Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers

Leonard Sacks, MD

Office of Medical Policy

CDER

FDA

Use of electronic systems in clinical investigations

- A myriad of ways in which electronic systems are used in clinical investigations to provide the records that FDA relies on
  - Data capture
  - Copying data
  - Data transfer
  - Data storage
  - Data analysis
- May apply to trial data, source documents, informed consent, required forms, tracking product, agreements with CROs and more

Ensuring the integrity of electronic records and signatures

- Part 11 regulations written in 1997
- They applied to electronic records and signatures required by FDA regulations or by predicate rules
- Provided a list of controls to ensure that electronic records and electronic signatures were equivalent to paper records, including:
  - Validation of systems
  - Audit trails
  - Access controls
  - Protection of records during retention period
  - Training of users

Advances in electronic systems

- Since 1997, enormous progress in electronic data capture and management
- There have been many changes in the way electronic systems and records are obtained and managed.
  - Many electronic functions are outsourced to service providers who are not part of the health care system- cloud storage and computational systems, commercial off- the-shelf software for data management, electronic signature packages
  - Clinical trial data may be obtained from real world data sources like Electronic health records which are not subject to FDA regulations
  - Digital health technologies are a new source of electronic clinical data
  - The internet has become the most widely used vehicle for data transfer
  - Electronic data flow between systems is more efficient and more prevalent
  - Electronic signatures, audit trails, encryption are in widespread use (e.g., healthcare, banking, commerce, Income tax)
- How do we ensure data integrity in these situations?

What is new in this draft guidance?

- Over the years FDA has published several guidances to keep pace with the changing electronic environment
- The draft guidance we are discussing today, when finalized, will replace our prior guidance entitled “Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11- Questions and Answers” (2017)
- In preparing this draft guidance we have attempted to address public comments in previous dockets and the many questions submitted directly to the Agency
- The major differences between this and the prior draft guidance revolve around:
  - RWD
  - Non US sites
  - Validation using a risk based approach- taking into account COTS software and customized systems
  - Certified copies
  - Digital health technologies
  - Electronic data transfer

Goals and limitations

- Added
  - Center for Food Safety and Applied Nutrition (CFSAN)
  - Center for Tobacco Products (CTP)
  - Center for Veterinary Medicine (CVM)
  - Office of Regulatory Affairs (ORA)
  - Office of Clinical Policy (OCLiP)
- Given the enormous range of circumstances involving electronic records and the variety of programs used to process them, it is not possible to address every specific use case. Our goal is to outline the principles for ensuring integrity of electronic records that can be broadly applied
- This is a draft guidance, and we will review all public comments in detail as we prepare to finalize this draft

Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers

Beth Kunkoski
Health Science Policy Analyst
CDER/Office of Medical Policy
April 25, 2023

Guidance Overview

- Electronic Records
- Electronic Systems
- Information Technology Service Providers and Services
- Digital Health Technologies
- Electronic Signatures

Real World Data (RWD) Sources (Q1)

- In general, 21 CFR part 11 applies to RWD sources
- However, FDA recognizes some RWD sources (e.g., electronic health records, registries) are not created in part 11 compliant systems and may still be used for marketing applications
- In these situations, sponsors should ensure the quality and integrity of electronic records to support marketing applications

Non-US clinical investigation sites (Q2)

- Electronic records from non-US clinical investigation sites, which are not conducted under an IND, IDE or INAD should be credible and accurate
- Quality of data should be comparable to data collected under an IND, IDE, or INAD

Certified Copies (Q3)

- Certified copy - a copy (irrespective of the type of media used) of the original record that has the same information including data that describe the context, content, and structure, as the original[1]
- Certified copies must be verified by a dated signature or by generation through a validated process (e.g., scanning or printing)
- Copies may be maintained and retained in place of the original records
- Copies should include the date and time when they were created
- Written standard operating procedures should be developed to ensure consistency

[1]See the ICH guidance for industry E6(R2) Good Clinical Practice: Integrated Addendum to ICH E6(R1).

Electronic Transmission (Q6)

- Part 11 does not address electronic communication methods used in the transmission of electronic records
- Regulated entity is responsible for ensuring secure end-to-end transfer of records
- Audit trails should capture date and time records are transferred and originators of those records

Electronic Systems (Sec. B)

- Overview of electronic systems owned or controlled by sponsors or other regulated entities to produce required records in a clinical investigation.
- Examples:
  - Electronic case report forms
  - Electronic trial master files
  - Electronic IRB management systems
  - Etc.

