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

Questions and Answers

Guidance for 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)
Oncology Center of Excellence (OCE)

October 2024
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
(Tel) 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
(Tel) 240-402-7970
https://www.fda.gov/tobacco-products/products-guidance-regulations/rules-regulations-and-guidance
and/or
Policy and Regulations Staff
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)
Oncology Center of Excellence (OCE)

October 2024
Procedural
Revision 1

Contains Nonbinding Recommendations

TABLE OF CONTENTS

Contains Nonbinding Recommendations

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

This guidance represents 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,[4] and electronic signatures[5] in clinical investigations[6] of medical products,[7] foods, tobacco products,[8] and new animal drugs.[9] The guidance provides

[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), the Office of Clinical Policy (OCLiP), and the Oncology Center of Excellence (OCE) at the Food and Drug Administration.

[2] 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 also apply to CROs to the extent they have accepted responsibility for the sponsor's obligations pursuant to § 312.52.

[3] Terms that appear in **bold** at first mention are defined in the Glossary.

[4] See § 11.3(b)(6) (21 CFR 11.3(b)(6)).

[5] See § 11.3(b)(7).

[6] 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), respectively. In this guidance, the terms *clinical trial*, *trial*, *clinical study*, *study*, *clinical investigation*, and *investigation* are interchangeable.

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

[8] Part 11 requirements apply to electronic records that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations and those submitted to FDA under the requirements of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and the Public Health Service Act; therefore, part 11 requirements do not apply to a proposed use of an investigational tobacco product at this time. See § 11.1(b). 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.

[9] See § 11.1(b).

recommendations regarding the requirements under 21 CFR part 11 (part 11), pursuant to which FDA considers electronic systems, electronic records, and electronic signatures to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures[10] executed on paper.

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)[11] that pertain to clinical investigations conducted under 21 CFR parts 312 and 812. Other related guidances are listed 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 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 handwritten signatures.[12] A *predicate rule* in this guidance refers to any requirement set forth in the Federal Food, Drug, and Cosmetic Act (FD&C Act), the Public Health Service Act, and FDA regulations other than part 11. Additionally, in this guidance, *archive* and *retain* are interchangeable terms. FDA considers electronic records to be equivalent to paper records[13] and considers electronic signatures to be equivalent to traditional handwritten signatures when they meet the requirements under part 11,[14] subject to specific exceptions for electronic records and signatures.

In August 2003, FDA issued the 2003 part 11 guidance.[15] 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 regulated entities, however, that electronic records must still be maintained in accordance with the underlying

---

[10] See § 11.3(b)(8).

[11] 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.

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

[13] See § 11.1(d).

[14] See § 11.1(c).

[15] Note that the 2003 part 11 guidance was prepared and issued by CFSAN, CVM, ORA, CDER, CDRH, and CBER.

predicate rules,[16] and the Agency can take regulatory action for noncompliance with such predicate rules. In this guidance, the term *regulated entities* refers to sponsors, CROs, clinical investigators, and IRBs to the extent they are responsible for regulatory obligations under a predicate rule to which the recommendations in the guidance pertain. The recommendations in this guidance primarily cover activities performed by sponsors, CROs, and clinical investigators, but more general recommendations (e.g., with respect to certified copies and system controls) are also applicable to IRBs' electronic records and electronic systems.

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 may be 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 retain records are standard components of many electronic systems.

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 when they are created, modified, maintained, archived, retrieved, or transmitted. See Q7 for additional information on validation.[17]

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.[18]

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 subjects.[19] Compliance with FDA's GCP regulations provides public assurance that the rights, safety, and welfare of subjects (i.e., participants) are protected and that the clinical investigation data are credible.[20] The appropriate use of electronic systems is an important

[16] See § 11.1.

[17] For more information, see page 6, Section III.C.1. Validation in the 2003 part 11 guidance.

[18] See the guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations* (December 2023).

[19] See the International Council for Harmonisation (ICH) guidance for industry *E6(R2) Good Clinical Practice: Integrated Addendum to ICH E6(R1)* (March 2018). GCP principles also apply to the conduct of studies to support new animal drug approval.

