Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – 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DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.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be submitted within 60 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance.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 Division of Dockets Management (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) Cheryl Grandinetti or Leonard Sacks at 301-796-2500; (CBER) Office of Communication, Outreach and Development, 800-835-4709 or 240-402-8010; or (CDRH) Program Operations Staff or Irfan Khan at 301-796-5640.

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)

June 2017
Procedural

Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – 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/GuidanceComplianceRegulatoryInformation/Guidances/default.htm
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/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/default.htm
and/or
Office of Communication and Education
CDRH-Division of Industry and Consumer Education
Center for Devices and Radiological Health
Food and Drug Administration
10903 New Hampshire Ave., Bldg. 66, Room 4621
Silver Spring, MD 20993-0002
Phone: 800-638-2041 or 301-796-7100; Fax: 301-847-8149
Email: DICE@fda.hhs.gov
https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/default.htm

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)
June 2017
Procedural

TABLE OF CONTENTS

I. INTRODUCTION 1

II. BACKGROUND 2

III. SCOPE 3

IV. QUESTIONS AND ANSWERS: SCOPE AND APPLICATION OF PART 11 REQUIREMENTS IN CLINICAL INVESTIGATIONS 5

A. Electronic Systems Owned or Managed by Sponsors and Other Regulated Entities 5

B. Outsourced Electronic Services 10

C. Electronic Systems Primarily Used in the Provision of Medical Care 13

D. Mobile Technology 13

E. Telecommunication Systems 17

V. ELECTRONIC SIGNATURES 18

APPENDIX I: OTHER GUIDANCES WITH APPLICABLE RECOMMENDATIONS . 22

APPENDIX II: GLOSSARY OF TERMS 23

Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – 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), and other interested parties on the use of electronic records and electronic signatures in clinical investigations of medical products[2] under 21 CFR part 11, Electronic Records; Electronic Signatures.[3]

This guidance clarifies, updates, and expands upon recommendations in the guidance for industry *Part 11, Electronic Records; Electronic Signatures – Scope and Application* (referred to as the 2003 part 11 guidance)[4] that pertain to clinical investigations conducted under 21 CFR parts 312 and 812.[5] Thus, this guidance is limited to outlining the scope and application of part 11 requirements for clinical investigations of medical products.

This guidance discusses the following:

[1] This guidance has been prepared by the Office of Medical Policy in the Center for Drug Evaluation and Research in coordination with the Center for Biologics Evaluation and Research, the Center for Devices and Radiological Health, and the Office of Regulatory Affairs at the Food and Drug Administration.

[2] For the purposes of this guidance, unless otherwise noted, the term *clinical investigations* refers to FDA-regulated clinical investigations of medical products conducted under an investigational new drug application (IND) according to 21 CFR part 312 or under an investigational device exemption according to 21 CFR part 812. In this guidance, *medical products* include human drugs and biological products, medical devices, and combination products.

[3] In this guidance, 21 CFR part 11 is referred to as part 11 regulations.

[4] For more information, see the guidance for industry *Part 11, Electronic Records; Electronic Signatures – Scope and Application*. We update guidances periodically. To make sure you have the most recent version of a guidance, check the FDA guidance web page at https://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/default.htm. Also, see the *Federal Register* of September 5, 2003 (68 FR 52779).

[5] See Appendix I of this guidance for a list of other guidances that contain applicable recommendations.

- Procedures that may be followed to help ensure that ***electronic records*** and ***electronic signatures*** meet FDA requirements and that the records and signatures are considered trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper

- The use of a risk-based approach when deciding to validate ***electronic systems,*** implement ***audit trails*** for electronic records, and archive records that are pertinent to clinical investigations conducted under parts 312 and 812

The goals of this guidance are as follows:

- Update recommendations for applying and implementing part 11 requirements in the current environment of electronic systems used in clinical investigations

- Clarify and further expand on the risk-based approach described in the 2003 part 11 guidance to validation, audit trails, and archiving of records

- Encourage and facilitate the use of electronic records and systems to improve the quality and efficiency of clinical investigations

The Glossary in Appendix II defines many of the terms used in this guidance. Words or phrases found in the Glossary appear in ***bold italics*** at first mention.

