Table of Contents

REQUIREMENTS FOR ELECTRONIC INFORMATION SYSTEMS FOR USE IN CLINICAL RESEARCH

INTRODUCTION

This appendix details the elements necessary to ensure electronic information systems used in the conduct of NIAID DAIDS Network studies conducted within the Clinical Trials Networks, unless otherwise specified in a formal agreement, comply with FDA, EMA, and other regulatory authority requirements, as applicable.

1.0 SECURITY

Maintain a security system that prevents unauthorized access to the data. Threats and attacks on systems containing clinical trial data and corresponding measures to ensure security of such systems are constantly evolving, especially for systems and services being provided over or interfacing the internet. [10]

Maintain the security of a system that ensures the protection of records to enable their accurate and ready retrieval throughout the records retention period.[9]

Staff should be thoroughly aware of system security measures and the importance of limiting access to authorized personnel.

a. Access Control

Access controls are integral to limit system access to authorized users and to ensure attributability to an individual.

The system must authorize users before allowing them to access, alter, or sign records.[9]

Access must be limited to authorized individuals based on role and privilege and may include different levels of security within the system.

Privilege should be granted based on the least-privilege rule, i.e., users should have the fewest privileges and access rights for them to undertake their required duties for as short a time as necessary.[10]

System access must be limited to persons who have documented training and authorization with their own individual user account traceable to a named owner. [9, 10]

b. User Management

A documented process must be in place to grant, change and revoke system accesses in a timely manner as people start, change, and end their involvement/responsibility in the management and/or conduct of the clinical trial projects. [10]

c. User Reviews

Data should be attributable to the person and/or system generating the data. Based on the criticality of the data, it should also be traceable to the system/device, in which the data were generated/captured. The information about originator (e.g., system operator, data originator) and system (e.g., device, process) should be kept as part of the metadata. [10]

Where treatment-related pertinent information is captured first in a direct data capture tool such as a trial participant diary, a PRO form or a special questionnaire, a documented procedure should exist to transfer or transcribe information into the medical record, when relevant.[10]

Direct data capture can also be done by automated devices such as wearables or laboratory or other technical equipment (e.g., medical imaging, electrocardiography equipment) that are directly linked to a data acquisition tool. Such data should be accompanied by metadata concerning the device used (e.g., device version, device identifiers, firmware version, last calibration, data originator, timestamp of events).[10]

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.

The system should record changes to user roles and thereby access rights and permissions.[10] At any given time, an overview of current and previous access, roles and permissions should be available from the system.[10]

This information concerning actual users and their privileges to systems should be verified at suitable intervals to ensure that only necessary and approved users have access and that their roles and permissions are appropriate. There should be timely removal of access no longer required, or no longer permitted.[10]

d. Physical Security

Computerised systems, servers, communication infrastructure and media containing clinical trial data should be protected against physical damage, unauthorized physical access, and unavailability.[10]

e. Firewalls

System controls must prevent unauthorized external software applications from altering, browsing, querying, exporting, or reporting data.

In order to provide a barrier between a trusted internal network and an untrusted external network, and to control incoming and outgoing network traffic, firewall rules should be defined. These should be defined as strict as practically feasible, only allowing necessary and permissible traffic.[10]

As firewall settings tend to change over time firewall rules and settings should be periodically reviewed. This should ensure that firewall settings match approved firewall rules and the continued effectiveness of a firewall.[10]

f. Vulnerability Management

Relevant security patches for platforms and operating systems should be applied in a timely manner, according to vendor recommendations.[10]

g. Platform Management

Platforms and operating systems for critical applications and components should be updated in a timely manner according to vendor recommendations, in order to prevent their use in an unsupported state.[10]

h. Bi-Directional Devices

The use of bi-directional devices (e.g., USB devices), which come from or have been used outside the organization, should be strictly controlled as they may intentionally or unintentionally introduce malware and impact data integrity, data availability, and rights of trial participants. [10]

i. Anti-Virus Software

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.