[20] See, e.g., 21 CFR parts 11, 16, 50, 54, 56, 58, 312, 314, 320, 511, 514, 601, 812, and 814. See ICH E6(R2).

component of GCP, and part 11 regulations help ensure that the electronic records and data for a clinical investigation are trustworthy and reliable.

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 retained under predicate rules in electronic form in place of paper form or where the electronic record is relied on to perform regulated activities[21]

- Records submitted to FDA in electronic form under predicate rules, even if such records are not specifically identified in FDA regulations[22]

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?

As stated in the guidance for industry *Use of Electronic Health Record Data in Clinical Investigations* (July 2018), FDA does not intend to assess compliance of an electronic health record (EHR) system[23] or other electronic systems that are sources of real-world data (RWD)[24] with part 11 regulations. These electronic systems may contain electronic records (e.g., hospital admission records, pharmacy records, laboratory records, imaging records) created during the course of patient care or for other purposes that are used to support marketing applications or other submissions under a predicate rule. Once the electronic record enters the sponsor's **electronic data capture (EDC) system,** FDA intends to assess compliance with part 11.[25] Regardless of how the data were originally generated, maintained, or retained, sponsors are responsible for ensuring the quality and integrity of the data they submit in support of marketing applications and other submissions.[26]

---

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

[22] See § 11.1(b).

[23] The guidance for industry *Use of Electronic Health Record Data in Clinical Investigations* was prepared and issued by CBER, CDER, and CDRH.

[24] See the guidance for industry *Considerations for the Use of Real-World Data and Real-World Evidence to Support Regulatory Decision-Making for Drug and Biological Products* (August 2023) and the guidance for industry *Data Standards for Drug and Biological Product Submissions Containing Real-World Data* (December 2023). These guidances were prepared and issued by CBER and CDER.

[25] See, e.g., the guidance for industry *Use of Electronic Health Record Data in Clinical Investigations*.

[26] See, e.g., § 314.126.

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 under an investigational new drug application (IND), investigational device exemption (IDE), or investigational new animal drug (INAD) file or other clinical investigation subject to FDA regulation, part 11 applies to records in electronic form that are required under predicate rules, including electronic records submitted to FDA in support of a marketing application or other submission.[27]

When a foreign clinical investigation is not conducted under an IND and the sponsor wants to rely on such data to support an IND or a marketing application, the sponsor must ensure that the study complies with § 312.120. A sponsor or applicant who submits data from a clinical investigation conducted outside the United States to support an IDE or a device marketing application or submission must comply with § 812.28. For sponsors to rely on such data in support of a marketing application or submission, sponsors must ensure that the data and results of the clinical investigation are credible and accurate.[28] For clinical investigations conducted at sites outside of the United States and not under an IND,[29] IDE,[30] or INAD,[31] the quality, integrity, and authenticity of the data submitted to FDA should be equivalent to that of the data collected under an IND, IDE, or INAD.

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

If a 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 that includes the date and time when the copy was created. 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

---

[27] See, e.g., §§ 11.1(b), 314.50, 514.1, 601.2, and 814.20. But see § 11.1(f) through (p), listing specific cases in which part 11 does not apply.

[28] See, e.g., §§ 312.120 and 812.28(a)(1); FDA Bioresearch Monitoring Compliance Program Manual 7348.810 Sponsors and Contract Research Organizations, available at https://www.fda.gov/media/75916/download; and FDA Bioresearch Monitoring Compliance Program Manual 7348.811 Clinical Investigators and Sponsor-Investigators, available at https://www.fda.gov/media/75927/download.

[29] For more information about foreign clinical investigations supporting INDs or drug marketing applications that are not conducted under an IND, see § 312.120. See also § 314.106 discussing marketing approval of a new drug based solely on foreign clinical data.

[30] For more information about data from clinical investigations conducted outside the United States to support an IDE or a device marketing application or submission, 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).

[31] For more information about foreign clinical investigations 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).

process) to have the same information, including data that describe the context, content, and structure, as the original.[32] 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. An original record can be discarded after a certified copy is created. 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** of the original record should be included (e.g., the date and time stamp for when the original data were acquired, changes made to the data). The retention period for certified copies maintained and retained in place of original records is the same as for original records.[33]

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

No. FDA is not recommending certification for 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 sent to a clinical investigator used either to determine eligibility for the clinical investigation or to report treatment for an adverse event).

