REQUIREMENTS FOR ELECTRONIC SYSTEMS FOR USE IN CLINICAL RESEARCH

INTRODUCTION

This appendix addresses how the elements of data quality might be satisfied where electronic systems are being used to create, modify, maintain, archive, retrieve, or transmit research study data.

1.0 SECURITY

Internal and external safeguards should be built into the electronic system, to ensure that access to the computerized system and to the data is restricted to only authorized personnel.

a. Physical Security

Staff should be thoroughly aware of system security measures and the importance of limiting access to authorized personnel. SOPs should be in place for handling and storing the system to prevent unauthorized access.

b. Authority Checks

The system must authorize users before allowing them to access or alter records. Access must be limited to authorized to individuals based on Role and Privilege. This may include different levels of security within the system. The system should limit and record the number of unauthorized log-in attempts. Automatic log off for long idle periods.

c. Access control

Access Control limiting system access to persons who have documented training and authorization with their own log-on and password. The electronic data entry system should be equipped with authentication mechanism such as combined identification codes/passwords or biometric-based electronic signatures, at the start of a data entry session. Passwords or other access keys should be changed at established intervals.

1.1 External Checks

System controls must prevent unauthorized external software applications from altering, browsing, querying, exporting or reporting data. Steps must be taken to prevent, detect and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software.

a. Logical Security

Access to the data should be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail. There should be a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. The record should be in the study documentation and be accessible. Controls should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.

b. Device Checks

The ability of the system to perform an input check to ensure the source of the data being input is valid. This means that data is restricted to particular input device or sources. Data should not be entered into a regulated computer system without the owner knowing the source of the data. In other words, device has controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.

1.2 Operational Checks

Computer systems will have sufficient controls or operational system checks to ensure that users must follow required procedures. If it is necessary to create, delete, or modify records in a sequence, explain how operational system checks will ensure that the proper sequence of events is followed.

a. Audit Trail

Computer generated; time stamped electronic audit trails are the preferred method for tracking the changes. Digital changes to the data must not obscure or delete the original entry, allowing others (including DAIDS monitors) to view both original and corrected electronic data. Alternatively, the corrected electronic record should be clearly labeled as such for future access ensuring that audits cannot be overridden.

Section 21 CFR 11.10(e) requires persons who use electronic record systems to maintain an audit trail as one of the procedures to protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records.

Audit trails must be secure, computer-generated, time-stamped to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.

Audit trails must be retained for a period at least as long as required unless dictated otherwise by the protocol and must be available for review and copying.

Personnel who create, modify, or delete electronic records should not be able to modify the audit trails and should retain either the original or a certified copy of audit trails. Regulatory authorities should be able to read audit trails both at the study site and at any other location where associated electronic study records are maintained.

Audit trails should be created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data.

b. Date/Time Stamps

Controls should be in place to ensure that the system's date and time are correct. The ability to change the date or time should be limited to authorized personnel and such personnel should be notified if a system date or time discrepancy is detected. Changes to date or time should be documented. Dates and times are to be local to the activity being documented and should include the year, month, day, hour, and minute. It is advised to either utilize a Network Time Protocol (NTP) time server or synchronize systems to the date and time provided by trusted third parties.

Calculation of the local time stamp may be derived in some cases from a remote server located in a different time zone.

2. VALIDATION

A process of establishing and documenting that the specified requirements of a computerized system can be consistently fulfilled from design until decommissioning of the system or transition to a new system. The approach to validation should be based on a risk assessment that takes into consideration the intended use of the system and the potential of the system to affect human subject protection and reliability of trial results. (ICH GCP E6 (R2)).

The validation process must have written design specification that describes what

the software is intended to do and how it is intended to do it. A written test plan based on the design specification, including both structural and functional analysis; and, Test results and an evaluation of how these results demonstrate that the predetermined design specification has been met for the validation.

For software purchased off-the-shelf, most of the validation should have been done by the company that wrote the software. The organization should have documentation (either original validation documents or on-site vendor audit documents) of this design level validation by the vendor, and should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.

In the special case of database and spreadsheet software that is (1) purchased off-the-shelf, (2) designed for and widely used for general purposes, (3) unmodified, and (4) not being used for direct entry of data, the sponsor or contract research organization may not have documentation of design level validation. However, the organization should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.

The user acceptance testing (UAT) should be accomplished through either actual or simulated use of the software being tested within the context in which it is intended to function. UAT should follow a pre-defined written plan with a formal summary of testing and a record of formal acceptance. Documented evidence of all testing procedures, test input data, and test results should be retained.