Anti-virus software should be installed and activated on systems used in clinical trials. The anti-virus software should be continuously updated with the most recent virus definitions in order to identify, quarantine, and remove known computer viruses. This should be monitored. [10]

j. Penetration Testing

For systems facing the internet, penetration testing should be conducted at regular intervals in order to evaluate the adequacy of security measures and identify vulnerabilities in system security including the potential for unauthorized parties to gain access to and control of the system and its data. [10]

k. Intrusion Detection and Prevention

An effective intrusion detection and prevention system should be implemented on systems facing the internet. [10]

l. Internal Activity Monitoring

An effective system for detecting unusual or risky user activities (e.g., shift in activity pattern) should be in place. [10]

m. Security Incident Management

Organizations managing clinical trial data should have and work according to a procedure that defines and documents security incidents, rates the criticality of incidents, and where applicable, implements effective corrective and preventive actions to prevent recurrence. [10]

In cases where data have been, or may have been, compromised, the procedures should include ways to report incidents to relevant parties where applicable. When using a service provider, the agreement should ensure that incidents are escalated to the sponsor in a timely manner.[9, 10]

n. Authentication Method

The method of authentication in a system should positively identify users with a high degree of certainty. A minimum acceptable method would be user identification and a password. The need for more stringent authentication methods should be determined based on a risk assessment of the criticality of the data and generally should include two-factor authentication. [10]

User accounts should be automatically locked after a pre-defined number of successive failed authentication attempts, either for a defined period of time, or until they are re-activated by a system administrator after appropriate security checks. [10]

o. Password Policies

Passwords or other access keys should be changed at established intervals.[9]

System should limit and record the number of unauthorized log-in attempts.

Formal procedures for password policies should be implemented. The policies should include but not necessarily be limited to length, complexity, expiry, login attempts, and logout reset. The policies should be enforced by systems and verified during system validation. [10]

p. Inactivity Logout

Systems should include an automatic inactivity logout, which logs out a user after a defined period of inactivity. The user should not be able to set the inactivity logout time (outside defined and acceptable limits) or deactivate the functionality. Upon inactivity logout, a re-authentication should be required (e.g., password entry). [10]

q. Device/Edit 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. [9]

Computerised systems should validate manual and automatic data inputs to ensure a predefined set of validation criteria is adhered to. Edit checks should be relevant to the protocol and developed and revised as needed. Edit checks should be validated, and implementation of the individual edit checks should be controlled and documented. [10]

r. 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. [9]

s. Audit Trail

Audit trails must be secure, computer-generated, and time-stamped to independently record the date and time of operator entries and actions that create, modify, or delete electronic records and must not obscure previously recorded information. [9]

Audit trails must be retained for a period at least as long as required for the subject electronic record unless dictated otherwise by the protocol and must be available for review and copying. [9]

An audit trail should be enabled for the original creation and subsequent modification of all electronic data.[10]

An audit trail is essential to ensure that changes to the data are traceable. Audit trails should be robust, and it should not be possible for 'normal' users to deactivate them. If possible, for an audit trail to be deactivated by 'admin users,' this should automatically create an entry into a log file (e.g., audit trail). Entries in the audit trail should be protected against change, deletion, and access modification (e.g., edit rights, visibility rights). The audit trail should be stored within the system itself. The responsible investigator, sponsor, and inspector should be able to review and comprehend the audit trail, and therefore audit trails should be in a human-readable format. [10]

Audit trails should be visible at data-point level in the live system, and it should be possible to export the entire audit trail as a dynamic data file to allow for the identification of systematic patterns or concerns in data across trial participants, sites, etc. The audit trail should show the initial entry and the changes (value - previous and current) specifying what was changed (field, data identifiers) by whom (username, role, organization), when (date/timestamp) and, where applicable, why (reason for change). [10]