Q5. How should regulated entities retain electronic records from a clinical investigation?

There are various ways to retain electronic records; for example, in electronic storage devices and using **cloud computing** services.[34] Regulated entities must ensure the authenticity, integrity, and confidentiality of the data and also should ensure that the meaning of the record is preserved.[35] The electronic records and all associated metadata should be preserved in a secure and traceable manner.

Regulated entities must ensure that electronic records are maintained for the applicable retention period,[36] and these records must be available for inspection in accordance with any applicable requirements.[37] When records exist only in electronic form, 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 separate from the original records as specified in appropriate system documentation or

---

[32] See the Glossary of ICH E6(R2).

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

[34] See also section III.C of this guidance for considerations when using IT service providers that provide cloud computing services.

[35] See § 11.30.

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

[37] See, e.g., §§ 56.115(b), 312.58, 312.68, 511.1(b)(8)(i), and 812.145. See also section 704(a)(5) of the FD&C Act.

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.

As part of an inspection, FDA may request that regulated entities provide all records and data needed to reconstruct a clinical investigation, including associated metadata and audit trails.[38] FDA may request copies of these records (e.g., screenshots or paper printouts) and data in a human-readable form. These copies should include metadata and audit trail information. When systems are decommissioned and cannot be recommissioned or a contract with a hosted system ends, sponsors should ensure that the metadata are obtained and retained and can be linked to each corresponding data element.[39]

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

Part 11 regulations do not address electronic communication methods. Regulated entities should determine whether the electronic communication method is appropriately secure for the type of clinical investigation information being transmitted and should take into consideration any other requirements that may be applicable to participant privacy.

B. Electronic Systems Deployed by Regulated Entities

This section describes recommendations for regulated entities regarding electronic systems they deploy in clinical investigations to create, modify, maintain, archive, retrieve, or transmit clinical investigation records. Regulated entities can deploy their own electronic systems or the systems of an IT service provider[40] to conduct clinical investigation activities such as randomization; data collection; collection and processing of adverse event reports; documenting informed consent; maintaining and retaining clinical investigation records; and medical product dispensation, administration, and accountability. Regulated entities should ensure that these systems are fit for purpose and implemented in a way that is proportionate to the risks to participant safety and the reliability of trial results.

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

The 2003 part 11 guidance states that FDA intends to exercise enforcement discretion regarding specific part 11 requirements for validation of computerized systems.[41] The 2003 part 11

---

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

[39] For the purposes of this guidance, *data element* means "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." See the guidance for industry *Electronic Source Data in Clinical Investigations* (September 2013), which was prepared and issued by CBER, CDER, and CDRH.

[40] See Q1 for information about the use of EHRs.

[41] See page 6, Section III.C.1. Validation in the 2003 part 11 guidance (describing how FDA intends to exercise enforcement discretion regarding the requirements in § 11.10(a) and corresponding requirements in § 11.30).

guidance recommends that industry base its approach to validation on a justified and documented risk assessment. Accordingly, we recommend that regulated entities use a risk-based approach[42] for validating the electronic systems they deploy.

For the purposes of this guidance, validation, including **user acceptance testing**, is a process to establish and document that the specified requirements of a computerized system can be consistently fulfilled from design until decommissioning of the system or transitioning to a new system. The level of validation may vary depending on the nature of the electronic systems (e.g., bespoke or customized systems, systems that are designed to be configured for the proposed use, and systems where no alterations are needed). Considerations when applying a risk-based approach for validation of electronic systems include:

- The intended use of the system;
- The purpose and importance of the data or records that are collected, generated, maintained, or retained in the system; and
- The potential of the system to affect the rights, safety, and welfare of participants or the reliability of trial results.

Validation should be applied to system functionality, configurations specific to the clinical trial protocol, customizations, data transfers, and interfaces between systems (e.g., interoperability and communication). When validation is performed by an IT service provider, the regulated entity that deploys the electronic system may consider reviewing the IT service provider's documentation to evaluate whether the electronic system is fit for purpose, including the following:

- Processes for developing and managing the system
- Validation processes
- Functional testing of the electronic system
- Change control procedures and tracking logs

Electronic systems should be validated prior to use in an investigation using a risk-based approach. Changes to electronic systems (including software upgrades, security and performance patches, equipment or component replacements, and new instrumentation) should be evaluated and validated throughout the life cycle of the system depending on risk. Changes should not adversely affect the traceability, authenticity, or integrity of new or existing data. All changes to the system should be documented.