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 must be met when a record required by a predicate rule[6] 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.[7] The part 11 regulations, which apply to all FDA program areas, were intended to permit the widest possible use of electronic technology. These regulations are compatible with FDA's responsibility for protecting the public health, while also ensuring the authenticity, the reliability, and, when appropriate, the confidentiality of electronic

[6] The underlying requirements 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) are referred to in this guidance as *predicate rules.*

[7] See 21 CFR part 11.

records, and ensuring that the signer cannot readily repudiate the signed record as not being genuine.[8]

The 2003 part 11 guidance represented FDA's interpretation of the regulations and was tailored to the technological environment that prevailed. 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 in new ways, and electronic data flow between parties is more efficient and more prevalent. The standards and capabilities of electronic systems have improved, and features – such as audit trails, automated date-and-time stamps, appropriate validation, and the ability to generate copies and retain records – are standard components of many electronic systems.

FDA's overall approach to the 2003 part 11 guidance was to provide a narrow and practical interpretation of part 11 requirements. FDA continues to support and promote such a narrow and practical interpretation in this guidance, including the Agency's continuing intent to exercise enforcement discretion regarding certain part 11 requirements for validation, audit trails, record retention, and record copying.[9] FDA reminds sponsors, however, that 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. In addition, FDA continues to encourage sponsors and other regulated entities to use a risk-based approach, as introduced in the 2003 part 11 guidance and further described in this guidance, when deciding to validate electronic systems, implement audit trails, or archive required records for clinical investigations.

Acknowledging the technological advances and remaining consistent with FDA's overall approach to the part 11 requirements, FDA clarifies in this guidance the part 11 controls that sponsors and other regulated entities must implement, as appropriate,[10] in the current technological environment. Furthermore, FDA regards the validation of electronic systems, the ability to generate complete and accurate copies of records, the ability to archive records, and the use of audit trails as powerful tools for ensuring the quality and reliability of electronic records. Therefore, in this guidance, FDA encourages and further clarifies the risk-based approach to validation of electronic systems, implementation of electronic audit trails, and archiving of electronic records to continue to ensure the quality, authenticity, and reliability of electronic records from their point of creation to their modification, maintenance, archiving, retrieval, or transmission.[11]

III. SCOPE

[8] See 62 FR 13430 (March 20, 1997).

[9] For more information about the part 11 requirements for validation, audit trails, record retention, and record copying, see § 11.10(a) through (c) and (e) and the corresponding requirements in § 11.30.

[10] For more information, see § 11.10(d) and (f) through (k) and § 11.30.

[11] See footnote 4.

In general, part 11 requirements apply to electronic records and electronic signatures and to the electronic systems used to create, modify, maintain, archive, retrieve, or transmit them (also, see section IV.A.Q5).[12]

This guidance applies to the following electronic records and electronic signatures:

- Records required for clinical investigations of medical products that are maintained in electronic format in place of paper format, including all records that are necessary for FDA to reconstruct a study

- Records required for clinical investigations of medical products that are maintained in electronic format and where the electronic record is relied on to perform regulated activities

- Records for clinical investigations submitted to FDA in electronic format under predicate rules, even if such records are not specifically identified in FDA regulations (see § 11.1(b))

- Electronic signatures required for clinical investigations intended to be the equivalent of handwritten signatures, initials, and other general signings

This guidance addresses the applicability of part 11 requirements for the following electronic systems used to create, modify, maintain, archive, retrieve, or transmit an electronic record referenced in the bulleted list above for clinical investigations:

- Electronic systems, including ***commercial off-the-shelf (COTS)*** and ***customized electronic systems*** owned or managed by sponsors and other regulated entities

- Electronic services, outsourced by the sponsor or other regulated entities

- Electronic systems primarily used in the provision of medical care

- ***Mobile technology***

- Telecommunication systems

For electronic systems that fall under the scope of part 11 regulations, the regulations distinguish the systems as closed or open (see §§ 11.10 and 11.30, respectively).[13] This distinction is seldom relevant because of the pervasive use of the internet and web-based systems. By permitting access to electronic systems through use of the internet, the security that results from restricting physical access may be lost. Therefore, it would be prudent to implement additional security

[12] See footnote 4.

