1.0 PURPOSE

1.1 This policy provides guidance and recommendations to NIAID Clinical Trials Networks, contract research organizations (CROs), data management centers, clinical research sites and clinical Investigators regarding the use of electronic systems in clinical research trials conducted by the NIAID Clinical Trials Networks.

2.0 SCOPE

2.1 This policy describes the requirements for electronic systems used in the conduct of NIAID DAIDS Network studies conducted within the Clinical Trials Networks, unless otherwise specified in a formal agreement. Electronic systems which fall under the scope of this policy include systems from which clinical trial data may be submitted to the FDA, EMA or any other regulatory authorities or systems that collect, manage, store, or generate data that can be used to reconstruct a clinical trial. The term "Electronic system" applies to records in electronic form that are used to create, modify, maintain, archive, retrieve, or transmit clinical or other data required to be maintained for, or submitted to the FDA, EMA or any other regulatory authorities.

The principles in this policy are applicable when electronic records are created (1) in hardcopy and later entered into an electronic system, (2) by direct entry by a human into a electronic system, and (3) automatically by an electronic system via a content management system.

Examples of electronic systems for electronic records:

- *TMF/eTMF*
- *Software versioning system*
- *Content management systems*
- *Electronic signature systems*

Examples of Direct Data Capture systems:

- Mobile devices, Mobile platforms/applications (apps), Laptops, Tablets

Note: This refers to direct data input from mobile telephones via an application (app), as the app would be within the scope of the policy.

  - Clinical outcome assessments (eCOAs), electronic participant diaries, Patient -Reported Outcomes (ePROs), Personal Digital Assistants (PDAs)
  - Telecommunication applications systems (apps), used to collect data via Short Message Service (SMS), online surveys, etc.
- Electronic Health Record (EHR) systems only when integrated with Electronic Data Capture (EDC) systems.
- Interactive Voice/Web Response Systems (IVRS/IWRS)
- Electronic Clinical Data Management System (eCDMS)
- Electronic Informed Consents (eICs)
- Data from Laboratory Information Systems (LIMS)
- Direct digitized data, such as data from, blood pressure monitors, electrocardiogram (ECG) machines, etc.
- Central image readings (such as from Magnetic Resonance Imaging (MRI), X-ray, or other scanning systems).

3.0 DEFINITIONS

For additional definitions, see DAIDS glossary.

3.1 **Audit Trail:** Documentation that allows reconstruction of the course of events. (ICH E6)

3.2 **Case Report Form (CRF):** A printed, optical, or electronic document designed to record all of the protocol required information to be reported to the sponsor on each trial subject.

3.3 **Commercial Off the Shelf (COTS):** Commercially available ready-made systems that are purchased and adapted as necessary.

3.4 **Data Originators:** The original source of data. Each data element is associated with an origination type that identifies the source of its capture in the eCRF. This could be a person, a computer system, a device, or an instrument that is authorized to enter, change, or transmit data elements into the eCRF (also sometimes known as an author). (FDA) Examples of data originators include:

- Clinical investigators and delegated clinical study staff
- Participants or their legally authorized representative
- Ancillary services representatives or other consultants such as radiologists, neurologists, etc.
- Devices such as electrocardiography (ECG) or blood pressure machines
- Electronic Health Records (EHRs)
- Automated laboratory reporting system
- IRT (Interactive Response Technology) web-based Randomization systems

3.5 **Direct Entry:** Recording data where an electronic record is the original capture of the data.

3.6 **Electronic System:** Computer hardware, software, and associated documents (e.g., user manual) that create, modify, maintain, archive, retrieve, or transmit in digital form information related to the conduct of a clinical trial. (FDA)

3.7 **Electronic Data Capture (EDC)** systems — Electronic systems designed to collect and manage clinical trial data in an electronic format into the electronic case report form (eCRF). Data entered onto the eCRF may be derived from a variety of sources including electronic health record systems (EHRs). (DAIDS).

3.8 **Electronic Health Record (EHR):** An electronic record for healthcare providers to create, import, store, and use clinical information for patient care, according to nationally recognized interoperability standards. NOTE: The EHR has the following distinguishing features: able to be obtained from multiple sources, shareable, interoperable, accessible to authorized parties. (FDA).

