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

Guidance for Industry

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Comments and suggestions regarding this draft document should be submitted within 60 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff (HFA-305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852. All comments should be identified with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this draft document, contact (CDER) Elizabeth Kunkoski, elizabeth.kunkoski@fda.hhs.gov or 301-796-6439; (CBER) Office of Communication, Outreach and Development, 800-835-4709 or 240-402-8010; (CDRH) Office of Clinical Evidence and Analysis, CDRHClinicalEvidence@fda.hhs.gov; (CFSAN) yuguang.wang@fda.hhs.gov or 240-402-1757; (CTP) ctp-bimo@fda.hhs.gov; or (CVM) Eric Nelson eric.nelson@fda.hhs.gov or 240-402-5642.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Devices and Radiological Health (CDRH)
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)

March 2023
Procedural
Revision 1

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

Additional copies are available from:
Office of Communications, Division of Drug Information
Center for Drug Evaluation and Research
Food and Drug Administration
10001 New Hampshire Ave., Hillandale Bldg., 4th Floor
Silver Spring, MD 20993-0002
Phone: 855-543-3784 or 301-796-3400; Fax: 301-431-6353
Email: druginfo@fda.hhs.gov
https://www.fda.gov/drugs/guidance-compliance-regulatory-information/guidances-drugs
and/or
Office of Communication, Outreach and Development
Center for Biologics Evaluation and Research
Food and Drug Administration
10903 New Hampshire Ave., Bldg. 71, Room 3128
Silver Spring, MD 20993-0002
Phone: 800-835-4709 or 240-402-8010
Email: ocod@fda.hhs.gov
https://www.fda.gov/vaccines-blood-biologics/guidance-compliance-regulatory-information-biologics/biologics-guidances
and/or
Office of Policy
Center for Devices and Radiological Health
Food and Drug Administration
10903 New Hampshire Ave., Bldg. 66, Room 5431
Silver Spring, MD 20993-0002
Email: CDRH-Guidance@fda.hhs.gov
https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/guidance-documents-medical-devices-and-radiation-emitting-products
and/or
Center for Food Safety and Applied Nutrition
Food and Drug Administration
5001 Campus Drive
College Park, MD 20740
Phone:240-402-1700
https://www.fda.gov/food/guidance-regulation-food-and-dietary-supplements
and/or
Center for Tobacco Products
Food and Drug Administration
10903 New Hampshire Ave., Bldg. 75
Silver Spring, MD 20993-0002
Phone: 240-402-7970
https://www.fda.gov/tobacco-products/products-guidance-regulations/rules-regulations-and-guidance
and/or
Policy and Regulations Staff, HFV-6
Center for Veterinary Medicine
Food and Drug Administration
7500 Standish Place, Rockville, MD 20855
https://www.fda.gov/animal-veterinary/guidance-regulations/guidance-industry

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Devices and Radiological Health (CDRH)
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)

March 2023
Procedural
Revision 1

TABLE OF CONTENTS

Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations Questions and Answers Guidance for Industry[1]

This draft guidance, when finalized, will represent the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff responsible for this guidance as listed on the title page.

I. INTRODUCTION

This document provides guidance to sponsors, clinical investigators, institutional review boards (IRBs), contract research organizations (CROs),[2] and other interested parties on the use of ***electronic systems***,[3] ***electronic records***, and ***electronic signatures*** in clinical investigations[4] of medical products,[5] foods, tobacco products,[6] and new animal drugs.[7] The guidance provides recommendations regarding the requirements, including the requirements under 21 CFR part 11 (part 11), under which FDA considers electronic systems, electronic records, and electronic

[1] This guidance has been prepared by the Office of Medical Policy in the Center for Drug Evaluation and Research (CDER) in coordination with the Center for Biologics Evaluation and Research (CBER), the Center for Devices and Radiological Health (CDRH), the Center for Food Safety and Applied Nutrition (CFSAN), the Center for Tobacco Products (CTP), the Center for Veterinary Medicine (CVM), the Office of Regulatory Affairs (ORA), and the Office of Clinical Policy (OCLiP) at the Food and Drug Administration.

[2] In some clinical investigations, a sponsor may transfer responsibility for any or all of its obligations under 21 CFR part 312 to a CRO (21 CFR 312.52). The requirements and recommendations that apply to sponsors throughout this guidance would also apply to CROs to the extent they have accepted responsibility for the sponsor's obligations.

[3] Words and phrases in ***bold italics*** are defined in the Glossary.

[4] For FDA's regulatory definitions of *clinical investigation* or *investigation*, see, e.g., 21 CFR 50.3(c), 56.102(c), 312.3(b), and 812.3(h). In this guidance, the terms *clinical trial*, *trial*, *clinical study*, *study*, *clinical investigation*, and *investigation* are interchangeable.

[5] In this guidance, the term *medical products* refers to human drugs and medical devices, including those that are licensed as biological products.

[6] Part 11 requirements only apply to records required under predicate rules; therefore, part 11 requirements do not apply to a request to use an investigational tobacco product at this time. However, we encourage sponsors, clinical investigators, and other interested parties to review this guidance for recommendations related to the use of electronic systems, electronic records, and electronic signatures in clinical investigations.

[7] See 21 CFR 11.1(b).

signatures to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

This guidance revises the draft guidance for industry *Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 — Questions and Answers* (June 2017).[8] This guidance expands upon recommendations in the guidance for industry *Part 11, Electronic Records; Electronic Signatures — Scope and Application* (August 2003) (2003 part 11 guidance) that pertain to clinical investigations conducted under 21 CFR parts 312 and 812. When finalized, this guidance will supersede the guidance for industry *Computerized Systems Used in Clinical Investigations* (May 2007). Other related guidances are included in the Appendix.

In general, FDA's guidance documents do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

II. BACKGROUND

In March 1997, FDA published a final rule to establish criteria that generally must be met when a record required by a predicate rule[9] is created, modified, maintained, archived, retrieved, or transmitted in electronic form in place of a paper record and when electronic signatures are used in place of traditional handwritten signatures.[10] FDA considers electronic records to be equivalent to paper records and considers electronic signatures to be equivalent to traditional handwritten signatures when they meet the requirements under part 11,[11] subject to program-specific rules for electronic records and signatures.[12]

In August 2003, FDA issued the 2003 part 11 guidance. The 2003 part 11 guidance provided recommendations that were narrowly tailored to reflect the technological environment that prevailed at that time. FDA continues to apply a narrow and practical interpretation of the part 11 regulations as described in the 2003 part 11 guidance. FDA reminds sponsors and other

[8] When final, this guidance will represent FDA's current thinking on this topic. For the most recent version of a guidance, check the FDA guidance web page at https://www.fda.gov/regulatory-information/search-fda-guidance-documents.

[9] The underlying requirements set forth in the Federal Food, Drug, and Cosmetic Act (FD&C Act), the Public Health Service Act (PHS Act), and FDA regulations (other than part 11) are referred to in this guidance as *predicate rules.* See 21 CFR 11.1.

[10] See § 11.1 and 62 FR 13430 (March 20, 1997).

