Nova Southeastern University
Standard Operating Procedure for GCP

Title: Electronic Source Documents for Clinical Research Study		Version # 1
SOP Number: OCR-RDM-006	**Effective Date: August 2013**	**Page 1 of 8**

PURPOSE: The participation of a patient in the clinical trial and all other study relevant data have to be documented in the source notes according to the instructions in the respective Clinical Trial Protocol.

POLICY: Source data verification (SDV) on electronic records can only be done, if the system is validated, a clear audit trail exists and the access to patient files can be limited to patients participating in the respective clinical trial (21 CFR, Part 11 compliant).

DEFINITIONS

Certified Copy: A certified copy is a copy of original information that has been verified, as indicated by a dated signature, as an exact copy having all of the same attributes and information as the original.

Source Documents: Original documents and records including, but not limited to, hospital records, clinical and office charts, laboratory notes, subject's diaries or evaluation checklists, pharmacy dispensing records, recorded data from automated instruments, copies or transcriptions certified after verification as being accurate and complete, magnetic media, x-ray, subject files, and records kept at the pharmacy, at the laboratories, and at medico-technical departments involved in a clinical trial.

Original data: For the purpose of this guidance, *original data,* are those values that represent the first recording of study data. FDA is allowing original documents and the original data recorded on those documents to be replaced by copies provided the copies are identical and have been verified as such. (FDA compliance Policy Guide #7150.13)

If a computer system is used by the site for recording, reporting and storing data, please consider:

1. Validated System with Audit Trails, such as Nexgin or Axiom which fulfil the 21 CFR part 11 requirements. In this case there is no need to print out patient files. The electronic records on the computer serves as the source documents.

2. System is not Validated and does not have Audit Trail

The patient files *must be printed, initialled and dated by the investigator or designee, preferably per visit, indicating that the paper file represents the patients' complete medical record and is an accurate representation of the electronic file.*

Source data verification will be conducted using the patients' paper file printed by the investigator or designee. From the patients' paper file that has been used for source data verification, the Sponsor representative (CRA) will compare a sample of the patients' paper file to the electronic patient file, to assess the completeness and accuracy of the printed patients' paper files. For each monitoring visit, after the SDV has been completed the electronic source print outs must be initialled/signed and dated by the CRA. It is also allowed to use a stamp with date and the name of the CRA for this purpose.

Use of electronic medical records for clinical research according 21 CFR Part 11

If College/Center intends to use e-records without printouts the following must be in place:

Electronic source files are properly managed

a. Validation of system to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records:	*Validation documentation (validation certificate or validation reports or at least installation tests) are available. Change control is ensured (at least system maintenance reports available). Contact person for system support is easily available.*
b. Ability to generate accurate and complete	*All elements of the e-*

copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency:	*patient file (including audit trail) are printable or transferable to another media to make it human readable.*
c. Protection of records to enable their accurate and ready retrieval throughout the records retention period:	*Regular backup process or other safety measure implemented. Data should be backed up at regular intervals (preferably at least weekly) to prevent the risk of losing data in the event of the system being damaged or stolen. Stored data should be kept separately from the computer system in a secure area to ensure data reconstruction in the event of source being lost. Either backup log book or backup media should be available for verification.* *Long term archival of electronic data (including audit trail) ensured.* *System data and audit trails are source documents, and must be retained for a*

period as agreed for all source documents (a minimum period of 15y is recommended) and must be available for regulatory review. Electronic source should be retained on media that will allow readability in the future.

d. Limiting system access to authorized individuals:

System access protected by unique usernames and passwords Unauthorized individuals should not be able to gain access to patient records or other study data i.e. a password is required to enter the system and access data. (Passwords noted e.g. on Post-It stickers indicate insufficient procedural control).

e. Use of secure, computer-generated, time-

stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	*(Minimum retention period of 15 years is recommended)*
f. Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate:	*Changes/deletions without audit trail should not be possible. There should be no possibility to switch off the audit trail.*
g. Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand:	*Each user should have a unique ID and password; these should not be shared.*
h. Use of device (e.g., terminal) checks to	*Data transfer from other systems (e.g. laboratory data) is safe and validated*

determine, as appropriate, the validity of the source of data input or operational instruction:	*(subject identifier checked, plausibility checks etc.)*
i. Determination that persons who develop, maintain, or use electronic record/electronic signature system have the education, training, and experience to perform their assigned tasks:	*All staff members using the system are trained, training documentation is available.*
j. The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification:	*Policy established that ID and passwords are not to be shared and that staff members are accountable for their electronic documentation.*

k. Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation:	*User manual / User Guide or SOP regarding use of the system is available to all users and is kept up-to date.*
Additional measures:	
l. System is in a secure area (e.g. secured against theft):	*The investigator should be aware of the risk of theft/damage and should have implemented precautional measures (e.g. Lock).*
m. Direct access for sponsor representatives available (read only or supervised and limited to trial subjects).	
n. Virus protection ensured:	*Systems should not be connected to any other systems (e.g. Internet) or virus protection software should be always on.*

Printouts need to be provided in case any of the above 21 CFR part 11 checklist items are not applied.

The printout must be signed and dated by the investigator or designee.