For certain types of systems (e.g., ePRO) the data entered may not be uploaded immediately but may be temporarily stored in local memory. Such data should not be edited or changed without the knowledge of the data originator prior to saving. Any changes or edits should be acknowledged by the data originator, should be documented in an audit trail and should be part of validation procedures. The timestamp of data entry in the capture tool (e.g., eCRF) and timestamp of data saved to a hard drive should be recorded as part of the metadata. The duration between initial capture in local memory and upload to a central server should be short and traceable (i.e., transaction time), especially in case of direct data entry. [10]

Data extracts or database extracts for internal reporting and statistical analysis do not necessarily need to contain the audit trail information. However, the database audit trail should capture the generation of data extracts and exports. [10]

Audit trails should capture any changes in data entry per field and not per page (e.g., eCRF page). [10]

t. Audit Trail Review

Procedures for risk-based trial specific audit trail reviews should be in place and performance of data review should be generally documented. Data review should focus on critical data. Data review should be proactive, and ongoing review is expected unless justified. [10]

u. Timestamp

Controls should be in place to ensure that the system's date and time are correct.

Accurate and unambiguous date and time information given in coordinated universal time (UTC) or time and time zone (set by an external standard) should be automatically captured. [10]

Users should not be able to modify the date, time and time zone on the device used for data entry, when this information is captured by the computerized system and used as a timestamp. [10]

2.0 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. [1, 9]

Refer to *FDA General Principles of Software Validation* [2] for full software development life cycle requirements necessary when developing software (e.g., in-house developed software, custom developed software).

a. User Requirements

Critical system functionality implemented and used in a clinical trial should be described in a set of user requirements or use cases, e.g., in a user requirements specification (URS). This includes all functionalities, which ensure trial conduct in compliance with ICH E6 and which include capturing, analyzing, reporting and archiving clinical trial data in a manner that ensures data integrity. User requirements should include, but may not be limited to operational, functional, data integrity, technical, interface, performance, availability, security, and regulatory requirements. The above applies independently of the sourcing strategy of the responsible party or the process used to develop the system. [10] [In-house software, Purchased software – run locally, or SaaS software]

b. Traceability Matrix

Traceability should be established and maintained between each user requirement and test cases or other documents or activities, such as standard operating procedures, as applicable.

This traceability may have many forms and the process may be automated by software. It should be continuously updated as requirements are changed to ensure that where applicable, for every requirement, there is a corresponding test case or action, in line with the risk evaluation. [10]

c. Validation Plan

Validation activities should be planned, documented, and approved. The validation plan should include information on the validation methodology, the risk-based approach taken and if applicable, the division of tasks between the responsible party and a service provider. [10]

d. Test Cases

Test cases should be pre-approved. They may have many formats and while historically consisting of textual documents including tables with multiple columns corresponding to the elements below, they may also be designed and contained in dedicated test management systems, which may even allow automatic execution of test cases (e.g., regression testing). However, expectations to key elements are the same.

Test cases should include:

- the version of the software being tested;
- any pre-requisites or conditions prior to conducting the test;
- a description of the steps taken to test the functionality (input);
- the expected result (acceptance criteria).

Test cases should require the tester to document the actual result as seen in the test step, the evidence if relevant and, if applicable, the conclusion of the test step (pass/fail). [10]

Where relevant, the access rights (role) and the identification of the person or automatic testing tool performing tests should be documented.

e. Validation Report

The validation report should be approved by the responsible party before release for production. [10]

f. Vendor Provided Validation Documentation

The responsible party may rely on validation documentation provided by the vendor of a system if they have assessed the validation activities performed by the vendor and the associated documentation as adequate; however, they may also have to perform additional validation activities based on a documented assessment. [10]

If the responsible party relies on the vendor's validation documentation, inspectors should be given access to the full documentation and reporting of the responsible party's examination of the vendor. If this examination is documented in an audit report, this may require providing access to the report. The responsible party, or where applicable, the service provider performing the examination activities on their behalf, should have a detailed understanding of the validation documentation. [10]

There should be no difference in the availability of documentation irrespective of whether the documentation is held by the sponsor/investigator or a service provider or sub-contracted party. The responsible party is ultimately responsible for e.g., the validation and operation of the computerised system and for providing adequate documented evidence of applicable processes. The responsible party should be able to provide the [Regulatory] authorities with access to the requested documentation regarding the validation and operation of computerised systems irrespective of who performed these activities. [10]

g. Spreadsheet/Database Validation

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.