[13] For the regulatory definition of a closed system, see 21 CFR 11.3(b)(4). For the regulatory definition of an open system, see 21 CFR 11.3(b)(9).

measures for such systems above and beyond those controls for closed systems described in § 11.10, such as encryption and the use of appropriate electronic signature standards to ensure the authenticity, integrity, and confidentiality of records (see § 11.30).

IV. QUESTIONS AND ANSWERS: SCOPE AND APPLICATION OF PART 11 REQUIREMENTS IN CLINICAL INVESTIGATIONS

A. Electronic Systems Owned or Managed by Sponsors, Sites, and Other Regulated Entities

Examples of electronic systems used in clinical investigations that are owned or managed by sponsors and other regulated entities (e.g., CROs, IRBs) include ***electronic case report forms (eCRFs)***; ***electronic data capture (EDC) systems***, electronic trial master files (eTMFs), electronic Clinical Data Management System (eCDMS), electronic Clinical Trial Management System (eCTMS), Interactive Voice Response System (IVRS), Interactive Web Response System (IWRS), centralized, web-based electronic patient-reported outcomes (ePRO) portals, and electronic IRB human subject application systems (eIRBs). Requirements and recommendations for these systems are described in this section.

Q1. What should sponsors and other regulated entities consider when using a risk-based approach for validation of electronic systems used in clinical investigations?

Consistent with the policy announced in the 2003 part 11 guidance, sponsors and other regulated entities should use a risk-based approach[14] for validating electronic systems owned or managed by sponsors and other regulated entities.[15] Validation is critical to ensure that the electronic system is correctly performing its intended function. Validation may include, but is not limited to, demonstrating correct installation of the electronic system and testing of the system to ensure that it functions in the manner intended.

Electronic records for FDA-regulated clinical investigations of medical products are used in a broad range of settings, which vary in importance and complexity. Similarly, the reliability and complexity of electronic systems that are used are variable. When using a risk-based approach for validating electronic systems, sponsors and other regulated entities should consider (1) the purpose and significance of the record, including the extent of error that can be tolerated without compromising the reliability and utility of the record for its regulatory purpose and (2) the attributes and intended use of the electronic system used to produce the record.

---

[14] 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 International Council for Harmonisation (ICH) guidance for industry *Q9 Quality Risk Management*. Also, see the International Organization for Standardization's (ISO) standard *ISO 31010:2009 Risk Management – Risk Assessment Techniques.*

[15] See the guidance for industry *Computerized Systems Used in Clinical Investigations*.

In general, sponsors and other regulated entities should have electronic systems validated if those systems *process*[16] critical records (e.g., records containing laboratory and study endpoint data, information on serious adverse events and study participant deaths, information on drug and device accountability and administration, protected health information, personally identifiable information, information critical to maintain blinding) that are submitted to FDA. The extent of validation should be tailored to the nature of the system and its intended use.

For COTS office utilities software in general use, such as word processing, spreadsheets, and portable document format (PDF) tools or for electronic systems that process non-critical procedural records, the extent of validation should be guided by the organization's internal business practices and needs.

For COTS systems that perform functions beyond office utilities, such as COTS EDC and eCRF systems, validation should include a description of standard operating procedures and documentation from the ***vendor*** that includes, but is not limited to, results of their testing and validation to establish that the electronic system functions in the manner intended. Validation should also be performed on any secondary programmable functionality of these COTS systems. For example, a COTS system used for a study to create and maintain eCRFs and electronically capture form data would need to be validated to ensure that business logic for data entry performs as expected (e.g., maximum values, minimum values, data type restrictions), branching logic is correctly applied if used, and subsequently captured data is captured as entered or intended. COTS software used to create CRFs that are only used in paper format for a study do not require this additional level of validation.

For COTS systems that are integrated with other systems or for customized systems that are developed to meet a unique business need of a user,[17] sponsors and other regulated entities should develop and document a validation plan, conduct the validation in accordance with the plan, and document the validation results. Such documentation may be reviewed and copied during an FDA inspection. Validation for these systems may include, but is not limited to, user acceptance testing, dynamic testing, and stress testing. Sponsors and other regulated entities should perform the validation before the use of these systems, in addition to initial testing of the electronic system, to ensure that the system functions in the manner intended.