[11] See § 11.1(a).

[12] Note that the 2003 part 11 guidance was prepared and issued by CFSAN, CVM, ORA, CDER, CDRH, and CBER. CTP continues to consider the relevance of the recommendations and policies in the 2003 part 11 guidance to tobacco product submissions.

regulated entities, however, that electronic records must still be maintained or submitted in accordance with the underlying predicate rules, and the Agency can take regulatory action for noncompliance with such predicate rules.

FDA recognizes that since 2003, advances in technology have expanded the uses and capabilities of electronic systems in clinical investigations. In addition, electronic systems and technologies are used and managed in novel ways, services are shared or contracted between organizations, and the electronic data flow between systems is more efficient and more prevalent. The capabilities of electronic systems have improved, and features such as automated date and time stamps, ***audit trails***, and the ability to generate complete and accurate copies and to archive records are standard components of many electronic systems. Understanding the evolving uses of electronic records, electronic systems, and electronic signatures in clinical investigations is important for FDA in its assessment of the authenticity, integrity, and reliability of data submitted in support of marketing applications or submissions.

Accordingly, this guidance provides additional recommendations regarding the risk-based approach to ***validation*** described in the 2003 part 11 guidance to continue to ensure the authenticity, integrity, and confidentiality of electronic data and records for clinical investigations during their creation, modification, maintenance, archival, retrieval, and transmission.[13]

This guidance also addresses the applicability of part 11 requirements for electronic systems and ***information technology*** (***IT***) ***services*** used to create, modify, maintain, archive, retrieve, or transmit an electronic record as well as for the use of ***digital health technology*** (***DHT***) to remotely acquire data in a clinical investigation.

III. QUESTIONS AND ANSWERS

Good clinical practice (GCP) is an international ethical and scientific standard for designing, conducting, recording, and reporting clinical investigations that involve the participation of human or animal subjects.[14] Compliance with FDA's GCP regulations provides public assurance that the rights, safety, and welfare of subjects are protected and that the clinical investigation data are credible.[15,16] The appropriate use of electronic records is an important component of GCP, and part 11 regulations help ensure that the electronic records and data for a clinical investigation are trustworthy and reliable.

[13] For more information, see the 2003 part 11 guidance. See also footnote 9.

[14] See the International Council for Harmonisation (ICH) guidance for industry *E6(R2) Good Clinical Practice: Integrated Addendum to ICH E6(R1)* (March 2018).

[15] See, e.g., 21 CFR parts 11, 16, 50, 54, 56, 58, 312, 314, 320, 511, 514, 601, 812, and 814.

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

A. Electronic Records

Electronic records used in clinical investigations that fall under the scope of part 11 requirements include:

- Records needed for FDA to reconstruct a clinical investigation that are maintained and archived under predicate rules in electronic format in place of paper format or where the electronic record is relied on to perform regulated activities[17]

- Records submitted to FDA in electronic format under predicate rules, even if such records are not specifically identified in FDA regulations[18]

Q1. Are electronic records from real-world data sources submitted to FDA as part of a marketing application or under other predicate rules subject to part 11 requirements?

Yes. 21 CFR part 11 requirements apply to electronic records from ***real-world data*** (***RWD***) sources that were created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations or submitted to the Agency under requirements of the Federal Food, Drug, and Cosmetic Act (FD&C Act) or the Public Health Service Act (PHS Act), even if such records are not specifically identified in FDA regulations.[19] FDA acknowledges that there may be instances when electronic records from RWD sources were not originally created in part 11-compliant systems with the intention of being submitted to FDA as part of a marketing application, but such records can be used for that purpose. Sponsors that intend to rely on such data in support of a marketing application should ensure the quality and integrity of such electronic records.[20]

[17] See § 11.1(b). For examples of relevant predicate rules, see 21 CFR 312.57, 312.58, and 312.62 (for drug and biological product investigational new drug applications (INDs)) and 21 CFR 812.28 and 812.140 (for investigational device exemptions (IDEs)).

[18] See § 11.1(b).

[19] See §§ 11.1(b), 314.50, and 601.2.

[20] As stated in the guidance for industry *Use of Electronic Health Records Data in Clinical Investigations* (July 2018) (2018 guidance), FDA does not intend to assess compliance of an ***electronic health record*** (***EHR***) ***system*** with part 11 regulations because, in general, they are under the control of organizations not regulated by FDA (e.g., health care providers, health care organizations, and health care institutions). These electronic systems provide electronic records (e.g., hospital admission records, pharmacy records, laboratory records, imaging records) during the course of patients' care that may be useful in clinical investigations. As noted above, FDA's acceptance of data in support of a marketing application or submission depends on FDA's ability to verify the quality and integrity of the data during FDA inspections (see 21 CFR parts 312 and 812). Note that the 2018 guidance was prepared and issued by CBER, CDER, and CDRH. CTP continues to consider the relevance of the recommendations and policies of the 2018 guidance to tobacco product submissions.

Q2. If a sponsor is conducting a clinical investigation with a non-U.S. (foreign) site, are the electronic records submitted to FDA as part of a marketing application or under other predicate rules subject to part 11 requirements?

If a sponsor is conducting a clinical investigation with a non-U.S. site, part 11 requirements generally apply to records in electronic form that are required under predicate rules,[21] including electronic records submitted to FDA in support of a marketing application or other submission.

For any data submitted in support of a marketing application or other submission, FDA recommends that sponsors ensure electronic records used in clinical investigations are credible and accurate. For example, the quality of data collected at foreign sites during clinical investigations that are not conducted under an IND,[22] IDE,[23] or investigational new animal drug file (INAD)[24] or that are submitted to FDA in support of a marketing application or submission should be equivalent to the quality of data collected under an IND, IDE, or INAD.[25] Namely, for sponsors to rely on such data in support of a human drug marketing application or submission, sponsors must ensure electronic records used in the clinical investigation are credible and accurate.[26]

Q3. Should sponsors, clinical investigators, and other regulated entities maintain and retain a certified copy of clinical investigation electronic records?

If a sponsor, clinical investigator, or other regulated entity intends to maintain and retain a copy of an electronic record required for the clinical investigation in place of an original paper or original electronic record, the copy maintained and retained should be a ***certified copy***. A certified copy is a copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original.[27] For example, for conversion between paper and electronic records, sponsors should rely on validated processes (e.g., scanning or printing) to generate certified paper or electronic copies. The copy generated by the validated process that is maintained and retained in place of

[21] See, e.g., §§ 11.1(b), 314.50, 514.1, 601.2, and 814.20. But see 21 CFR 11.1(f) through (p).

[22] For more information about foreign clinical studies supporting drug applications that are not conducted under an IND, see § 312.120. Marketing approval of a new drug based solely on foreign clinical data is governed by § 314.106.

[23] For more information about foreign clinical data supporting IDE or device marketing applications or submissions, see § 812.28 as well as the guidance for industry and FDA staff *Acceptance of Clinical Data to Support Medical Device Applications and Submissions: Frequently Asked Questions* (February 2018).