3. SYSTEM DEPENDABILITY

The sponsor should ensure and document that computerized systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance.

a. Systems documentation

System documentation should be readily available at the site where clinical trials are conducted. Such documentation should provide an overall description of computerized systems and the relationship of hardware, software, and physical

environment.

Documentation should identify what software and hardware will be used to create, modify, maintain, archive, retrieve, or transmit clinical data. This documentation should be retained as part of the study records and be available either on-site or be remotely accessible.

b. Change Control

Written procedures should be in place to ensure that changes to the computerized system such as software upgrades, equipment or component replacement, or new instrumentation will maintain the integrity of the data or the integrity of protocols.

The impact of any change to the system should be evaluated and a decision made regarding the need to revalidate. Revalidation should be performed for changes that exceed operational limits or design specifications. All changes to the system should be documented.

4. SYSTEM CONTROLS

a**.** Software Version Control

Measures should be in place to ensure that versions of software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.

b. Contingency Plans

Written procedures should describe contingency plans for continuing the study by alternate means in the event of failure of the computerized system.

c. Backup and Recovery of Electronic Records

Backup-Restore and disaster recovery procedures should be clearly outlined in the SOPs and be sufficient to protect against data loss. Records should be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data. Backup records should be stored at a secure location specified in the SOPs. Storage is typically offsite or in a building separate from the original records. Backup and recovery logs should be maintained to facilitate an assessment of the nature and scope of data loss resulting from a system failure. This documentation should address business continuity (temporary outage) as well as disaster recovery.

5. SYSTEM FEATURES

Systems used for direct entry of data should be designed to include features that will facilitate the direct inspection and review of data.

Prompts, flags, or other help features within the computerized system should be used to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. Features that automatically enter data into a field when that field is bypassed should not be used. Data tags (e.g., different color, different font, flags) should be used to indicate which data have been changed or deleted, as documented in the audit trail.

a. Retrieval of Data

Recognizing that computer products may be discontinued or supplanted by newer (possibly incompatible) systems, it is nonetheless vital that there is the ability to retrieve and review the data recorded by the older systems. This may be achieved by maintaining support for the older systems or transcribing data to the newer systems. When migrating to newer systems, it is important to generate accurate and complete copies of study data and collateral information relevant to data integrity. This information would include, for example, audit trails and computational methods used to derive the data. Any data retrieval software, script, or query logic used for manipulating, querying, or extracting data for report generating purposes should be documented and maintained for the life of the report. The transcription process needs to be validated.

b. Reconstruction of Study

Regulatory authorities expect to be able to reconstruct a study. This applies not only to the data, but also how the data were obtained or managed. Therefore, all versions of application software, operating systems, and software development tools involved in processing of data or records should be available as long as data or records associated with these versions are required to be retained.

c. Electronic Informed Consent (eIC)**:**

The computerized system used in eIC must be secure with restricted access and have methods to protect the participant's confidentiality (e.g., encryption). eIC process should incorporate procedures that electronic documents can be archived and

retrieved.

d. Electronic Signature (eSignature):

An electronic signature is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Electronic records that are electronically signed must contain information associated with the signing that clearly indicates the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature. The name, date and time, and meaning are subject to the same controls as electronic records and must be included as part of any human readable form of the electronic record. In addition, electronic signatures and handwritten signatures executed to electronic records must be linked to the respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. The electronic system must also capture and record the date that the subject or subject's legally authorized representative (LAR) provides consent (if applicable).

6. TRAINING OF PERSONNEL

Those who use computerized systems must determine that individuals (e.g., employees, contractors) who develop, maintain, or use computerized systems have the education, training and experience necessary to perform their assigned tasks. Training should be provided to individuals in the specific operations about computerized systems that they are to perform.

Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the study. It is recommended that computer education, training, and experience be documented at the organization that owns the computer system.

System users (including system administrators) will: Be trained before they are assigned tasks in the system. Documentation of system training will include of a listing of: trainee

name(s), date of training, name of trainer, title of course, and primary contents covered in the training.
System users must maintain documentation of the training. System administrators should disable the user access if an individual user discontinues involvement during the study or is not up to date with required training.