In addition, processes should be in place to control changes to the electronic system and evaluate the extent of revalidation that the changes may necessitate. When changes are made to the electronic system (e.g., system and software upgrades, including security and performance patches, equipment or component replacement, or new instrumentation), sponsors and other regulated entities should evaluate the effect of the changes and validate the changes using a risk-based approach.[18] For example, some changes may be minor (e.g., bug fixes or security patches); other changes may be major or particularly significant (e.g., that cause the system to operate outside of previously validated operating limits). If the risk assessment determines that the change is minor or does not affect the system requirements, the extent of validation should be guided by the organization's internal business practices and needs. Major changes may require

[16] For the purposes of this guidance, *to process records* includes actions such as creating, modifying, maintaining,

archiving, retrieving, or transmitting.

[17] An example of a user's unique business need may include customization in order to integrate with other software systems or to address internal processes.

[18] See footnote 15.

additional re-validation and critical changes could trigger a re-validation of the entire system.

Q2. For electronic systems owned or managed by sponsors and other regulated entities that fall under the scope of 21 CFR part 11, what will be FDA's focus during inspections?

For these electronic systems that fall under the scope of part 11, an FDA inspection will focus on the implementation of the electronic system, including changes made to the system once in use and documentation of validation to test system functionality after implementation, where applicable. During inspection, FDA will focus on any ***source data*** that are transferred to another data format or system to ensure that checks are in place and that ***critical data***[19] are not altered in value or meaning during the migration process. FDA will also review standard operating procedures and support mechanisms in place, such as training, technical support, and auditing to ensure that the system is functioning and is being used in the manner intended.

Q3. Should sponsors and other regulated entities perform audits of third-party vendor's electronic systems and products?

Sponsors and other regulated entities often perform audits of the vendor's electronic systems and products to assess the vendor's design and development methodologies used in the construction of the electronic system or the product, as well as the vendor's validation documentation. To reduce the time and cost burden, sponsors and other regulated entities should consider periodic, but shared audits conducted by trusted third parties.

Sponsors and other regulated entities should base their decision to perform vendor audits on a risk-based approach as described in this guidance (see section IV.A.Q1). For example, vendor audits may be important when using customized electronic systems or when integrating COTS systems with other systems.

Q4. Under 21 CFR 11.10(d), what are FDA's expectations regarding the use of internal and external security safeguards?

Sponsors and other regulated entities must ensure that procedures and processes are in place to safeguard the authenticity, integrity, and, when appropriate, the confidentiality of electronic records (see §§ 11.10 and 11.30). Therefore, logical and physical access controls must be employed for electronic systems that are used in clinical investigations, particularly for systems that provide access to multiple users or that reside on networks (see §§ 11.10(d) and 11.30). Sponsors and other regulated entities must ensure that

[19] Examples of critical data may include documentation of informed consent, drug accountability and administration information, or study endpoints and protocol-required safety assessments. For more information, see section IV.A of the guidance for industry *Oversight of Clinical Investigations – A Risk-Based Approach to Monitoring*.

procedures and processes are in place to limit access to their electronic system to authorized users (see §§ 11.10(d) and 11.30). There should also be external security safeguards in place to prevent, detect, and mitigate effects of computer viruses, worms, and other potentially harmful software code on study data and software (e.g., firewalls, antivirus and anti-spy software).[20]

Q5. Under what circumstances are part 11 requirements not applicable for electronic copies of paper records?

Part 11 requirements are not intended to apply to electronic systems that are merely incidental to creating paper records that are subsequently maintained in traditional paper-based systems. In such cases, the electronic systems would function essentially the same way that manual typewriters or pens would function, and any signatures would be traditional handwritten signatures. Storage and retrieval of records would be of the traditional file cabinet variety. More importantly, the overall reliability and trustworthiness of the records and FDA's ability to access the records would primarily derive from generally accepted procedures and controls for paper records. Therefore, when sponsors or other regulated entities use electronic systems to generate paper printouts of electronic records and those paper records meet all the requirements of the applicable regulations, and persons rely on the paper records to perform regulated activities, FDA generally would not consider sponsors or other regulated entities to be using electronic records in place of paper records (see § 11.1(b)). In these instances, part 11 regulations would not apply to the electronic systems used to generate paper records.