[24] For more information about foreign clinical studies supporting new animal drug applications or submissions, see the guidance for industry *Use of Data from Foreign Investigational Studies to Support Effectiveness of New Animal Drugs* (October 2021).

[25] See § 312.120 (for further information on the requirements for foreign clinical studies not conducted under an IND to support an IND or application for marketing approval).

[26] See, e.g., § 312.120.

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

the original record should include the date and time when it was created. Sponsors, clinical investigators, and other regulated entities should have written standard operating procedures (SOPs) to ensure consistency in the certification process.

When providing certified electronic or paper copies of electronic records, the associated ***metadata*** should be included, such as units of the data (e.g., mg); a date and time stamp for when the data were acquired; and the individual responsible for creating the copy, size of file, and number of files. Additional metadata are important for establishing authenticity or integrity for certain record types, such as digital photographs and audiovisual files.

Q4. Is FDA recommending that electronic records from medical service providers not involved in the clinical investigation be certified?

No. FDA's recommendation to maintain and retain certified copies of electronic records does not extend to electronic copies of records from medical service providers such as hospitals, laboratories, or health care practitioners not involved in the clinical investigation (e.g., copies of paper health records or EHRs containing a potential participant's medical history to a clinical investigator used either to determine eligibility for the clinical investigation or to report treatment for an adverse event). The clinical investigator should retain documentation that indicates the source of the records (e.g., cover sheet sent by the hospital).

Q5. How should sponsors, clinical investigators, and other regulated entities retain electronic records from a clinical investigation?

There are various ways to retain electronic records, including in durable electronic storage devices and using ***cloud computing*** services.[28] Sponsors, clinical investigators, and other regulated entities must ensure the authenticity, integrity, and confidentiality of the data from the point of creation and also ensure that the meaning of the record is preserved.[29] The relationship between records, ***source data***, and all associated metadata should be preserved in a secure and traceable manner.

FDA's expectation is that sponsors, clinical investigators, and other regulated entities will ensure that records are maintained throughout the records' retention period per applicable regulations[30] and, as applicable, made available to FDA during an inspection.[31] When electronic formats are the only formats used to create, preserve, and archive electronic records, sufficient backup and recovery procedures should be in place to protect against data loss. For example, records should be backed up regularly to prevent loss. Backup records should be stored in a secure electronic location independent from the original records as specified in an SOP. Backup and recovery logs should be maintained to facilitate an assessment of the nature and scope of data loss resulting from a system failure.

[28] See also section III.C for considerations when using IT service providers who provide cloud computing services.

[29] See § 11.30.

[30] See §§ 56.115(b), 312.57, 312.62, 511.1(b)(7)(ii), 511.1(b)(8)(i), and 812.140(d).

[31] See §§ 56.115(b), 312.58, 312.68, 511.1(b)(8)(i), and 812.145.

As part of an inspection, sponsors, clinical investigators, and other regulated entities may be requested to provide all records and data needed to reconstruct a clinical investigation, including associated metadata and audit trails.[32] FDA may request copies of these records and data in a human-readable form. Screenshots or paper printouts of electronic records should include metadata and audit trail information recorded in the electronic system. When systems are decommissioned and cannot be recommissioned, sponsors should ensure that files containing the metadata are retained before decommissioning and can be linked to each corresponding ***data element***.

Q6. Are electronic communication methods (e.g., email systems or text messages) for transmitting electronic records addressed by 21 CFR part 11?

Part 11 regulations do not address electronic communication methods used in the transmission of electronic records. When electronic records required by a predicate rule are transmitted via an electronic communication method, the regulated entity should ensure secure end-to-end transfer of that record. Audit trails in the sponsor's electronic system should capture the date and time that electronic records are transferred and the originator of those records.

B. Electronic Systems Owned or Controlled by Sponsors or Other Regulated Entities

This section describes recommendations for electronic systems that are owned or controlled by sponsors or other regulated entities and are used by such regulated entities to produce required records in clinical investigations.

Examples of these electronic systems can include:

- ***Electronic case report forms*** (***eCRFs***) and ***electronic data capture*** (***EDC***) ***systems***, including EDC systems that capture source data directly into eCRFs
- Electronic trial master files (eTMFs)
- Electronic clinical data management systems (eCDMS)
- Electronic clinical trial management systems (eCTMS)
- Electronic quality management systems
- Interactive response technology (IRT) systems
  - Interactive voice response system (IVRS)
  - Interactive web response system (IWRS)

[32] See §§ 312.58, 312.68, 511.1(b)(8)(i), 812.140, and 812.145.

- Electronic IRB management systems

- Electronic informed consent (eIC) systems

- Centralized, web-based portals that display, maintain, and archive essential data (i.e., electronic patient-reported outcomes (ePROs), electronic clinical outcome assessments (eCOAs), DHT-collected patient data (see section III.D), or eIC documents and records)

- Adverse event reporting (AER) and processing systems

Q7. What should be considered when using a risk-based approach for validation of electronic systems used in clinical investigations?

The 2003 part 11 guidance, which states that FDA intends to exercise enforcement discretion regarding specific part 11 requirements for validation of computerized systems (§§ 11.10(a) and corresponding requirements in 11.30), recommends that industry base its approach to such validation on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety as well as record integrity.[33] Accordingly, we recommend that sponsors and other regulated entities use a risk-based approach[34] for validating electronic systems owned or managed by sponsors and other regulated entities.

For purposes of this guidance, validation means a process of establishing and documenting that the specified requirements of an electronic system can be consistently fulfilled from design until decommissioning of the system or transitioning to a new system.[35] Validation ensures that the electronic system is correctly performing its intended function.

Considerations when applying a risk-based approach for validation of electronic systems include the following:

- The purpose and significance of the record and the criticality of the data (e.g., how the record and data will be used to support the regulatory decision and/or ensure participant safety).

- The intended use of the electronic system (e.g., used to process records[36] that are essential to the clinical investigation). Validation is critical for electronic systems that

[33] See the 2003 part 11 guidance.

[34] This guidance does not provide comprehensive detail on how to perform a risk assessment. There are many risk assessment methodologies and tools from a variety of industries that can be applied. For more information, see the ICH guidance for industry *Q9(R1) Quality Risk Management* (June 2022). Also, see the International Organization for Standardization's (ISO's) standard ISO 31010:2019 Risk management – Risk assessment techniques.

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

[36] In this guidance, *to process records* includes actions such as creating, modifying, maintaining, archiving, retrieving, or transmitting.

are used for activities such as data integration, data analysis, adverse event recording or processing, endpoint evaluation, medical product dispensation, administration, and accountability.

- The nature of the electronic system (e.g., ***commercial off-the-shelf*** (***COTS***) ***system***, ***customized electronic system***).

  - For COTS office utility software, such as word processing, spreadsheet, and PDF tools, the extent of validation should be guided by the organization's internal business practices and the intended use of the software in the clinical investigation. Generally, validation should not be necessary for COTS office utility software used as intended by the manufacturer.

