recovery Plan (Section 11.1, Appendix J)		

SYSTEM RELEASE

Agreed System Release (Provide description of what part(s) of the system is being released)	Date	Approved By
		<i>..continue as necessary</i>

PERIODIC REVIEW

Name of Reviewer:

Frequency of periodic review:

Reviewed By	Date Completed	Action Required
		<i>..continue as necessary</i>

APPENDIX B - REQUIREMENTS SPECIFICATION TEMPLATE

NAME OF TRIAL:

NAME OF COMPUTERISED SYSTEM:

Author: **Tim Cross**

Current Version:

0.1 Draft

Date:

16-Jan-2013

Approved By:

Date:

Position:

REVIEWED

Initials:

Date:

1	Requirement (Completed by the Chief Investigator or Nominee)
	Include the name of the trial. Outline in detail the requirement for a computer system (hardware or software) and how this is to be used within the trial and how this may impact on the integrity and quality of clinical data.
2	Needs Analysis (Completed by the Chief Investigator or Nominee)
	Is there a supported and validated University application or equipment that will meet the above requirement? (e.g. SPSS) Is there an off-the-shelf pre-validated computer system that will meet the above requirement? Is there a hardware requirement? (e.g. scanner, server). Is this currently available/suitable? Is there a software development requirement? Reference supporting documentation (such as proposal or needs analysis). Ensure all requirements are specified including post-trial requirements such as archiving, data lockdown, data preservation, retention period etc.

APPENDIX C – TEST PLAN / LOG TEMPLATE

Author:	Tim Cross		
Current Version:	0.1 Draft	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:

NAME OF COMPUTERISED SYSTEM:

If Test Script is used, note name and location of Test Script:

No	Date	Tested By	Screen, Form or Module Name	Success/Fail	Error Message or Observations	Action Required
1						
2						
3						

APPENDIX D - SATISFACTORY COMPLETION AND HAND-OVER TEMPLATE

Author:	Tim Cross		
Current Version:	0.1 Draft	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:

NAME OF COMPUTERISED SYSTEM:

To be completed by the developer.

The development of the modules, forms or database as listed below have been completed by the Developer including any post-testing issues identified and recorded in the Test Log. The modules, forms or database as listed below have been tested by the end-user and have been validated successfully (including re-testing following any issues identified during a previous test).

The End-User (business owner) is satisfied that the following modules, forms or database has passed user-testing and is fit for purpose as specified. The following modules, forms or database can be uploaded onto the production version:

Module / Form / Database	Version	Date

Signed Developer:

Date:

Signed End-User:

(Normally Chief Investigator)

Date:

APPENDIX E – INSTALLATION TEST LOG

Author:	Tim Cross		
Current Version:	0.1 Draft	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:**NAME OF COMPUTERISED SYSTEM:**

To validate a computer system has been successfully installed. Record any installation observations and tests conducted to evidence the system has been installed successfully. To be completed by the person installing the system.

Date	Installed By	System Installation Notes and Post-Installation Test	Success/Fail	Action Required

APPENDIX F – USER ACCEPTANCE SIGN-OFF TEMPLATE

Author:	Tim Cross		
Current Version:	0.1 Draft	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:**NAME OF COMPUTERISED SYSTEM:**

To be completed by the end-user, including for future releases, bug fixes, additional modules etc.

The development of the modules, forms or database as listed below have tested in accordance with the requirements specification including any post-testing issues identified and recorded in the Test Log. The modules, forms or database as listed below have been tested by using test scripts by the end-user and have been validated successfully (including re-testing following any issues identified during a previous test).

The End-User is satisfied that the following modules, forms or database has passed user-testing and is fit for purpose as specified. The following modules, forms or database can be released onto the production system:

Module / Form / Database	Version	Date

Signed End-User:

(Normally Chief Investigator)

Date:

APPENDIX G – CHANGE REQUEST TEMPLATE

Author:	Tim Cross		
Current Version:	0.1 Draft	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:

NAME OF COMPUTERISED SYSTEM:

RFC	Date Received	Change Description	Impact of Change	Approved /Declined (Include name and signature if approved)
1				
2				
3				
4				
etc				

RFC (Request For Change number)

APPENDIX H – ISSUE LOG TEMPLATE

Author:	Tim Cross		
Current Version:	0.1 Draft	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:

NAME OF COMPUTERISED SYSTEM:

Nominated Issue Log Owner:

No	Issue Date	Recorded By	Screen, Form or Module Name	Issue Description (Include any error message)	Remedial Action (Include any support reference number)	Date Resolved
1						
2						
3						

APPENDIX I – SYSTEM BACKUP PROCESS TEMPLATE

Author:	Tim Cross		
Current Version:	0.1 Draft	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:

NAME OF COMPUTERISED SYSTEM:

1	Type of Backup
	Describe the type of backup and the medium used. Include whether backup is a complete system backup, data backup or incremental.
2	Backup Routine
	Describe the regularity and routine of the backup. Include who is responsible for conducting the backup. Describe the retention policy.
3	Backup Log
	Describe how a log of the backup is to be maintained.

APPENDIX J – SYSTEM DISASTER RECOVERY TEMPLATE

Author:	Tim Cross		
Current Version:	0.1 Draft	Date:	16-Jan-2013
Approved By:	Date:		
Position:			
REVIEWED			
Initials:	Date:		

NAME OF TRIAL:

NAME OF COMPUTERISED SYSTEM:

Directory No	Service Name	
1.a (example)		
Service Description (include dependencies, critical files, data store etc.)		
Account Name	Account Password	Account Description
		Add more rows if necessary
Backup Procedure (include types of backup, critical files, location etc.)		

Restore Procedure		
Directory Version	Date / By Whom	Comments