[42] 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* (May 2023). Also, see the International Organization for Standardization's standard ISO 31010:2019 Risk management – Risk assessment techniques.

If, based on the sponsor's risk assessment, validation is conducted by or on behalf of a sponsor, FDA may request documentation of system validation during an inspection. It is the responsibility of the regulated entity to ensure such documentation is available if requested for review during an inspection, including documentation created and maintained by the IT service provider.[43]

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

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, data security, 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, including during the transfer of data to **durable electronic data repositories**
- Processes and procedures to ensure only authorized individuals are given appropriate access to electronic systems
- Change control procedures and any changes made to the system once in use
- Relevant contracts with IT service providers or other contracted entities that detail their functions and responsibilities
- Corrective and preventive actions implemented to address errors and noncompliance that may reasonably be expected to impact data integrity or the protection of participants

For each clinical investigation, the sponsor should document (1) the electronic systems (e.g., EDC system, clinical trial management system, interactive response technology system, electronic clinical outcome assessment) used to create, modify, maintain, archive, retrieve, or transmit pertinent electronic records and (2) the system requirements. Documentation should include a diagram that depicts the flow of data from data creation to final storage of data.

Consistent with a risk-based approach to validation (see Q7), sponsors should consider (1) the intended use of the system; (2) the purpose and importance of the data or records that are collected, generated, maintained, or retained in the system; and (3) the potential of the system to

[43] See, e.g., §§ 312.58(a) and 812.145(b).

affect the rights, safety, and welfare of participants or the reliability of trial results to determine when documentation or SOPs addressing the following are appropriate:

- System setup, installation, and maintenance
- System validation (e.g., risk assessment, validation plans, execution, and reports) and any assessment performed by the sponsor to demonstrate that the IT service provider's electronic system functions as intended
- User acceptance testing
- Change control procedures
- System account setup and management, including user access controls
- Data migration, data retention, data backup, data recovery, and contingency plans
- Alternative data entry methods (in the case of system unavailability)
- Audit trail and other information pertinent to use of the electronic system (e.g., interoperable data standards)
- Support mechanisms in place, such as training (including training records) and technical support
- Roles and responsibilities of sponsors, clinical investigation 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.[44]

Q9. What will be FDA's focus during inspections of clinical investigators for electronic systems that fall under the scope of part 11?

FDA will generally focus on the following issues related to electronic systems that fall within the scope of part 11 during a clinical investigator inspection:

- Records related to staff training on the use of electronic systems[45]

[44] See § 312.58(a) (for a discussion of FDA inspections related to a clinical investigation and access to records and reports related to a clinical investigation conducted under an IND).

[45] See § 11.10(i).

- Procedures and controls for system access, data creation, data modification, and data maintenance[46]

- Documentation regarding the use of electronic systems in the clinical investigation, including that users have their own accounts and appropriate access; that sponsors are notified of changes in clinical trial personnel so that access rights can be revoked; and that any backup, recovery, or contingency plans for source records have been used[47]

In addition, if a clinical investigator deploys their own electronic system to create, modify, maintain, retain, or transmit electronic records under the scope of part 11 (e.g., an EDC system deployed by clinical investigators, an electronic investigator site file for a clinical investigation), then investigators should retain the documentation related to that system described in Q8 and make it available during inspection.

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, development, and maintenance 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.[48]

Q11. What are FDA's requirements and recommendations regarding the use of security safeguards for electronic systems deployed by regulated entities?

Regulated entities must ensure that procedures and processes are in place to safeguard the authenticity, integrity and, when appropriate, confidentiality of electronic records.[49] Logical and physical access controls should be integral to electronic systems used in clinical investigations to

---

[46] See § 11.10(d) and (k).