  - For new electronic systems that are custom-made or for existing systems that are customized (e.g., IRT system or eCRF system designed to meet the requirements of the protocol), sponsors should review the ***vendor's*** SOPs, the system and software development life cycle model, validation documentation, change control procedures, and change control tracking logs. In addition, sponsors should perform ***user acceptance testing*** (***UAT***) and document the criteria for and results of testing to ensure that the electronic system fulfills its intended purpose. Alternatively, sponsors should review the vendor's UAT and document that the UAT was reviewed and was found to be adequate.

Changes to electronic systems (including software upgrades, security and performance patches, equipment or component replacements, and new instrumentation) should be evaluated and validated depending on risk. They should not affect the collection, storage, and retrieval of existing or new records or the traceability, authenticity, and integrity of existing data. Changes that affect operational limits or design specifications should be validated. Finally, all changes to the system should be documented. It may be appropriate for FDA to request documentation of system validation during an FDA inspection.

Q8. What documentation should the sponsor have in place for electronic systems that fall under the scope of part 11, and what will be FDA's focus during inspections of the sponsor?

For each clinical investigation protocol, the sponsor should describe the electronic systems (e.g., IRT system, EDC, eCOA) used to collect clinical investigation data as well as the electronic systems used to create, modify, maintain, archive, retrieve, or transmit pertinent electronic records. Sponsors should create a diagram that depicts the flow of data from creation to final storage.

Consistent with a risk-based approach to validation (see Q7), sponsors should consider (1) the purpose and significance of the record and the criticality of the data, (2) the intended use of the electronic system, and (3) the nature of the electronic system to determine when documentation or SOPs addressing the following are appropriate:

- System setup, installation, and maintenance
- System validation (e.g., validation plans, execution, and reports)
- UAT performed by the sponsor or vendor
- Change control procedures and change control
- System account setup and management, including user access controls
- Data backup, recovery, and contingency plans
- Alternative data entry methods (in the case of system unavailability)
- Information pertinent to use of the electronic system (e.g., audit trail information, interoperable data standards)
- Support mechanisms in place, such as training (including training records) and technical support
- Internal and external ***audits*** of electronic systems and of vendors that are performed or provided by the sponsor or independent consultants (see Q10) to ensure that the system is functioning and is being used consistently as intended
- Roles and responsibilities of sponsors, clinical sites, and other parties with respect to the use of electronic systems in the clinical investigation

Documentation related to the bulleted list above should be retained as part of the clinical investigation records and be available for inspection by FDA in order to assess whether such records contain information bearing on the sponsors' adequate compliance with relevant requirements. For electronic systems that fall under the scope of part 11, FDA will generally focus on the following during a sponsor inspection:

- Data collection, data handling, and data management plans and procedures
- The life cycle of the electronic system, from design and implementation to decommissioning or transitioning to a new system
- Processes and procedures that are in place to ensure that the data and records required to reconstruct the clinical investigation are not altered in value or meaning
- Authority checks in the electronic systems to ensure only authorized individuals are given appropriate access
- Change control procedures and any changes made to the system once in use

- Any contracts with vendors or other delegated entities that detail their functions and responsibilities

- All corrective and preventive actions implemented across all relevant activities and systems

Q9. What documentation should be available at clinical investigator sites for electronic systems that fall under the scope of part 11, and what will be FDA's focus during inspections of clinical investigator sites?

Sponsors should provide information to clinical investigator sites regarding electronic systems used in the clinical investigation that are owned or controlled by sponsors and vendors and that fall under the scope of part 11. This information may include 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. The clinical investigator should retain this information for review during an FDA inspection so that FDA can assess whether such records contain information bearing on the sponsor's adequate compliance with relevant requirements.

Clinical investigator sites that own or control electronic systems used in the clinical investigation that fall under the scope of part 11 (e.g., site-owned EDC system, electronic clinical investigator site file) should retain the documentation related to the use of the electronic systems as described in Q8.

Clinical investigator sites may have their own SOPs and documentation pertinent to the use of electronic systems. Such information may include, for example, SOPs that ensure users at the clinical investigator sites have their own accounts and appropriate access; SOPs for notifying sponsors of changes in clinical investigation personnel at the site so that access rights can be terminated; backup, recovery, and contingency plans for source documentation retained at the site; and site-generated user training. Clinical investigator sites should retain this information for review during an FDA inspection.

FDA will generally focus on the following during a clinical investigator site inspection:

- Records related to staff training on the use of electronic systems[37]

- Procedures and controls in place for system access, data creation, data modification, and data maintenance[38]

- Use of electronic systems at the clinical investigator site to generate, collect, transmit, and archive data[39]

[37] See § 11.10(i).

[38] See §§ 11.10(d) and (k).

[39] See § 11.10.

Q10. During an inspection, will FDA review the reports of audits performed by sponsors or other regulated entities of IT service providers' electronic systems, products, and services?

Sponsors and other regulated entities often conduct audits to assess the ***IT service provider's*** quality management plan and the content of and compliance with relevant SOPs used in the design and development of the electronic system, product, or service. Sponsors and other regulated entities also often conduct audits of clinical investigation data in electronic systems to ensure the functionality of the system.

FDA will generally not review audit reports of the IT service provider's electronic systems, products, and services.[40]

Q11. What are FDA's requirements and recommendations regarding the use of security safeguards?

Sponsors, clinical investigators, and other regulated entities must ensure that procedures and processes are in place to safeguard the authenticity, integrity and, when appropriate, confidentiality of electronic records.[41] Logical and physical access controls should be integral to electronic systems used in clinical investigations to limit system access to authorized users, particularly for systems that provide access to multiple users or systems that are accessed through networks.[42] The selection and application of access controls should be based on an appropriately justified and documented risk-based approach that protects the authenticity, integrity, and confidentiality of the data or information.[43] Part 11 requirements do not specify any particular methods for implementing access controls. Access controls may include multifactor authentication, strong login credentials, and/or ***biometrics*** (e.g., facial recognition, fingerprints, voice prints, iris scans).

A cumulative record should be maintained of all clinical investigation personnel who are authorized to access the electronic system as well as a description of their access privileges. These records should be accessible for use by appropriate clinical investigation personnel and for inspection by FDA. System administrators should not be involved in data collection or clinical investigation assessments.

[40] Compliance policy guide *CPG Sec. 130.300 – FDA Access to Results of Quality Assurance Program Audits and Inspections*, available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cpg-sec-130300-fda-access-results-quality-assurance-program-audits-and-inspections.

[41] See §§ 11.10 and 11.30.

[42] See §§ 11.10(d) and 11.30 (for requirements to limit system access to authorized individuals).

[43] Part 11 differentiates electronic systems as closed or open (§§ 11.10 and 11.30) and describes additional measures that may be necessary for open systems. Because of changing technologies and the increased risk of cybersecurity threats, a risk-based approach to validation should be used for all electronic systems.

Individuals should work only under their own usernames and passwords or other access controls and should not share log-on information with others. Steps must be taken to prevent unauthorized access to the system.[44] For example, individuals should log off the system when leaving their workstations. An automatic log off may be appropriate for idle periods. The system should be designed to limit the number of login attempts and to record unauthorized login attempts. Processes should be in place to detect, document, report, and remedy security protocol breaches involving attempted and confirmed unauthorized access.