However, if simple screenshots or paper printouts are used to produce a report and that report fails to capture important metadata (e.g., the ***data originator*** and the audit trail of the data) that are recorded in the electronic system, such paper records would be regarded as incomplete unless the accompanying metadata are included. FDA would require access to the electronic system used to produce those data to review the complete record (see 21 CFR 312.58, 312.68, 812.140, and 812.145).

Q6. Can sponsors and other regulated entities use and retain electronic copies of source documents in place of the original paper source documents?

Yes. FDA permits the interchangeable use of electronic records and paper records for the archiving and protection of records provided that recordkeeping and retention requirements are met (see 21 CFR 56.115, 312.57, 312.62, and 812.140). If the sponsor or other regulated entity intends to use an electronic copy in place of the paper source data (i.e., intends to destroy the paper source data), then part 11 regulations would apply to the electronic system used to create the copy (see §§ 11.10 and 11.30)). A process should be in place to certify that the electronic copy is an accurate representation of the original paper document. The copy of the original record should be verified as having all of the same attributes and information as the original record and certified as indicated by

[20] For more information on internal and external security controls, see the guidance for industry *Computerized Systems Used in Clinical Investigations*.

a dated signature. Sponsors and other regulated entities should have written procedures to ensure consistency in the certification process.

In addition, some electronic copies vary in terms of their ability to be modified. For electronic copies in which the records are modifiable, it would be important to have audit trails in place to ensure the trustworthiness and reliability of the electronic copy. Also, as noted earlier, 21 CFR 11.10 and 11.30 require physical, logical, and procedural controls designed to ensure the authenticity and integrity of electronic records.

Q7. Can electronic copies be used as accurate reproductions of electronic records?

Yes. True copies of electronic records may be made and maintained in the format of the original records or in a compatible format if the content and meaning of the original records are preserved and if a suitable reader and copying equipment (e.g., software and hardware, including media readers) are readily available. Sponsors and other regulated entities should designate which electronic document is the original and should certify the electronic copies by generating the copies through a validated process. This process should ensure that electronic copies of electronic originals have the same information, including data that describe the context, content, and structure of the data as the original.

Q8. Can sponsors and other regulated entities use durable electronic storage devices or cloud storage services to archive required records from a clinical investigation?

Yes. Using an electronic means, such as a durable electronic storage device or cloud storage service is an acceptable method to archive study-related records at the end of the study. Sponsors and other regulated entities should ensure that the integrity of the original data and the content and meaning of the record are preserved and protected from unauthorized access. In addition, if the electronic records are archived in such a way that the records can be searched, sorted, or analyzed, sponsors and other regulated entities should provide electronic copies with the same capability to FDA during inspection if it is reasonable and technically feasible. During inspection, FDA may request to review and copy records in a human readable form using electronic system hardware.

Q9. Does FDA provide preliminary audit service to inspect an electronic system used in a clinical investigation to ensure compliance with part 11 controls?

No. FDA does not perform preliminary audits to evaluate electronic systems (e.g., EDC system, CTMS) to ensure compliance with part 11 requirements. These systems would be evaluated during a regulatory inspection.

Q10. If a non-U.S. site is conducting a clinical investigation, are records required by FDA regulations subject to part 11 requirements?

If a non-U.S. site is conducting a clinical investigation under an investigational new drug application (IND), the clinical investigator and the sponsor must follow FDA regulations, including part 11. If required records (e.g., drug disposition, case report forms, case

histories)[21] are kept in electronic format, part 11 requirements will apply (see section III). Device clinical investigations conducted at non-U.S sites generally are not conducted under an investigational device exemption (IDE). However, in the event where non-U.S. clinical investigation sites agree to comply with 21 CFR part 812, for example, per the requirements outlined in the study protocol or in the investigator agreement, then the clinical investigator and the sponsor should follow FDA regulations, including part 11.