7. STANDARD OPERATING PROCEDURES

Standard Operating Procedures (SOPs) pertinent to the use of the computerized system should be available on site. SOPs should be maintained either on-site or be remotely accessible through electronic files as part of the specific study records, and the SOPs should be made available for use by personnel and for inspection by Regulatory authorities.
SOPs should be established for, but not limited to:

- System Setup/Installation
- Data Collection and Handling
- System Maintenance
- Data Backup, Recovery, and Contingency Plans
- Security
- Change Control
- Access and Authentication
- Information Security
- Data Integrity.

a. INTEROPERABILITY AND INTEGRATION OF SYSTEMS

For the purposes of this appendix, interoperability refers to the ability of two or more products, technologies, or systems to exchange information and to use the information that has been exchanged without special effort on the part of the user. EHR and EDC systems may be noninteroperable, interoperable, or fully integrated, depending on supportive technologies and standards.

b. Noninteroperable systems:

Without the capability for electronic exchange of EHR data in clinical investigations, involve manual transcription of data elements from the EHR to the eCRF or to the paper case report form, similar to the transcription performed with paper records. Such manual transcription procedures may introduce risks of data entry errors unless effective quality control systems are in place.

c. Interoperable systems

Allow electronic transmission of relevant EHR data to the EDC system. For example, data elements originating in an EHR (e.g., demographics, vital signs, laboratory data, medications) may automatically populate the eCRFs within an EDC system. In addition, an interoperable EHR and EDC system could provide access to additional patient information populated from other clinical information systems (e.g., radiology information systems, laboratory information systems). Interoperable systems may simplify data collection for a clinical investigation by enabling clinical investigators and study personnel to capture source data at the patient's point-of-care visit. Interoperable systems may also reduce errors in data transcription, allowing for the improvement in data accuracy and the quality and efficiency of the data collected in clinical investigations.

8. Fully integrated systems

Allow clinical investigators to enter research data directly into the EHR. This may involve, for example, use of research modules, use of research tabs built into the EHR system, or use of custom research fields within the EHR system for data that are entered for research purposes.

a. Data Standards:

The data exchange between EHR and EDC systems should leverage the use of existing open data standards, when possible, while ensuring that the integrity and security of data are not compromised.

b. Validation of Interoperable systems:

Interoperability of EHR and EDC systems (e.g., involving the automated electronic transmission of relevant EHR data to the EDC system) functions in the manner intended in a consistent and repeatable fashion and that the data are transmitted accurately, consistently, and completely must be ensured. Software updates to the EDC systems must not affect the

integrity and security of EHR data transmitted to the EDC systems. *Refer to Validation section as well.*

c. Data from Multiple EHR Systems:

The EHR system at the clinical investigation site may be interoperable with multiple EHR systems from many different health care organizations or institutions that are not affiliated with the clinical investigation site. If data from multiple EHR systems from different health care organizations and institutions are integrated with EHR data at the clinical investigation site, data from another institution's EHR system may be used and transmitted to the EDC system if data sharing agreements are in place.

9. SOURCE DOCUMENTATION AND RECORDS RETENTION:

The electronic system in use must have the ability to retain records in compliance with applicable regulations and to be available for inspection. When original observations are entered directly into a computerized system, the electronic record is the source document. This requirement applies to the retention of the original source document, or a copy of the source document. When source data are transmitted from one system to another, or entered directly into a remote computerized system (e.g., data are entered into a remote server via a computer terminal that is located at the clinical site), or an electrocardiogram at the clinical site is transmitted to the sponsor's computerized system, a copy of the data should be maintained at another location, typically at the clinical site but possibly at some other designated site.

Copies should be made contemporaneously with data entry and should be preserved in an appropriate format, such as XML, PDF or paper formats. Regulatory authorities may inspect all records that are intended to support submissions to the Agency, regardless of how they were created or maintained. Therefore, systems should be able to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying.

REFERENCES:

1. ICH E6 (R2) Good Clinical Practice: Integrated Addendum to International Conference of Harmonization (ICH) E6 (R1)
2. **FDA** General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002
3. FDA Guidance for Industry, Electronic Source Data in Clinical Investigations, 2013
4. FDA Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers; Guidance for Industry DRAFT GUIDANCE June 2017
5. FDA Guidance for Industry, Electronic Records: Electronic Signatures – Scope and Application, 2003
6. FDA Guidance for Industry - COMPUTERIZED SYSTEMS USED IN CLINICAL TRIALS, 1999
7. FDA Use of Electronic Informed Consent in Clinical Investigations, Questions and Answers, 2015

REVISION HISTORY

APP-A15-OPC-005.00 is the original version of this Appendix.