Sponsors should conduct a risk assessment to determine appropriate procedures and controls to secure data at rest and in transit to prevent access by intervening or malicious parties.

Security safeguards (e.g., firewalls; antivirus, anti-malware, and anti-spyware software) should be in place and continually updated, as appropriate, to prevent, detect, and remedy the effects of computer viruses; replicating malware computer programs (i.e., worms); and other potentially harmful software code on clinical investigation data, software, and hardware. Other safeguards, such as encryption, should be used to ensure confidentiality of the data. In the case of security breaches to devices or systems, sponsors and other regulated entities should make reasonable efforts to ensure the continued validity of the source data.[45] Security breaches that could affect the safety or privacy of clinical investigation participants and data should be reported to the IRB and FDA as soon as possible.

Q12. What are considerations for sponsors and other regulated entities when implementing audit trails?

Audit trails provide a means to verify the quality, authenticity, and integrity of data, allowing reconstruction of significant details about clinical investigation conduct and source data collection. Electronically generated, time-stamped audit trails, in addition to other security measures, can also capture information related to the creation, modification, or deletion of electronic records.

Audit trails must capture electronic record activities including all changes made to the electronic record, the individuals making the changes, the date and time of the changes, and the reasons for the changes.[46] Original information must not be obscured by the use of audit trails or other security measures.[47,48] Audit trails should be protected from modification and from being disabled. Periodic review of the audit trail may be helpful for sponsors to ensure data quality, authenticity, and integrity. The decision to review audit trails should be based on a risk

[44] See § 11.10(d).

[45] Note that this security functionality should be part of the validation process of the software.

[46] See §§ 11.10(e) and 11.30.

[47] Ibid.

[48] See the guidance for industry *Electronic Source Data in Clinical Investigations* (September 2013) (2013 guidance). Note that the 2013 guidance was prepared and issued by CBER, CDER, and CDRH. CTP continues to consider the relevance of the recommendations and policies of the guidance to tobacco product submissions.

assessment of the clinical investigation, taking into account the systems, procedures, and controls in place.

All audit trail information on the creation, modification, and deletion of electronic records must be available for FDA inspection.[49] A risk-based approach should be applied for retaining access logs (i.e., records of individuals who accessed the system and the times they did so). For example, regulated entities should retain all system access logs for electronic systems or files that contain unblinding information to verify the authenticity and integrity of the blind throughout the clinical investigation.

FDA recommends that the audit trail be retained as a dynamic file (i.e., a file where the audit trail can be seen in the system while the record is being reviewed). If it is not possible to retain a dynamic file, the audit trail should be retained as a fixed-data document (e.g., PDF) provided that the copy of the audit trail information is a certified copy and is clearly linked to the respective record (see Q3). The audit trail information should accompany all copies of the record, including those retained by clinical investigators (whether at the clinical investigation site or at an alternate location). The information should be complete and understandable with clear and concise terms to describe the components of the audit trail. Audit trail components must include (1) the date and time the data element or information was entered or modified; (2) the individual making the change (e.g., user ID and user role); and (3) the old value, new value, and reason for the change if applicable.[50]

In the 2003 part 11 guidance, FDA stated that it intends to exercise enforcement discretion with respect to specific part 11 requirements, including, but not limited to, computer-generated, time-stamped audit trails (§§ 11.10(e) and (k)(2) and any corresponding requirement in 11.30). Persons must still comply with all applicable predicate rules. Even where there are no predicate rule requirements related to documentation, it is nonetheless important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the electronic records. FDA recommends basing a decision regarding whether to apply audit trails or other appropriate measures on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on product quality and record integrity.

Q13. Should an audit trail record every key stroke?

It is not necessary to record every key stroke in an audit trail. However, the audit trail should be available once the user has taken a deliberate action to create, modify, or delete electronic records. Any edits to completed fields should be captured in the audit trail. If an edit check exists for submitted data and prompts the user to make a correction, the audit trail should include the original response, the fact that the edit check prompted a correction, and any change made in response.

[49] Audit trail documentation must be retained for a period at least as long as the period required for the subject electronic records and must be available for FDA review and copying (see §§ 11.10(e) and 11.30).

[50] See § 11.10(e).

Q14. What controls should be in place to ensure that the electronic system's date and time are correct?

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 system administrators (see Q11), who should be notified if a system date or time discrepancy is detected. Any changes to date or time should be documented, except for automatic time changes made by systems for daylight savings.

For electronic systems used in clinical investigations that span different time zones, the sponsor should indicate the time zone that corresponds to the date and time stamp.

Q15. What are the requirements and recommendations regarding training of individuals who use electronic systems in clinical investigations?

Anyone who develops, maintains, or uses electronic systems subject to part 11 must have the education, training, and experience necessary to perform their assigned tasks.[51] Relevant training should be provided to individuals regarding the electronic systems they will use during the clinical investigation. Training should be conducted before the start of the clinical investigation and as needed during the study when changes are made to the electronic system. Training should cover processes and procedures to access the system, to complete clinical investigation documentation, and to detect and report incorrect data. Training should be documented. Current training materials should also be available to clinical investigation personnel and participants during the clinical investigation if needed. See Q8 and Q9 for more information on retention of training documentation.

Q16. Does FDA provide preliminary evaluations of electronic systems to be used in a clinical investigation to determine whether they comply with part 11 requirements?

No. FDA does not perform preliminary evaluations of electronic systems (e.g., EDC system, eCTMS) to determine whether they comply with part 11 requirements. These systems will be evaluated during an inspection.

C. Information Technology Service Providers and Services

Sponsors and other regulated entities can contract with vendors to provide IT services for a clinical investigation (e.g., data hosting, cloud computing software, platform and infrastructure services). Sponsors and other regulated entities are responsible for ensuring that electronic records meet applicable part 11 regulatory requirements. When determining the suitability of the IT service and IT service provider, sponsors and other regulated entities should consider the following regarding the IT service provider's ability to ensure the authenticity, integrity, and confidentiality of clinical investigation records and data:

- Policies the IT service provider has in place to allow the sponsor to perform oversight of the clinical investigation functions provided by the IT service provider

[51] See § 11.10(i).

- Processes and procedures the IT service provider has in place for validation of specific IT services to be used in the clinical investigation (see Q7)

- Ability of the IT service provider to generate accurate and complete copies of records and to provide access to data for as long as the records are required to be retained by applicable regulations (see Q5)[52]

- Processes and procedures the IT service provider has for retaining records and making them available for FDA inspection for as long as the records are required to be retained by applicable regulations (see Q5)[53]

- Access controls used by the IT service provider for specific IT services used in the clinical investigation, including SOPs for granting and revoking access (see Q11)

- Ability of the IT service provider to provide secure, computer-generated, time-stamped audit trails of users' actions and changes to data (see Q12)

- Ability of the IT service provider to secure and protect the confidentiality of data at rest and in transit (as appropriate for the content and nature of the record)

- Processes and procedures the IT service provider has in place related to electronic signature controls (see section III.E)

- Relevant experience of the IT service provider

Q17. Should sponsors or other regulated entities establish service level agreements with IT service providers?