For foreign clinical studies not conducted under an IND or an IDE that are submitted to FDA in support of a research or marketing application, good clinical practice standard for electronic records and electronic systems would apply.[22]

B. Outsourced Electronic Services

FDA recognizes that sponsors and other regulated entities may choose to outsource electronic services. Examples of these types of electronic services are data management and hosting services, including ***cloud computing*** services. According to the National Institute of Standards and Technology, cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[23]

When these electronic services are used to process data for FDA-regulated clinical investigations, sponsors and other regulated entities should consider whether there are adequate controls in place to ensure the reliability and confidentiality of the data. Sponsors and other regulated entities should consider the factors in the following bulleted list when determining the suitability of the outsourced electronic services. If the outsourced electronic service does not provide the data security safeguards described in the following bulleted list, sponsors and other regulated entities should consider the risks of using such service (e.g., infringement of patient privacy rights, lack of reliability of the data in the clinical investigation and its regulatory implications).

- Validation documentation (see sections IV.A.Q1 and IV.B.Q15)

- Ability to generate accurate and complete copies of records

[21] See § 312.62.

[22] For more information about foreign clinical studies not conducted under an IND, see 21 CFR 312.120 and the ICH guidance *E6(R2) Good Clinical Practice – Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(R2)* (available at http://www.ich.org/products/guidelines/efficacy/article/efficacy-guidelines.html). For information about devices, see the draft guidance for industry and Food and Drug Administration staff *Acceptance of Medical Device Data From Studies Conducted Outside the United States*. When final, this guidance will represent FDA's current thinking on this topic.

[23] See the National Institute of Standards and Technology's definition of *cloud computing* (available at http://csrc.nist.gov/publications/PubsSPs.html#800-145).

- Availability and retention of records for FDA inspection for as long as the records are required by applicable regulations

- Archiving capabilities

- Access controls (see section IV.A.Q4) and authorization checks for users' actions

- Secure, computer-generated, time-stamped audit trails of users' actions and changes to data

- Encryption of data at rest and in transit

- Electronic signature controls (see section V)

- Performance record of the electronic service vendor and the electronic service provided

- Ability to monitor the electronic service vendor's compliance with electronic service security and the data integrity controls

Q11. If sponsors and other regulated entities outsource electronic services, who is responsible for meeting the regulatory requirements?

Sponsors and other regulated entities are responsible for meeting the regulatory requirements. Moreover, sponsors are responsible for assessing the authenticity and reliability of any data used to support a marketing application for a medical product. Thus, the sponsor is ultimately responsible for the clinical investigation and for ensuring that all records and data required to adequately perform and document the clinical investigation are obtained and available to FDA upon request and in a timely and reasonable manner (21 CFR 312.57, 312.58, 312.62, 312.68, 812.140, and 812.145).

Q12. Should sponsors or other regulated entities establish service agreements with the electronic service vendor?

Yes, sponsors and other regulated entities should obtain service agreements with the electronic service vendor to ensure records are highly accessible. Before entering into an agreement, the sponsor or other regulated entity should evaluate and select electronic services based on the electronic service vendor's ability to meet the part 11 requirements and data security safeguards described in the previous bulleted list (see section IV.B). Service agreements should include a clear description of these specified requirements and the roles and responsibilities of the electronic service vendor.

Electronic service vendor may themselves rely on secondary electronic service vendors in order to provide their service. An example of this setup is a CTMS written by a contracted vendor which is hosted on a cloud platform provided by another vendor. In this case, it is not expected for the sponsor or regulated entity to obtain a service level agreement with the contracted vendor's vendor.

Q13. Does FDA consider it acceptable for data to be distributed across a cloud computing service's hardware at several different geographic locations at the same time without being able to identify the exact location of the data at any given time?

428

If appropriate controls are in place, part 11 does notlimit the geographic location of cloud computing services. However, it is critical for sponsors and other regulated entities to understand the data flow and know the location of the cloud computing service's hardware in order to conduct a meaningful risk assessment regarding data access, integrity, and security. Data privacy laws may differ from country to country. Therefore, sponsors and other regulated entities should perform appropriate risk assessments to ensure that data residing on storage devices outside their country can be retrieved and accessed during FDA inspections, and that they comply with all laws and regulations.

Q14. What should sponsors and other regulated entities have available on site to demonstrate that their electronic service vendor is providing services in accordance with FDA's regulatory requirements?