Security Safeguards (Q11)

- Procedures and processes to safeguard electronic records
- Logical and physical access controls
- Records to track authorized personnel and their access privileges
- Security safeguards (e.g., firewalls; antivirus, anti-malware, and anti-spyware software) should be in place and continually updated
- Security breaches should be reported to FDA and IRB

Information Technology (IT) Service Providers and Services (Sec. C)

- IT service vendors provide services such as data hosting, cloud computing software, platform and infrastructure services
- Sponsors and other regulated entities are responsible for ensuring that electronic records provided by IT service vendors meet applicable part 11 regulatory requirements
  - accurate and complete records
  - access controls
  - audit trails
  - data security and confidentiality

Digital Health Technologies (DHTs) (Sec. D)

- DHT is a system that uses computing platforms, connectivity, software, and/or sensors for health care and related uses.
- DHTs may take the form of hardware and/or software. In many instances, DHT software may run on general-purpose computing platforms (e.g., mobile phone, tablet, or smart watch).
- Draft guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations* (December 2021)

DHTs and Data Originators (Q20)

- For patient reported outcome measures (PROs), participants are the data originators.
- If the DHT transmits data automatically (e.g., activity tracker, mobile cardiac monitor, glucose monitor), the DHT (e.g., name and type) is the data originator.
- The sponsor should develop and maintain a list of authorized data originators.

Transfer of Data from DHT to Electronic Data Repository (Q22)

- Data from a DHT is generally transferred to a durable electronic data repository, such as an EDC system, a clinical investigation site database, and/or a vendor database.
- Transmission should occur contemporaneously or as soon as possible after data are generated.
- The date and time the data are transferred from the DHT to the electronic data repository should be included in the audit trail.
- Source data captured by a DHT can be subsequently moved from one durable electronic data repository to a different durable electronic data repository using a validated process.

DHT Source Data (Q23)

- Electronic source data are considered to be located in the first durable electronic data repository (e.g., EDC system, clinical investigation site database, cloud-based digital platform) to which the data are transferred.
- When the data captured by the DHT, including all associated metadata, are securely transferred to and retained in the durable electronic data repository according to the sponsor's pre-specified plan, then FDA does not intend to inspect individual DHTs for source data.

Electronic Signatures (Sec. E)

- 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. (§ 11.3(b)(7))
- Part 11 specifies that signed electronic records must contain the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature. (§ 11.50)
- Electronic signatures 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. (§ 11.70)

Electronic Signatures (Sec. E) (cont.)

- Signatures drawn with a finger or an electronic stylus are NOT considered electronic signatures. (11.3(b)(8))
- Electronic signatures based on **biometrics** that meet the requirements under part 11 subpart C are considered trustworthy, reliable, and generally equivalent to handwritten signatures. (§§ 11.1(a) and (c))

Methods for Electronic Signatures (Q24)

- Part 11 regulations do not specify a particular method to create electronic signatures.
- Examples include use of computer-readable ID cards, biometrics, digital signatures, and username and password combinations.
- Various commercial off-the-shelf (COTS) electronic signature services are available to create electronic signatures.
- Sponsors, clinical investigators, and other regulated entities should ensure that these COTS services conform to part 11 requirements based on information from the COTS vendors or their own validation of the services when warranted.

Certification of Electronic Systems to Create Electronic Signatures (Q28)

- FDA does not certify individual electronic systems and methods used to obtain electronic signatures.
- Sponsors should work with COTS electronic signature service vendors to ensure compliance with part 11.

21 CFR 11.100(c)(1) – Non-Repudiation Letters

- Technical amendment published March 2, 2023[1]
- Non-repudiation letters
  - A letter of non-repudiation is required to certify that a person's electronic signature is intended to be the legally binding equivalent of a traditional handwritten signature.
- May now submit letters electronically through the ESG mailbox ESGHelpDesk@fda.hhs.gov
- Paper copy not required
- FDA webpage on non-repudiation letters[2]

1 https://www.federalregister.gov/documents/2023/03/02/2023-04010/change-of-address-technical-amendment#:~:text=Letters%20of%20non%2Drepudiation%20are,equivalent%20of%20traditional%20handwritten%20signatures

2 https://www.fda.gov/industry/about-esg/appendix-g-letters-non-repudiation-agreement

Docket Comments

Submit Comments by 05/15/2023

Submit Comments Online

Although you can comment on any guidance at any time (see 21 CFR 10.115(g)(5)), to ensure that the FDA considers your comment on a draft guidance before it begins work on the final version of the guidance, submit either online or written comments on the draft guidance before the close date.