Yes, FDA recommends that sponsors and other regulated entities have written ***service level agreements*** (***SLAs***) with IT service providers that describe how the IT services will meet the sponsor's requirements. Before entering an agreement, the sponsor or other regulated entity should evaluate and select IT services based on the IT service provider's ability to provide data integrity and data security safeguards (described in the bulleted list in section III.C) that are relevant to the IT service being provided. The SLAs should address services that provide data integrity and data security safeguards, such as participant confidentiality, data reliability, and adherence to applicable regulatory requirements. This should include, but not be limited to, the following:

- The scope of the work and IT service being provided.

[52] See, e.g., §§ 56.115(b), 312.57, 312.62, 511.1(b)(7)(ii), 511.1(b)(8)(i), and 812.140(d).

[53] Ibid.

- The roles and responsibilities of the sponsor or other regulated entity and the IT service provider, including those related to quality and risk management. The sponsor is responsible for any duties and functions related to the clinical investigation not specifically and lawfully transferred to and assumed by an IT service provider (e.g., via a transfer of regulatory obligation (TORO)).[54]

- Details regarding access to the data throughout the regulatory retention period.

Q18. What should sponsors and other regulated entities have available to demonstrate that the IT services are performed in accordance with FDA's regulatory requirements?

Sponsors and other regulated entities who outsource IT services should make the following information available for FDA upon request:

- SLAs and any other agreements that define the sponsor's expectations of the IT service provider

- All quality or risk management procedures related to the IT service

- Documentation of ongoing oversight of IT services

Q19. Would FDA inspect or investigate IT service providers in a clinical investigation?

FDA may inspect IT service providers who have assumed obligations in an IND set forth in a TORO in writing as described in § 312.52. FDA can also request to conduct focused investigations of IT service providers for examination of trial records, regardless of whether a TORO is established. An investigation is a targeted information-gathering activity triggered by a specific regulatory concern; for example, concerns regarding the integrity of trial data. Regardless, the sponsor should have access to all study-related records maintained by IT service providers since those records may be reviewed during a sponsor inspection.[55]

D. Digital Health Technologies

For the purposes of this guidance, a 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.[56] In many instances, DHT software may run on general-purpose computing platforms (e.g., mobile phone, tablet, or smart watch).

[54] See § 312.52.

[55] See, e.g., § 312.57 for specific requirements.

[56] In this guidance, the term *hardware* includes its firmware (i.e., software that is embedded within the hardware and that is essential to the core operation of the hardware). The term *software* refers to other software (e.g., a mobile application) that is not part of the hardware.

Sponsors, clinical investigators, and other regulated entities can use DHTs to record and transmit data during a clinical investigation. The recommendations in this section apply to DHTs used in a clinical investigation, whether the sponsor provides the DHT or the participants use their own DHTs.

When final, the draft guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations* (December 2021)[57] will provide recommendations for sponsors, clinical investigators, and other parties on the use of DHTs for ***remote data acquisition*** from participants in clinical investigations evaluating medical products. The draft guidance discusses, among other things, selection of DHTs for clinical investigations; verification, validation, and usability testing;[58] use of DHTs to collect data for clinical investigation endpoints; training on the use of DHTs; and identification and management of risks related to the use of DHTs in clinical investigations. The draft guidance also provides recommendations for designing clinical investigations incorporating DHTs.

The principles previously discussed in sections III.A through C regarding electronic systems are applicable when DHTs are used to record data in a clinical investigation. In addition, the following questions and answers discuss specific considerations regarding part 11 compliance for data collection from DHTs in a clinical investigation.

Q20. When using DHTs to capture data from participants in clinical investigations, how do sponsors identify the data originator?

As part of an audit trail, each electronic data element should be associated with an authorized ***data originator***. The data originator may be a person, a computer system, a DHT, or an EHR that is authorized to enter, change, or transmit data elements via a secure protocol into a ***durable electronic data repository***, such as an EDC system, a clinical investigation site database, and/or a vendor database (e.g., database of the CRO, IT service provider, DHT manufacturer).[59]

If a participant manually enters data into the DHT (e.g., when using an ePRO app or when performing a task-based measure, such as a cognitive test) and the data are then uploaded into a durable electronic data repository, the clinical investigation participant should be identified as the data originator. In cases where another individual (e.g., clinical investigation personnel, health care provider, parent, or other caregiver) enters data on behalf of the clinical investigation participant, the individual entering the data should be identified as the data originator, and the reason should be documented.

---

[57] When final, this guidance will represent FDA's current thinking on this topic. Note that the draft guidance covers drugs, biologics, and devices.

[58] As used in the draft guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations* (December 2021) (when final, this guidance will represent FDA's current thinking on this topic), the terms *verification* and *validation* are not intended to be synonymous with the terms defined in 21 CFR 820.3(aa) and 820.3(z) under the Quality System Regulation for devices (21 CFR part 820) or the terms *device software function verification* and *validation* as described in the guidance for industry and FDA staff *General Principles of Software Validation* (January 2002).

[59] See the 2013 guidance.

If a DHT, such as an activity tracker or a glucose sensor, transmits data automatically to the durable electronic data repository without any human intervention, the DHT should be identified as the data originator. In these cases, a ***data element identifier*** should be created that automatically identifies the particular DHT (e.g., name and type) as the originator of the data element. Other information associated with a data element, such as the date and time of entry and the unique identifier of the participant to whom it applies, should be recorded in the durable electronic data repository.

In some cases, data from DHTs are obtained in the course of medical care and entered manually or automatically into an EHR. The EHR data can, in turn, under appropriate circumstances be used in a clinical investigation and entered into the EDC system. In this situation, identifying the EHR as the data originator is sufficient because sponsors are not expected to ascertain the details about all of the users and DHTs that contribute information to the patient's EHR.

The sponsor should develop and maintain a list of authorized data originators, which should be available during an FDA inspection. When identification of data originators relies on unique codes, usernames, and passwords, access controls should be employed to ensure the security, authenticity, and integrity of the authorized usernames and passwords (see Q21).[60] When fingerprints or other biometrics are used by data originators in place of username and password combinations, controls should be designed to ensure that the biometrics cannot be used by anyone other than the data originator (see Q27).[61,62]

Q21. How should data attribution be ensured when DHTs are used to capture, transmit, and record data in clinical investigations?

Sponsors should ensure that data obtained using DHTs are correctly attributed to the data originator. Approaches may include the use of access controls, education of participants, and data monitoring. Data attribution concerns should be addressed during protocol development and at the time of DHT selection.

DHTs should be designed to prevent unauthorized changes to the data stored on the DHT before data are transmitted to and recorded in a durable electronic data repository. Access controls (e.g., biometrics, multi-factor authentication) should be in place for a ***mobile application*** that relies on user entry of data to ensure that entries come from the clinical investigation participants, personnel, or other individuals authorized to enter the data (e.g., health care providers, parents, or other caregivers).[63] Clinical investigation personnel, participants, and

[60] See §§ 11.10(d) and (g) and 11.30 (for additional information related to the requirements to limit system access to authorized individuals and the use of authority checks to ensure that only authorized individuals can access and use the system).

