St George's University Hospitals NHS
NHS Foundation Trust

Standard Operating Procedure (SOP)

SOP ID number:	JREOSOP0024	**Effective Date:**	02/11/2015
Version number and date:	Version Two, 30/10/2015	**Review Date:**	02/11/2017
Author:	Mallikarjuna Rao Vemula (Arjun)	**Title:**	Clinical Trials Monitor
Approved by:	Lucy H H Parker	**Date:**	30/10/2015
Signature of Authorisor			

This is a controlled document.
The master document is posted on the JREO website and any print-off will be classed as uncontrolled.

Researchers and their teams are responsible for checking the JREO website for the most recent version.
They may print off this document for training and reference purposes.

Standard Operating Procedure (SOP)

Computerised Systems

SOP Chronology		
SOP Version Number:	**Reason for Change:**	**Author:**
Draft v1.0	New SOP	Lucy H H Parker
V2.0	Updated trust name; trust logo; newly added information	Mallikarjuna Rao Vemula (Arjun)

© St George's

Table of Contents	Page
1. Background	3
2. Joint Research and Enterprise Office (JREO) Policy	3
3. Scope	3
4. Definitions 4.1 Calidcott Guardian	4 4
5. Responsibilities	4
6. Procedures 6.1 Purchasing and evaluation 6.2 Validation 6.3 Implementation 6.4 Disaster Recovery/Back Up plans	4 4 5 5 5
7. References	5
8. Appendices NA	5

© St George's

1. Background

It is the responsibility of the Chief Investigator (CI) in the clinical trial to ensure that any computerised system used during the study complies with both St George's University and St George's Trust policies as well as any applicable EU and UK regulations.

Any data that is stored on SGUL networked computers, laptops, tablets, iCloud, smart watches, smart phones or Personal Digital Assistants (PDAs) must be stored in an anonymised form with no identifiable information. Users have a duty of care to protect the confidentiality of any information which they might access through the university network in the course of legitimate employment activities or through academic studies.

Patient identifiable data must be stored on NHS systems unless the patient has given explicit consent for it to be stored outside the NHS Trust. This will also need to be highlighted in the ethics application and applicable supporting documentation. Any system holding identifiable data should be sufficiently secure and should be assessed by the department Data Protection Officer and comply with the university's data protection policy. In a clinical trial CI/ PI wish to access patient data without consent they should obtain permission from the Confidentiality Advisory group (CAG).

2. Joint Research and Enterprise Office (JREO) Policy

All JREO SOPs will be produced and approved in accordance with the JREO SOP on SOPs and must be used in conjunction with local NHS Trust and St George's policies and procedures.

The JREO acts as the representative of both St George's University of London (SGUL) and St George's University Hospitals NHS Foundation Trust (SGHT). St George's will be the official name used on all SOPs to represent both institutions acting as Sponsor.

3. Scope

This Standard Operating Procedure (SOP) will focus on computerised systems that St George's University Hospitals NHS Foundation Trust (SGHT) or St George's, University of London (SGUL) may utilise as Sponsor of a clinical trial and as such, will not be a list of all computerised systems used in clinical trials. Information and Communication Technology (ICT) at SGUL maintains a

© St George's

database of all registered information systems connected to the University network. ICT at SGHT also maintains a database of all registered information systems connected to the Trust network.

4. Definitions

4.1 Caldicott Guardian

The definition of Caldicott Guardian according to the Department of Health (DoH) is "a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing". Each NHS organisation is required to have a Caldicott Guardian; this was mandated for the NHS by Health Service Circular: HSC 1999/012. The Guardian plays a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information.
The Caldicott Guardian for St George's Hospital is the Medical Director- Dr Simon Mackenzie.

5. Responsibilities

This SOP is to be followed by the Chief Investigator (CI) of the proposed study.

6. Procedure

6.1 Evaluation and Purchasing

It is the CI's responsibility to ensure that any computerised systems that are used for clinical trial research are compliant with SGUL or SGHT ICT policies. If in doubt, the CI should contact the relevant ICT department for advice and guidance.

6.2 Validation

The CI must ensure when using electronic systems to capture trial data that the system conforms to established requirements for completeness, accuracy, reliability and consistent intended performance (i.e. validation) ICH GCP 5.5.3a. This should be documented (Refer to JREOSOP0038 Data Management).

6.3 Implementation

Any CI of a study who wishes to use new computerised systems (as opposed to systems already approved) must seek the approval from the relevant Trust and their Caldicott Guardians as well

© St George's

as SGUL to ensure compliance with both Trust and University policies in addition to applicable EU and UK regulations.

ICT at SGUL may be able to aid with implementation of the computerised system if the software is supported for use on Windows (https://portal.sgul.ac.uk/org/lis/computing-services/helpdesk/forms/software/software-request-forms)

The CI must also ensure that there are appropriate SOPs for the chosen computerised system.

6.4 Disaster Recovery/Backup Plans

The CI has the responsibility for the collection of data either remotely on a server or on a hard disk and should consult with ICT regarding the existence of local back-up systems (to guard against loss of data due to software and environment disasters) and disaster recovery procedures.

If the CI does not use the facilities provided by ICT or those at the local Trust, he/she must put into place his/her own procedures. See https://portal.sgul.ac.uk/org/lis/computing-services/policies/pdfs/SOP_InfoSecurity.pdf for further information.

7. References

ICH GCP 1996
SGUL ICT policies - https://portal.sgul.ac.uk/org/lis/computing-services/policies
http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563
JREOSOP0038

8. Appendices

Not applicable to this SOP

© St George's