If unable to submit comments online, please mail written comments to:

Dockets Management
Food and Drug Administration
5630 Fishers Lane, Rm 1061
Rockville, MD 20852

All written comments should be identified with this document's docket number: FDA-2017-D-1105

https://www.regulations.gov/docket/FDA-2017-D-1105

U.S. FOOD & DRUG ADMINISTRATION

Questions?

Submit questions to: cderomp@fda.hhs.gov

U.S. FOOD & DRUG ADMINISTRATION

GCP Expectations

Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations Questions and Answers, Draft Guidance for Industry

April 25, 2023

Kassa Ayalew, M.D., M.P.H.
Division of Clinical Compliance Evaluation
Office of Scientific Investigations
Office of Compliance
Center for Drug Evaluation and Research

FDA Disclaimer

- The views expressed in this presentation are those of the speaker and not necessarily those of the US Food and Drug Administration.

- I have no financial interest to disclose.

Objective

- Providing perspectives on GCP inspections in relation to the revised draft guidance on Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations

Challenge Question 1: Elements of Data Quality

- The fundamental elements of data quality and integrity expected for Digital Health Technology are different from paper records
  1. True
  2. False

Challenge Question 2: Regulatory Requirements

- Data generated from electronic clinical outcome assessments (eCOAs) are not subject to similar regulatory requirements as data that come from paper records
  1. True
  2. False

Background

- FDA's drug approval determination depends on the submission of reliable data from any source

- FDA has a comprehensive Bioresearch Monitoring (BIMO) program of on-site inspections and data audits designed to monitor all aspects of the conduct and reporting of FDA regulated research that assess the validity/reliability of the data

Objectives of BIMO Inspection

- To ensure that rights, welfare, and safety of human research participants are adequately protected
- To verify the quality and integrity of data submitted to FDA to support safety and efficacy
- To determine compliance with the FDA regulations

Relevant Regulatory Requirements

- **Part 312:** Investigational New Drug Application
- **Part 50:** Protection of Human Subjects
- **Part 54:** Financial Disclosure by Clinical Investigators
- **Part 56:** Institutional Review Boards
- **Part 58:** Good Laboratory Practice for Nonclinical Laboratory Studies
- **Part 314:** Applications for FDA approval to market a new drug
- **Part 320:** Bioavailability and Bioequivalence Requirements
- **Part 361:** Radioactive Drug Research Committees

- **Part 11: Electronic Records; Electronic Signatures**
  - Establishes criteria under which FDA will accept electronic records and electronic signatures
  - Part 11 applies to electronic records and electronic signatures required to be maintained under the predicate rules or submitted to the Agency, in place of or in addition to paper format
  - It is a companion regulation to other FDA regulations called "predicate rules”

Requirements for Records

- Regardless of the **types of records**, the evidence submitted by a sponsor in a marketing applications to support the safety and/or effectiveness of a drug must satisfy the legal standards necessary for drug approval or licensing

- Electronic records are subject to the same regulatory expectations as paper records

- Compliance with regulatory requirements will be evaluated in accordance with appropriate predicate rules during inspection

Expectations that Fall under the Scope of Part 11

- Validation
- Access Controls
- External Security Safeguards
- Audit Trails/Reports
- Training
- Maintaining and Retaining Records
- DHT and Source Data
- Documentation

Validation

- Validation ensures that the electronic system is correctly performing its intended function

- Risk assessment should be done to validate things that affect product quality, safety as well as record integrity

- FDA inspection review activities related to electronic system validation in particular when there are potential concerns with data reliability

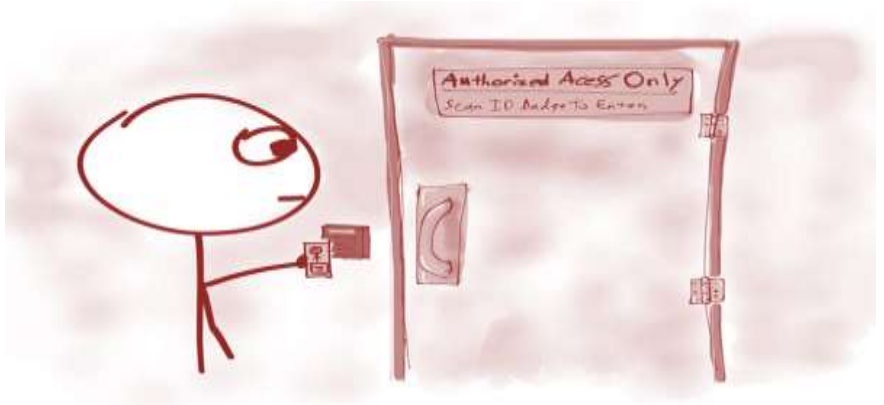
21 CFR 11.10(a) Validation of Systems

Access Controls

- Procedures and processes are in place to safeguard the authenticity, integrity, and the confidentiality of electronic records