[61] See § 11.200(b) (for additional information related to the rule regarding electronic signatures based upon biometrics).

[62] See the 2013 guidance.

[63] See footnote 60.

other individuals should use their own usernames and passwords and not share them with others or use access controls belonging to others (e.g., biometrics).

For certain DHTs (e.g., wearable sensors), access controls may be difficult to implement. Sponsors should consider how they will address user authentication and data attribution for these DHTs, particularly when the data collected from such DHTs will be used to support a clinical investigation endpoint. The clinical investigator should discuss the appropriate use of such DHTs with participants. Clinical investigation participants should be instructed that only they should wear or use such DHTs. This discussion should be documented in the clinical investigation records. Periodic monitoring of DHT data during the clinical investigation can help to identify situations where data may be coming from individuals other than the intended user.

Q22. What should be considered during the initial transfer of the data from a DHT to the durable electronic data repository?

Data captured from a DHT and any relevant associated metadata should be transmitted to a durable electronic data repository according to the sponsor's pre-specified plan. The durable electronic data repository can be owned by sponsors or by vendors such as IT service providers. 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.

Q23. What is the location of the source data collected by a DHT, and what DHT-collected data would FDA intend to inspect during an inspection?

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. FDA does not intend to inspect individual DHTs for source data 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.

FDA may verify the data the sponsor submits in support of an application or submission against the electronic source data during an inspection.[64] As discussed in the 2003 part 11 guidance, FDA intends to exercise enforcement discretion with regard to the requirements for generating copies of records in human readable and electronic form for inspection, review, and copying by the Agency (§ 11.10(b) and any corresponding requirement in §11.30).[65] However, such records are also subject to requirements under predicate rules.[66] FDA recommends that sponsors allow for the inspection, review, and copying of such records in human readable form.[67]

[64] See § 11.10(b).

[65] See the 2003 part 11 guidance.

[66] See, e.g., §§ 211.180(c) and (d).

[67] See the 2003 part 11 guidance.

E. Electronic Signatures

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.[68] In general, a signature may not be denied legal effect or validity solely because it is in an electronic format, and a record relating to a transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[69]

In general, electronic signatures and their associated electronic records that meet all applicable requirements under part 11 will be considered to be equivalent to handwritten signatures.[70] 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.[71] In addition, 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.[72] In situations where electronic signatures cannot be placed in a specified signature block, a statement of testament (e.g., "I approved the contents of this document") should be placed elsewhere in the document to state the meaning of the signature and link the signature to the electronic record.

Q24. What methods might be used to create valid electronic signatures?

Part 11 regulations do not specify a particular method to confirm the user's identity when creating electronic signatures. Examples of methods used to create valid electronic signatures include, but are not limited to, the use of computer-readable ID cards, biometrics, ***digital signatures***, and username and password combinations.

Various COTS electronic signature services are available to create electronic signatures. Sponsors, clinical investigators, and other regulated entities should ensure that these services conform to part 11 requirements based on information from the COTS vendors or their own validation of the services when warranted.

[68] See § 11.3(b)(7).

[69] See the Government Paperwork Elimination Act (GPEA), enacted on October 21, 1998 (Public Law 105-277), and the Electronic Signatures in Global and National Commerce Act, enacted on June 30, 2000 (Public Law 106-229, 114 Stat. 464) (15 U.S.C. 7001-7006).

[70] See § 11.1(c).

[71] See § 11.50.

[72] See § 11.70.

Q25. Does FDA consider signatures drawn with a finger or an electronic stylus on a mobile platform or other electronic system to be electronic signatures?

No. Signatures drawn with a finger or an electronic stylus are considered handwritten signatures.[73] A handwritten signature executed to an electronic record must be linked to its respective electronic record.[74] The handwritten signature should be placed on the electronic document just as it would appear on a printed document to link the signature to the respective electronic record.

Q26. How should sponsors and regulated entities verify the identity of the individual who will be electronically signing records as required in § 11.100(b)?

Part 11 regulations do not specify a particular method for verifying the identity of the individual who will be electronically signing records.[75] Methods for verifying someone's identity may include, but are not limited to, use of official Government-issued identification, security questions, or strong digital login credentials accompanied by multi-factor authentication or video observation.

Q27. What requirements must an electronic signature based on biometrics meet to be considered acceptable?

Biometrics are "a method of verifying an individual's identity based on measurements of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable."[76] Examples of biometrics may include, but are not limited to, fingerprints, hand geometry (i.e., finger length and palm size), iris patterns, retinal patterns, or voice prints.

Electronic signatures based on biometrics must be designed to ensure that they cannot be used by anyone other than their genuine owners.[77] Suitable biometrics should be uniquely identified with the individual and should not change over time.

Electronic signatures based on biometrics that meet the requirements under part 11 subpart C are considered trustworthy, reliable, and generally equivalent to handwritten signatures.[78]

[73] See § 11.3(b)(8).

[74] See § 11.70.

[75] See § 11.100.

[76] See § 11.3(b)(3).

[77] See § 11.200(b).

[78] See §§ 11.1(a) and (c).

Q28. Does FDA certify electronic systems and methods used to obtain electronic signatures?

No. FDA does not certify individual electronic systems and methods used to obtain electronic signatures. FDA would consider an electronic signature to be trustworthy, reliable, and generally equivalent to handwritten signatures if electronic signatures and their associated electronic records meet the requirements of part 11,[79] regardless of the particular technology or brand used. Sponsors should work with COTS electronic signature service vendors to ensure compliance with part 11.

[79] Ibid.

GLOSSARY

Audits: Systematic and independent examinations of trial-related activities and documents to determine whether the evaluated trial-related activities were conducted and the data were recorded, analyzed, and accurately reported according to the protocol, sponsor's standard operating procedures (SOPs), good clinical practice (GCP), and the applicable regulatory requirements.[80]

Audit Trails: Processes that capture details such as additions, deletions, or alterations of information in an electronic record without obscuring the original record. Audit trails facilitate the reconstruction of the course of such details relating to the electronic record.[81] Audit trails typically capture each change itself, the individual making the change, the data and time of the change and, when applicable, the reason or reasons for the change.

Biometrics: Methods of verifying an individual's identity based on measurements of the individual's physical features or repeatable actions where those features and/or actions are both unique to that individual and measurable.[82]

Certified Copy: A copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original.[83]

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[84]

Commercial Off-the-Shelf (COTS) System: A commercially available electronic system (including hardware or software) that can be purchased from third-party vendors.

Customized Electronic System: System and software including functionalities that are adapted for the needs of the clinical investigation.

---

[80] See, e.g., 21 CFR parts 11, 16, 50, 54, 56, 58, 312, 314, 320, 511, 514, 601, 812, and 814; see also the ICH guidance for industry *E6(R2) Good Clinical Practice: Integrated Addendum to ICH E6(R1)*.

[81] See the 2013 guidance.

[82] See § 11.3(b)(3).