[47] See § 11.10(d) and (k). In this guidance, *source records* are "original documents or data (which includes relevant metadata) or certified copies of the original documents or data, irrespective of the media used. This may include trial participants' medical/health records/notes/charts; data provided/entered by trial participants (e.g., electronic patient-reported outcome (ePROs)); healthcare providers' records from pharmacies, laboratories and other facilities involved in the clinical trial; and data from automated instruments, such as wearables and sensors." This definition also appears in the Glossary of the ICH draft guidance for industry *E6(R3) Guideline for Good Clinical Practice* (May 2023). When final, this guidance will represent FDA's current thinking on this topic.

[48] 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.

[49] See §§ 11.10 and 11.30.

limit system access to authorized users, particularly for systems that provide access to multiple users or systems that are accessed through networks.[50] The selection and application of access controls should be based on an appropriately justified and documented risk assessment to protect the authenticity, integrity, and confidentiality of the data or information.[51] 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[52] (e.g., facial recognition, fingerprints, voice prints, iris scans).

A record should be maintained of all clinical trial personnel who are authorized to access the electronic system as well as a description of their access privileges. This record should include the date when a user is added, the user's access rights and permissions, and any changes to rights and permissions. These records should be accessible for clinical investigators to ensure trial personnel have been granted appropriate access and for inspection by FDA (see Q8 and Q9).

Individuals should work only under their own usernames and passwords or other access controls and should not share login information with others. Steps must be taken to prevent unauthorized access to the system.[53] For example, individuals should log out of the system when leaving their workstations. An automatic logout of the system 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.

Regulated entities should conduct a risk assessment to determine appropriate procedures and controls to secure records and 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 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, regulated entities should address the continued validity of the source data.[54,55] Security breaches that have been internally investigated and confirmed as impacting

---

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

[51] 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 assessment should be conducted for all electronic systems for the selection and application of appropriate security safeguards.

[52] See § 11.3(b)(3).

[53] See § 11.10(d).

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

[55] For the purposes of this guidance, *source data* means "all information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical trial necessary for the

the safety or privacy of participants or the validity of source data should be reported to the IRB and FDA in a timely manner.

Q12. What are FDA's expectations for the use of audit trails by regulated entities?

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. Record changes must not obscure previously recorded information.[56]

To ensure the trustworthiness and reliability of electronic records, audit trails must capture electronic record activities including all changes made to the electronic record, the individuals making the changes, and the date and time of the changes[57] and should include the reasons for the changes. 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 assessment of the clinical investigation, considering the systems, procedures, and controls in place.

All audit trail documentation on the creation, modification, and deletion of electronic records must be available for FDA inspection.[58] A risk-based approach should be applied for retaining information on the individuals who accessed the system and the times they did so. For example, regulated entities should retain audit trail information on individual system access 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 in a format that is searchable and sortable. If this is not practical, audit trail files should be retained in a static format (e.g., PDFs) and clearly correspond to the respective data elements and/or records (see Q3 on certified copies). 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 (see Q14), (2) the individual making the change (e.g., user ID and user role), and (3) the old value and the new value.[59] The audit trail should include the reason for the change if applicable.

---

reconstruction and evaluation of the trial. Source data are contained in source documents (original records or certified copies)." See ICH E6(R2).

[56] See §§ 11.10(e) and 11.30.

[57] Ibid. See page 5, Section III.A.3. Data Element Identifiers in the guidance for industry *Electronic Source Data in Clinical Investigations* for additional information.

[58] 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).

[59] See § 11.10(e).

The 2003 part 11 guidance states that FDA intends to exercise enforcement discretion with respect to specific part 11 requirements, including but not limited to computer-generated, time-stamped audit trails.[60] 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 (see Q11). 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 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 record deliberate actions that a user takes to create, modify, or delete electronic records (e.g., save or submit). 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.

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, and individuals with system administrator roles should be notified if a system date or time discrepancy is detected. The ability to change the date or time should be limited to authorized individuals with system administrator roles, and any changes to date or time should be documented.

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 or indicate that times are recorded as Greenwich Mean Time (GMT).

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.[61] Relevant training should be provided to individuals regarding the electronic systems they will use during the clinical investigation. Training should be conducted before an individual uses the system, during the study as needed, and when changes are made to the electronic system that impact the user. 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 for reference to clinical trial

[60] See page 6 of the 2003 part 11 guidance.