3.9 **Electronic Record:** Any combination of text, graphics, data, audio, pictorial, or any other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. (FDA).

3.10 **Electronic Source Data:** The data that are initially recorded in an electronic

format. (FDA)

3.11 **Encryption:** Encoding information in a way that only authorized individuals may access it.

3.12 **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (NIST)

3.13 **Interoperability**: 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. Fully integrated systems allow clinical investigators to enter research data directly into the EHR. (FDA)

3.14 **Risk Mitigation:** A strategy and steps taken to reduce or eliminate a risk or potential risk to data or systems integrity.

3.15 **Software as a Service (SaaS):** Software available by subscription and centrally hosted by a third-party provider; a form of cloud computing.

3.16 **Software Validation:** Confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the requirements implemented through the software can be consistently fulfilled. (FDA)

3.17 **User Acceptance Test (UAT):** A testing protocol to verify the system performs as required.

4.0 RESPONSIBILITIES

4.1 **DAIDS/Sponsor:**

a. Program Officer:

The *DAIDS Network Leadership Grant Program Officer (PO)* is responsible for approving the applicable network protocol documentation (as obtained from vendor/quality audits) for any electronic system to ensure data integrity, attributability, reliability, and compliance with the applicable regulatory

requirement(s).

The *DAIDS OCSO PO* is responsible for verifying that the clinical research site has written policies and processes for use of electronic systems (that fall within the scope of this policy) in the conduct of for National Institute of Allergy and Infectious Diseases (NIAID) Division of AIDS (DAIDS) supported and/or sponsored clinical trials. *See Appendix for requirement using electronic systems in clinical trials.*

b. DAIDS Quality Management Personnel:

As part of quality assurance, *DAIDS quality management personnel (QMP)* and/or designees are responsible for performing quality audits to ensure compliance with this policy. The audits performed by DAIDS QMP are separate from routine monitoring or quality control functions.

c. DAIDS Monitoring Contractor:

The *DAIDS Monitoring Contractor* or designee is responsible for verifying that the data required by the protocol are complete and accurately recorded on the CRFs are consistent with the source documents and that, the eSignatures and eIC if used, are thoroughly executed. The eSignatures and eIC must contain all elements required by regulations. *See Appendix for more information on Source Documentation and Record Retention.*

4.2 **The LOC PI, the LC PI, the SDMC PI, the CTU PI, the CRS Leader, and Investigator of Record (IoR) are each responsible for ensuring that the electronic systems under their purview meet the following requirements:**

- The electronic systems within the scope of this policy are designed to ensure data quality and integrity. These systems must have the capacity to be customized to meet protocol-specific data collection requirements to ensure completeness, accuracy, reliability and be validated for their intended use and performance.
- For non-COTS/in-house systems under the scope of this policy, the end user validation may be carried out by either the software owner organization/entity or by the end user/entity, as appropriate.
- Any systems which are interoperable or fully integrated are validated and have appropriate controls in place to ensure data integrity and protection of human subjects. *See Appendix for more information on interoperability and integration of systems.*
- That written standard operating procedures are established and maintained for each electronic system and ensure that there is adequate documentation that the SOPs have been followed.
- There is adequate documentation that written standard operating procedures are established, maintained and followed for each electronic system.
- Verifying that electronic systems in use are compliant with the U.S. Federal and all applicable regulations (local, national, and international).
- Providing direct data access to research records and source data for authorized personnel, including DAIDS, other monitoring contractors, auditors, and regulatory inspectors as required.
- Maintaining a list of each electronic data originator and the user access to the respective electronic system.
- Maintaining the staff system and training records for all internal staff system users and conforming to all required security and data policies when using electronic systems for direct data capture. *See Appendix section Training of Personnel for additional information and SOPs.*
- Ensuring that system validation procedures and controls are in place when using electronic systems for direct data capture. *See Appendix for more information on Validation.*

- Ensuring that procedures and work instructions include adequate quality control measures to maintain confidentiality, data integrity, and compliance with applicable laws, regulations, and policies.
- When applicable, ensuring eIC and eSignatures are captured as per regulations for each participant. *See Appendix for additional information on eIC and eSignature guidelines and Certification of eSignature.*
- Ensuring that the electronic systems can retain records in compliance with applicable regulations and are available for inspection. *See Appendix for Source documentation and Records Retention*.