3.0 SYSTEM DEPENDABILITY

The sponsor should ensure and document that computerised systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance. (i.e., validation). [1]

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.

For each trial, it should be identified what electronic data and records will be collected, modified, imported and exported, archived and how they will be retrieved and transmitted. [10]

The responsible party should maintain a list of physical and logical locations of the data, e.g., servers, functionality and operational responsibility for computerised systems and databases used in a clinical trial together with an assessment of their fitness for purpose. [10]

Where multiple computerised systems/databases are used, a clear overview should be available so the extent of computerization can be understood. System interfaces should be described, defining how the systems interact, including validation status, methods used, and security measures implemented. [10]

Systems documentation should have adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. Systems documentation should follow revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. [9]

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.

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.

Requests for change should be documented and authorized and should include details of the change, risk-assessment (e.g., for data integrity, current functionalities and regulatory compliance), impact on the validated state and testing requirements. For trial specific configurations and customizations, the change request should include the details of the protocol amendment if applicable. [10]

As part of the change control process, all documentation should be updated as appropriate (e.g., requirements, test scripts, training materials, user guide) and a report of the validation activities prepared and approved prior to release for production. The system should be version controlled. [10]

c. Contingency Plans

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

d. 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.

Checks of accessibility to data, irrespective of format, including relevant metadata, should be undertaken to confirm that the data are enduring, continue to be available, readable and understandable by a human being. There should be procedures in place for risk-based (e.g., in connection with major updates) restore tests from the backup of the complete database(s) and configurations, and the performed restore tests should be documented. [10]

Disaster mitigation and recovery plans should be in place to deal with events that endanger data security. Such plans should be regularly reviewed. Disaster mitigation and recovery plans should be part of the contractual agreement, if applicable. [10]

e. 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.

An inventory of all essential data and documents and corresponding retention periods should be maintained. It should be clearly defined which data are related to each clinical trial activity and where this record is located and who has access/edit rights to the document. Security controls should be in place to ensure data confidentiality, integrity, and availability. It should be ensured that the file and any software required (depending on the media used for storage) remain accessible, throughout the retention period. Data should be maintained in a secure manner and should only be transferred between different (physical) locations in a validated process. Data should be archived in a read-only state. [10]

f. 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.

4.0 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.

All relevant computerised systems should be readily available with full, direct and read-only access (this requires a unique identification method e.g., username and password) upon request by inspectors from regulatory authorities. [10] Source documents and data should always be available when needed to authorized individuals to meet their regulatory obligations. [10]

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. 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.

The system used should ensure that the investigator can grant and revoke access to the electronic informed consent system to monitors, auditors and regulatory authority inspectors. [10]

The system should prevent the use of obsolete versions of the information and informed consent document.[10]

The system should use timestamps for the audit trail for the action of signing and dating by the trial participant and investigator or qualified person who conducted the informed consent interview, which cannot be manipulated by system settings. Any alterations of the document should invalidate the electronic signature. [10]

If an electronic signature is used, it should be possible for monitors, auditors, and inspectors to access the signed informed consent forms and all information regarding the signatures, including the audit trail. [10]

b. 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).[9]

Each electronic signature shall be unique to one individual, used only by the genuine owner, not reused or reassigned to anyone else and employ at least two distinct identification components such as an identification code and password. [9]

When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. [9]

When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. [9]

Electronic signatures must be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. [9]

Electronic signatures based on biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. [9]

Procedures must be in place to hold individuals accountable for actions initiated under their electronic signatures, in order to deter record and signature falsification. [9]