[61] See § 11.10(i).

personnel and participants during the clinical investigation. 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, electronic clinical trial management system) to determine whether they comply with part 11 requirements. These systems will be evaluated during an inspection.

C. Information Technology Service Providers and Services

Regulated entities can contract with IT service providers for IT services in a clinical investigation (e.g., data hosting, cloud computing software, platform and infrastructure services). Regulated entities are responsible for ensuring that electronic records meet applicable part 11 requirements. When determining the suitability of the IT service and IT service provider, 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 regulated entity to perform oversight of the clinical investigation activities provided by the IT service provider
- 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)[62]
- Processes and procedures the IT service provider has for data migration, data backup, recovery, contingency plans, and 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)[63]
- 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 to provide secure, computer-generated, time-stamped audit trails of users' actions and changes to data (see Q12)
- Ability to secure and protect the confidentiality of data at rest and in transit (as appropriate for the content and nature of the record)

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

[63] Ibid.

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

- Relevant experience of the IT service provider

Q17. What should regulated entities include in agreements with IT service providers?

FDA recommends that regulated entities have a written agreement (e.g., a master service agreement with an associated service level agreement or quality agreement) with IT service providers that describes how the IT services will meet the regulated entities' requirements. Before entering into an agreement, the 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 of this guidance) that are relevant to the IT service being provided. The agreements 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.

- The roles and responsibilities of the regulated entity and the IT service provider, including those related to quality management. Sponsors are responsible for any regulatory obligations related to the clinical investigation not specifically and lawfully transferred to and assumed by an IT service provider.[64]

- A plan that ensures the sponsor will have access to data throughout the regulatory retention period.

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

Regulated entities that outsource IT services should make the following available for FDA upon request:

- Any agreements that define the sponsor's expectations of the IT service provider

- Documentation of quality management activities related to the IT service, including documentation of the regulated entity's oversight of IT services throughout the conduct of the trial

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

FDA may inspect IT service providers who have assumed regulatory responsibilities as described, for example, in § 312.52 or other relevant provisions. FDA may also conduct focused

[64] See § 312.52.

inspections of IT service providers to ensure the accuracy and reliability of trial records; for example, when there are concerns regarding the integrity of trial data, regardless of whether there has been a transfer of regulatory obligations.[65] In all cases, the sponsor should have access to all study-related records maintained by IT service providers because those records may be reviewed during a sponsor inspection.[66]

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 for remote data acquisition in clinical investigations can include hardware and/or software to perform one or more functions. DHTs may rely on or work with other technologies that support their operation, such as general-purpose computing platforms (e.g., smartphones) and communication networks. Examples of DHTs include wearable sensors, environmental sensors, or mobile applications to measure clinical events or characteristics. 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 and/or other technologies.

The guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations* provides recommendations for sponsors, investigators, and other stakeholders on the use of DHTs for remote data acquisition from participants in clinical investigations that evaluate medical products. The guidance provides recommendations for ensuring that a DHT is fit for purpose, which involves considerations of both the DHT's form (i.e., design) and function(s) (i.e., distinct purpose(s) within an investigation). The guidance discusses, among other things, selection of DHTs that are suitable for use in clinical investigations; verification, validation, and usability evaluations of DHTs;[67] use of DHTs to collect data for trial endpoints; training for trial personnel and trial participants on using DHTs according to the protocol; and identification and management of risks associated with the use of DHTs during clinical investigations.

The principles previously discussed in sections III.A through C of this guidance 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.

---

[65] See section 704(a)(5) of the FD&C Act (21 U.S.C. 374(a)(5)), which was added by section 3612 of the Food and Drug Omnibus Reform Act of 2022 (Public Law 117-328, 136 Stat. 5869-71).

[66] See, e.g., § 312.57 for specific requirements related to recordkeeping and record retention for studies conducted under an IND.

[67] As in the guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations*, the terms *verification* and *validation* as used in this guidance are not intended to be synonymous with these terms as defined for the purposes of quality management system obligations for devices under 21 CFR part 820 or the terms *software verification* and *validation* as described in the guidance for industry and FDA staff *General Principles of Software Validation* (January 2002).