- Systems should be designed to prevent unauthorized access (e.g., automatic log-outs after system inactivity)

- Inspections review access controls for electronic systems to ensure unauthorized access to restricted records or data (such as assessing if unblinding had occurred)



11.10(d) Limiting system access

Security Safeguards

- The safety and the privacy of study participants and the confidentiality of the study data are important
- The sponsor/CRO should have cybersecurity plans:
  - To protect the confidentiality of the data (e.g., document encryption)
  - To prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software (e.g., firewalls, antivirus and anti-spy software)

Audit Trials

- They are critically important in verifying the quality and integrity of data
- Periodic review of the audit trails may be helpful to ensure data quality and integrity
- During inspection, FDA review if electronic systems contain audit trails that fully capture the creation, modification, or deletion of all system data, including the ability to capture metadata (e.g., date and time stamps, data originator, reason for the change)
- FDA assess if audit trial can be modified or disabled

Training

- FDA expects anyone who develops, maintains, or uses electronic systems to have the education, training, and experience necessary to perform their assigned tasks
- Training should be conducted before the start of the clinical investigation and as needed when changes are implemented
- Training and experience with electronic systems used in clinical investigations should be documented
- Current training materials should also be available to study personnel and participants during the clinical study if needed

11.10(i) Persons who develop/maintain,…have the education, training, and experience

Retention of Electronic Records

- The records should be maintained throughout the records' retention period per applicable regulations and made available to FDA during an inspection
  - Sufficient backup and recovery procedures should be in place to protect against data loss
  - Screenshots or paper printouts of electronic records should include metadata and audit trail information recorded in the electronic system
  - When systems are decommissioned, sponsors should ensure that files containing the metadata are retained before decommissioning and can be linked to each corresponding data element
- Inspection determines if the sponsor had processes and procedures for retention and access to all records and data, including metadata associated with those records and data

Requirements for Maintaining and Retaining Records

Sponsor Records

- Records of receipt, shipment, or other disposition of the investigational drug
- Records showing any financial interest of investigators

Investigator Records

- Case histories, case report forms, consent forms, medical records including, progress notes
- Records of the disposition of the drug, including dates, quantity, and use by subjects

Retain the records and reports for **2 years after drug approval**; or, if drug is not approved, until **2 years** after shipment and delivery of the drug for investigational use is discontinued and **FDA has been so notified**.

Digital Health Technologies and Source Data

- For inspection purposes, electronic source data are considered to be located in the first durable electronic data repository
- FDA does not intend to inspect individual DHTs for source data
- All associated metadata should be securely transferred to and retained in the durable electronic data repository

Sponsor Oversight of Services

- Ensure all services and activities associated with the clinical investigation are performed according to the protocol and investigational plan, GCP, and applicable FDA regulations

- FDA inspection will evaluate the sponsor's oversight of services with focus on services that played significant role in the clinical trial

Documentation for Electronic Systems

Sponsor/CRO

- System setup, installation, and maintenance
- Validation plans, reports
- UAT reports, change control procedures
- System account setup, management
- Data backup, recovery, contingency plans
- Alternative data entry methods
- Audit trail information; training, technical support
- Roles and responsibilities; training records
- Records of contracts for delegated functions
- Data management procedures, data flow
- Other processes/procedures to ensure data reliability

Investigator

- Information regarding electronic systems
- Policies and procedures related to system account setup and management, access controls and user access privileges, system user manuals, and system training materials and records
- Procedures and controls in place for data access, data creation, data modification, and data maintenance
- Records related to staff training on the use of electronic systems
- Source records

- Electronic records used in clinical investigations should be fit for purpose
- Sponsors or investigators should use risk-based approach for designing/utilizing computerized systems for clinical data (focus on the data and processes that matter)
- Basic Requirements (predicate rules) for clinical data do not change for paper, computer, or hybrid approaches
- Inspections help to assess responsibilities for activities related to maintaining electronic system data integrity and procedures and controls for electronic records (e.g., access controls, audit trails, electronic system validation, training of users, SOPs for the use of the electronic system)

Thank you for your attention!

Kassa Ayalew, M.D., M.P.H.
Division of Clinical Compliance Evaluation
Office of Scientific Investigations
Office of Compliance
Center for Drug Evaluation and Research