- Ensuring that the access to all electronic systems under the scope of this policy is revoked promptly and documented upon staff departure.
- Ensuring that the DMCs are promptly notified of staffing updates with regards to access to electronic systems under the scope of this policy.

5.0 POLICY

5.1 The electronic systems used should be "(COTS)" systems (when one is available that meets the business requirements), designed to comply with the requirements in 21 CFR Part 11 and any other regulatory authority requirements. *See Appendix for System Dependability and System Controls.*

5.2 Each electronic system must be validated for its intended use and purpose and conform to the guidelines below. *See Appendix for more information on:*

a) Access Control
b) Audit Trail
c) Authority Checks
d) External Checks
e) Device Checks
f) Operational checks
g) Validation
h) Data element identifier checks
i) Electronic Informed Consent
j) Electronic Signature Guidelines.

5.3 An electronic system should be configurable for each protocol without compromising reliability, quality, and integrity of the data. *See Appendix for more information on Security.*

5.4 Electronic systems which are interoperable or fully integrated must be validated and have appropriate controls in place to ensure data integrity and quality. *See Appendix for more information on interoperability and integration of systems.*

5.5 Electronic system users must have the education, training, and experience necessary to perform their assigned tasks using the system for its intended purpose. *See Appendix for more information on Training of Personnel.*

5.6 For each protocol identify and document the software and hardware used in electronic systems that create, modify, maintain, archive, retrieve, or transmit data. This documentation must be retained as part of the protocol essential documents. *See Appendix for System Dependability and System Controls.*

5.7 The electronic system will be configured to ensure that all applicable regulatory requirements for recordkeeping and record retention in clinical trials are met. *See Appendix for Source documentation and Records Retention.*

5.8 Changes to data that are stored on electronic media require an audit trail, in accordance with all applicable regulatory requirements. *See Appendix for more information on Audit Trail.*

5.9 Electronic Information systems and data originator devices must have adequate controls in place to ensure confidentiality, reliability, quality, and integrity of the source data as related to risk to participants. The documentation must be readily available for sponsor oversight.

5.10 A risk assessment must be performed at the system level for each electronic system being used in the study. The assessment must evaluate the potential of the system to adversely affect human subject protection and the reliability of the study results. Security measures must be in place to prevent unauthorized access to the data and to the electronic system. *See Appendix for additional information on System Security.*

5.11 DAIDS encourages the use of interoperable systems for NIAID (DAIDS) sponsored and/or supported clinical research. *See Appendix for additional information on Interoperability and Integration of Systems.*

5.12 Electronic systems, whether interoperable or not, must have adequate controls to ensure the confidentiality, integrity, and security of data. *See Appendix for additional information on Interoperability and Integration of Systems.*

6.0 REFERENCES

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

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

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

6.4 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

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

6.6 FDA Guidance for Industry - COMPUTERIZED SYSTEMS USED IN CLINICAL TRIALS, 1999

6.7 FDA Use of Electronic Informed Consent in Clinical Investigations, Questions and Answers, 2015

7.0 APPENDICIES

7.1 APP-A15-OPC-005, Requirements for using Electronic Information Systems

in Clinical Research

7.2 APP-A15-OPC-006, Electronic Information System Evaluation Checklist

8.0 REVISION HISTORY

8.1 POL-A15-OPC-013.00 is the original version of this policy.

8.2 POL-A15-OPC-013.01 Updated the scope to clarify that the electronic systems that collect, manage, store, or generate data that can be used to reconstruct a clinical
Added Electronic Signature systems as example systems for electronic records

4.2 Clarified the responsibilities that non-cots validation may be carried our by either the software owner organization/entity or by the end user/entity, as appropriate.