Q20. When using DHTs to record 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.[68] 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 data transfer protocol.[69]

If a participant manually enters data into the DHT (e.g., when using an electronic patient-reported outcome mobile application or when performing a task-based measure, such as a cognitive test), the participant should be identified as the data originator. In cases where another individual (e.g., clinical trial personnel, health care provider, parent, or other caregiver) enters data on behalf of the participant, the individual entering the data should be identified as the data originator, and the reason that the participant is not the data originator should be documented.

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[70] should be created that automatically identifies the DHT as the originator of the data element. This and other information associated with a data element, such as the date and time the data are recorded and the unique identifier of the participant to whom it applies, are considered part of the DHT metadata and 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).[71] When

---

[68] For the purposes of this guidance, *data originator* means "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)." See the guidance for industry *Electronic Source Data in Clinical Investigations.*

[69] See page 3, Section III.A.1. Electronic Source Data Origination in the guidance for industry *Electronic Source Data in Clinical Investigations* for additional information.

[70] For the purposes of this guidance, *data element identifier* means "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 computerized system, this value should not be alterable in any way." See the guidance for industry *Electronic Source Data in Clinical Investigations.*

[71] 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).

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).[72]

Q21. How should data attribution be ensured when DHTs are used to record and transmit 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, participant education, and data monitoring. Data attribution concerns should be addressed during clinical trial protocol development and at the time of DHT selection.

DHTs should be designed to prevent unauthorized changes to the data stored on the DHT. Access controls (e.g., personal identification numbers, 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 participants, clinical trial personnel, or other individuals authorized to enter the data (e.g., health care providers, parents, or other caregivers).[73] Clinical trial personnel, participants, and other individuals should use their own usernames and passwords and not share them with others or use access controls belonging to others.

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. Participants should be instructed that only they should wear or use such DHTs. This discussion should be documented in the clinical investigation records.

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

Data recorded by a DHT and any relevant associated metadata should be transmitted by a validated process to a durable electronic data repository according to the sponsor's pre-specified plan. Transmission should occur contemporaneously or as soon as possible after data are recorded. The date and time the data are transferred from the DHT to the electronic data repository should be included in the audit trail. Data stored in a durable electronic data repository can be moved to a different durable electronic data repository using a validated process.

---

[72] See § 11.200(b) (for additional information related to the rule regarding electronic signatures based upon biometrics). See page 3, Section III.A.1. Electronic Source Data Origination in the guidance for industry *Electronic Source Data in Clinical Investigations* for additional information.

[73] 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).

Q23. For inspection purposes, what is the location of the source data recorded by a DHT?

FDA does not intend to inspect individual DHTs for source data verification. For inspection purposes, electronic source data are considered to be located in the durable electronic data repository (e.g., EDC system, clinical investigation site database, cloud-based digital platform) into which the data (including all metadata) recorded by the DHT are transmitted via direct, uninterruptable, and secure connection according to the sponsor's pre-specified plan (including the information security plan). See Q8 for the information that may be reviewed during an inspection regarding the validated data transfer process. FDA may verify the data the sponsor submits in support of an application or submission against the electronic source data during an inspection.[74]

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.[75] 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.[76]

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.[77] 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.[78] When an individual executes a series of signings during a period of single, continuous controlled system access, the first signing must be executed using all electronic signature components, but repeated (subsequent) signings may be executed using one electronic signature component that is only executable by and designed to be used only by the individual.[79]

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.[80] Any changes made to the record, including those subsequent to the

---

[74] See § 11.10(b). For more information on the protection and retention of DHT-recorded data, see section IV.G of the guidance for industry *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations*.

[75] See § 11.3(b)(7).

[76] See the Government Paperwork Elimination Act, 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).

[77] See § 11.1(c).

[78] See § 11.50.

[79] See § 11.200(a)(1)(i).

[80] See § 11.70.

electronic signature, must be reflected in the audit trail.[81] In situations where electronic signatures cannot be placed in a specified signature block, an electronic testament (e.g., "I approved the contents of this document") should be placed elsewhere in the document linking the signature to the electronic record.