For 'closed' systems, which constitute the majority of systems used in clinical trials and which are typically provided by the responsible party or by their respective service provider, the system owner knows the identity of all users and signatories and grants and controls their access rights to the system. The electronic signature functionality in these systems should be proven during system validation.[10]

Loss management procedures shall be employed to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised IDs, tokens, cards, and other devices that bear or generate identification code or password information that are used for access and/or electronic signature purposes. [9]

Initial and periodic testing procedures shall be employed for IDs, tokens, cards, and other devices that bear or generate identification code or password information that are used for access and/or electronic signature purposes to ensure that they function properly and have not been altered in an unauthorized manner. [9]

5.0 TRAINING OF PERSONNEL

Those responsible for the use of computerized systems must determine that individuals (e.g., employees, contractors) who develop, maintain, or use computerized systems, electronic records/electronic signatures 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. [9]

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.

6.0 STANDARD OPERATING PROCEDURES (SOPS)

Documented procedures should be in place to ensure that computerised systems are used correctly. These procedures should be controlled and maintained by the responsible party. [10]

SOPs should be in place for handling and storing the system to prevent unauthorized access.

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:

- Validation [10]
- Functionality Testing
- System Setup/Installation
- Data Collection and Handling
- Data Transfer, Data Changes [10]
- Audit Trail, Audit Trail Review [10]
- System Maintenance
- Data Backup, Recovery
- Restore from Backup [10]
- Contingency Plans, Trial Continuation [10]
- Security, Security Incident Management [10]
- Password Policies [10]
- User Management, User Support [10]

- Access and Authentication
- Change Control
- Data Integrity

7.0 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. [8]

EHR and EDC systems may be noninteroperable, interoperable, or fully integrated, depending on supportive technologies and standards. [8]

a. 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. [8]

b. 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]

c. 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.[8]

d. 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. [8]

e. 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. [8] Refer to Validation section as well.

f. 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. [8]

g. Interface

Interfaces between systems should be clearly defined and validated e.g., transfer of data from one system to another. [10]

h. Transfer

Trial data are transferred in and between systems on a regular basis. The process for file and data transfer needs to be validated and should ensure that data and file integrity are assured for all transfers. [10]

All transfers that are needed during the conduct of a clinical trial need to be pre-specified. [10]

Validation of transfer should include appropriate challenging test sets and ensure that the process is available and functioning at clinical trial start (e.g., to enable ongoing sponsor review of diary data, lab data or adverse events by safety committees). [10]

8.0 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. [9]

9.0 REFERENCES

9.1 ICH E6 (R2) Good Clinical Practice: Integrated Addendum to International Conference of Harmonization (ICH) E6 (R1)

9.2 FDA General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002

9.3 FDA Guidance for Industry, Electronic Source Data in Clinical Investigations, 2013

9.4 Guidance for Industry: Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations Questions and Answers (fda.gov)

9.5 FDA Guidance for Industry, Electronic Records: Electronic Signatures – Scope and Application, 2003

9.6 FDA Guidance for Industry - COMPUTERIZED SYSTEMS USED IN CLINICAL TRIALS, 2007

9.7 FDA Use of Electronic Informed Consent in Clinical Investigations, Questions and Answers, 2016

9.8 FDA Guidance for Industry, Use of Electronic Health Record Data in Clinical Investigations, 2018

9.9 FDA 21 CFR Part 11 Electronic Records, Electronic Signatures, 1997

9.10 EMA Guideline on computerised systems and electronic data in clinical trials, 2023

10.0 REVISION HISTORY

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

10.2 DAIDS-OPC-A15-GUD-00005 rev 01 is the first revision of this guidance document in MasterControl. The document format and numbering were updated to reflect the current requirements. Also, the additional word “to” from the second sentence of section 1b was removed, in response to an internal audit finding from 2021.

10.3 DAIDS-OPC-A15-GUD-00005 rev 02 Document was update throughout to align with new EMA Guideline on computerized systems and electronic data in clinical trials, 2023 (reference 10). Updated Reference section to update existing references and add new references.