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

[84] See the National Institute of Standards and Technology's definition of *cloud computing*, available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Data Element: A single observation associated with a subject in a clinical study. Examples include birth date, white blood cell count, pain severity measure, and other clinical observations made and documented during a study.[85]

Data Element Identifier: The information associated with a data element that includes the origin of the data element, the date and time of entry, and the identification number of the study subject to whom the data element applies. Once set by the electronic system, this value should not be alterable in any way.[86]

Data Originator: 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).[87]

Digital Health Technology (DHT): A system that uses computing platforms, connectivity, software, and/or sensors for health care and related uses. These technologies span a wide range of uses, from applications in general wellness to applications as a medical device. They include technologies intended for use as a medical product, in a medical product, or as an adjunct to other medical products (devices, drugs, and biologics). They may also be used to develop or study medical products.[88]

Digital Signatures: Electronic signatures based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.[89]

Durable Electronic Data Repository: An enduring database that is electronically protected from alterations and maintained until the end of the record retention period.

Electronic Case Report Forms (eCRFs): Auditable electronic records of information that generally are reported to the sponsor on each participant, according to a clinical investigation protocol. An eCRF enables clinical investigation data to be systematically captured, reviewed, managed, stored, analyzed, and reported.[90]

---

[85] See the 2013 guidance.

[86] Ibid.

[87] Ibid.

[88] See the draft guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations*. When final, this guidance will represent FDA's current thinking on this topic. This draft guidance covers drugs, biological products, and devices. See also BEST (Biomarkers, EndpointS, and other Tools) Resource Glossary (2016), available at https://www.ncbi.nlm.nih.gov/books/NBK338448.

[89] See § 11.3(b)(5).

[90] See the 2013 guidance.

Electronic Data Capture (EDC) Systems: Electronic systems designed to collect, manage, and store clinical investigation data in an electronic format.

Electronic Health Record (EHR) System: An electronic platform that contains individual health records for patients. EHR systems are generally maintained by health care providers, health care organizations, and health care institutions and are used to deliver care.[91]

Electronic Records: Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.[92]

Electronic Signatures: Computer data compilation of any symbol or series of symbols executed, adopted, or authorized by individuals to be the legally binding equivalent of the individuals' handwritten signatures.[93]

Electronic Systems: Systems, including hardware and software, that produce electronic records.

Information Technology (IT) Services: Data hosting and/or computing services, such as software as a service, platform as a service, and infrastructure as a service.

IT Service Provider: A vendor who provides IT services to sponsors and other regulated entities.

Medical Claims Data: The compilation of information from medical claims that health care providers submit to insurers to receive payment for treatments and other interventions. Medical claims data use standardized medical codes, such as the World Health Organization's International Classification of Diseases Coding (ICD-CM) diagnosis codes, to identify diagnoses and treatments.[94]

Metadata: The contextual information required to understand the data. Metadata is structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data. Examples of metadata include units of the data (e.g., mg), a date and time stamp for when the data were acquired, data originator, and other audit trail information associated with the data.

Mobile Application: A software application that can be executed (run) on a mobile platform (i.e., a handheld COTS computing platform, with or without wireless connectivity) or a web-based software application that is tailored to a mobile platform but is executed on a server.[95]

---

[91] See the 2018 guidance.

[92] § 11.3(b)(6).

[93] § 11.3(b)(7).

[94] See the Framework for FDA's Real-World Evidence Program (December 2018), available at https://www.fda.gov/media/120060/download.

[95] For more information, see the guidance for industry and FDA staff *Policy for Device Software Functions and Mobile Medical Applications* (September 2022).

Registries: Organized systems that collect clinical and other data in standardized formats for populations defined by a particular disease, condition, or exposure.[96]

Real-World Data (RWD): Data relating to individual patient health status or the delivery of health care routinely collected from a variety of sources. Examples of RWD include data from EHRs; ***medical claims data***; data from product and disease ***registries***; patient-generated data (including data from in-home use settings); and data gathered from other sources that can inform on health status, such as DHTs.

Remote Data Acquisition: Collection of data from locations that are distant from the investigator or trial personnel.[97]

Sensor: A transducer that converts a physical, biological, or chemical parameter into an electrical signal; for example, temperature, pressure, flow, or vibration sensor. A sensor is typically hardware.[98]

Service Level Agreements (SLAs): Formal, negotiated documents that define the terms of service being offered to a customer.

Source Data: All information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical investigation necessary for the reconstruction and evaluation of the clinical investigation. Source data are contained in ***source documents*** (original records or certified copies).[99]

Source Documents: Original documents, data, and records (e.g., hospital records; clinical and office charts; laboratory notes; memoranda; subjects' diaries or evaluation checklists; pharmacy dispensing records; recorded data from automated instruments; copies or transcriptions certified after verification as being accurate copies; microfiches; photographic negatives; microfilm or magnetic media; x-rays; subject files; and records kept at the pharmacy, at the laboratories, and at medico-technical departments involved in the clinical investigation).[100]

User Acceptance Testing (UAT): A phase of testing in which users test the electronic system to ensure it can handle required tasks according to specifications.

---

[96] See the draft guidance for industry *Real-World Data: Assessing Registries to Support Regulatory Decision-Making for Drug and Biological Products* (November 2021). When final, this guidance will represent FDA's current thinking on this topic.

[97] See the draft guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations*. When final, this guidance will represent FDA's current thinking on this topic.

[98] See the National Institute of Standards and Technology web page, available at https://www.nist.gov/el/intelligent-systems-division-73500/definitions.

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

[100] Ibid.

968
969 **Validation**: A process of establishing and documenting that the specified requirements of an
970 electronic system can be consistently fulfilled from design until decommissioning of the system
971 or transition to a new system.[101]
972
973 **Vendor**: A supplier that sells electronic goods or services to sponsors and other regulated
974 entities.

[101] Ibid.

APPENDIX: RELEVANT GUIDANCE DOCUMENTS

The following guidance documents, among others, have additional information pertaining to 21 CFR part 11.[1] They are listed in the order referenced in this guidance document.

1. Guidance for industry *Part 11, Electronic Records; Electronic Signatures — Scope and Application* (August 2003).

2. Guidance for industry *E6(R2) Good Clinical Practice: Integrated Addendum to ICH E6(R1)* (March 2018).

3. Guidance for industry *Use of Electronic Health Records Data in Clinical Investigations* (July 2018).

4. Guidance for industry and FDA staff *Acceptance of Clinical Data to Support Medical Device Applications and Submissions: Frequently Asked Questions* (February 2018).

5. Guidance for industry *Q9(R1) Quality Risk Management* (June 2022).

6. Guidance for industry *Electronic Source Data in Clinical Investigations* (September 2013).

7. Draft guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations* (December 2021).[2]

8. Guidance for institutional review boards, investigators, and sponsors *Use of Electronic Informed Consent in Clinical Investigations: Questions and Answers* (December 2016).

[1] We update guidances periodically. For the most recent version of a guidance, check the FDA guidance web page at https://www.fda.gov/regulatory-information/search-fda-guidance-documents.

[2] When final, this guidance will represent FDA's current thinking on this topic.