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

Although part 11 specifies criteria under which FDA considers electronic signatures to be trustworthy, reliable, and generally equivalent to handwritten signatures executed on paper,[82] part 11 regulations do not specify a particular method to create a valid electronic signature. 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,[83] and username and password combinations.

Various commercial off-the-shelf electronic signature services are available to create valid electronic signatures. Regulated entities should ensure that these services conform to part 11 requirements based on information from the commercial off-the-shelf electronic signature service providers or their own validation of the services when warranted.

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.[84] A handwritten signature executed to an electronic record must be linked to its respective electronic record.[85] 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 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.[86] Methods for verifying an individual'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.

---

[81] See §§ 11.10(e) and 11.30.

[82] See § 11.1(a).

[83] See § 11.3(b)(5).

[84] See § 11.3(b)(8).

[85] See § 11.70.

[86] See § 11.100(b).

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.[87] 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.[88] 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.[89]

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

No. FDA does not certify electronic systems and methods used to obtain electronic signatures. FDA would consider electronic signatures to be trustworthy, reliable, and generally equivalent to handwritten signatures if electronic signatures and their associated electronic records meet the requirements of part 11, regardless of the particular technology or brand used.[90]

Q29. Are users of electronic signatures required to submit letters of non-repudiation to FDA to certify that an electronic signature is the legally binding equivalent of a traditional handwritten signature?

Yes. Before or at the same time a person uses an electronic signature in an electronic record required by FDA, users of electronic signatures must submit a letter of non-repudiation to FDA to certify that the electronic signature is intended to be the legally binding equivalent of a traditional handwritten signature.[91] Organizations may submit one letter of non-repudiation to cover all the electronic signatures used by that organization. Information on how to submit the certification either electronically or by mail is on FDA's web page on letters of non-repudiation agreement.[92]

---

[87] See § 11.3(b)(3).

[88] See § 11.200(b).

[89] See § 11.1(a) and (c).

[90] Ibid.

[91] See § 11.100(c).

[92] See Appendix G: Letters of Non-Repudiation Agreement, FDA Electronic Submissions Gateway User Guide, available at https://www.fda.gov/industry/about-esg/appendix-g-letters-non-repudiation-agreement.

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.[93]

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.[94]

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

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

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

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 a date and time stamp for when the data were acquired, data originator, and other audit trail information associated with the data.

User Acceptance Testing: A phase of testing in which users test the electronic system to ensure required tasks can be performed according to specifications. User acceptance testing helps ensure that the program aligns with user expectations and business needs before it is officially deployed.

[93] See, e.g., 21 CFR parts 11, 16, 50, 54, 56, 58, 312, 314, 320, 511, 514, 601, 812, and 814; see also ICH E6(R2).

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

APPENDIX: RELEVANT FDA REFERENCES

The following FDA references, 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. International Council for Harmonisation guidance for industry *E6(R2) Good Clinical Practice: Integrated Addendum to ICH E6(R1)* (March 2018)

3. Guidance for industry, investigators, and other stakeholders *Digital Health Technologies for Remote Data Acquisition in Clinical Investigations* (December 2023)

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

5. Guidance for industry *Considerations for the Use of Real-World Data and Real-World Evidence to Support Regulatory Decision-Making for Drug and Biological Products* (August 2023)

6. Guidance for industry *Data Standards for Drug and Biological Product Submissions Containing Real-World Data* (December 2023)

7. FDA Bioresearch Monitoring Compliance Program Manual 7348.810 Sponsors and Contract Research Organizations, available at https://www.fda.gov/media/75916/download

8. FDA Bioresearch Monitoring Compliance Program Manual 7348.811 Clinical Investigators and Sponsor-Investigators, available at https://www.fda.gov/media/75927/download

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

10. Guidance for industry *Use of Data from Foreign Investigational Studies to Support Effectiveness of New Animal Drugs* (October 2021)

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

12. Guidance for industry *Q9(R1) Quality Risk Management* (May 2023)

[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.

13. International Council for Harmonisation draft guidance for industry *E6(R3) Guideline for Good Clinical Practice* (May 2023)[2]

14. 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

15. Appendix G: Letters of Non-Repudiation Agreement, FDA Electronic Submissions Gateway User Guide, available at https://www.fda.gov/industry/about-esg/appendix-g-letters-non-repudiation-agreement

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