Sponsors and other regulated entities should have the following information available to FDA upon request at each of their regulated facilities that use the outsourced electronic services:

- Specified requirements of the outsourced electronic service
- A service agreement defining what is expected from the electronic service vendor (see section IV.B.Q12)
- Procedures for the electronic service vendor to notify the sponsor or other regulated entity of changes and incidents with the service

Q15. What should sponsors and other regulated entities consider when deciding to validate outsourced electronic services that are used in clinical investigations?

A risk-based approach to validation similar to that described in section IV.A.Q1 should be taken for outsourced electronic services.

It is ultimately the responsibility of the sponsor or other regulated entity to ensure that the outsourced electronic service is validated as appropriate. Sponsors and other regulated entities should obtain documentation from the electronic service vendor that includes, but is not limited to, a description of standard operating procedures and results of testing and validation to establish that the outsourced electronic service functions in the manner intended.

Q16. Under what circumstances would FDA choose to inspect the electronic service vendor?

Under certain circumstances, FDA may choose to inspect the electronic service vendors, such as when they are or were engaged in providing services and functions that fall under areas regulated by FDA. For example, if the criticality of the investigation requires inspection and the required records are not available from the sponsor or the clinical investigation site, FDA may choose to inspect records specific to the clinical

investigation at the vendor's facilities to ensure that FDA requirements are met. The sponsor or other regulated entity is ultimately responsible for ensuring that regulated records and data are available to FDA during an investigation or an inspection.

Q Does part 11 allow for the use of blockchain technology in clinical research?

FDA is aware of the ongoing interest in blockchain technology in the life sciences industries. Blockchain technology used to create immutable, cryptographically secure, distributed records could potentially be used to implement part 11 control requirements for audit trails, identity verification, and encryption, among other possible uses. FDA does not prohibit the use of blockchain applications in clinical research, but as with any electronic system, the burden is on the sponsor, site, or other regulated authority to validate the system, meet part 11 control requirements, and comply with any other applicable laws and regulations.

C. Electronic Systems Primarily Used in the Provision of Medical Care

For the purposes of this guidance, electronic systems used in the provision of medical care (e.g., electronic health records (EHRs)) generally are systems that are (1) designed for medical care of patients not enrolled in a clinical investigation and (2) owned and managed by the institutions providing medical care. These electronic systems may produce additional electronic records during the course of patients' care (e.g., hospital admission records, electronic health records, pharmacy records, laboratory records, imaging records, electronic consultation records) that may be useful for providing data in clinical investigations. As provided in the guidance for industry *Electronic Source Data in Clinical Investigations*, FDA does not intend to assess compliance of these systems with part 11.[24] For more information on best practices for using data from EHRs in FDA-regulated clinical investigations, see the guidance for industry *Use of Electronic Health Records Data in Clinical Investigations*."[25]

D. Mobile Technology

Sponsors and other regulated entities may use mobile technology during the course of a clinical investigation to capture, record, or transmit data directly from study participants. The recommendations in this section apply to mobile technology used in a clinical investigation whether that technology is provided by the sponsor or owned by the study participant (i.e., ***bring your own device (BYOD)***). For the purposes of this guidance, mobile technology refers to portable electronic technology used in clinical investigations that allows for off-site and remote data capture directly from study participants and includes ***mobile platforms***, ***mobile applications (mobile apps)***,[26] ***wearable biosensors*** and other remote and ingestible sensors**,** and other portable and implantable electronic devices.

Q17. What access controls should sponsors implement for mobile technology accessed by study participants for use in clinical investigations?

Where possible, sponsors should ensure that basic user access controls (e.g., identification (ID) code, username and password combination, or electronic thumbprints

[24] For more information, see the guidance for industry *Electronic Source Data in Clinical Investigations.*

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

[26] For the purposes of this guidance, we do not distinguish between a *mobile app* and a "mobile medical app." A "mobile medical app" is a *mobile app* that meets the definition of device in section 201(h) of the FD&C Act and either is intended to be used as an accessory to a regulated medical device or to transform a mobile platform into a regulated medical device. For more information, see the guidance for industry and Food and Drug Administration staff *Mobile Medical Applications*.

and other ***biometrics***) are implemented, as appropriate, for mobile technology used by study participants in clinical investigations.

Specifically, for mobile apps that rely on study participants' user entry, access controls must be in place to ensure that entries come from the study participant (see 21 CFR 11.10(d)). For wearable biosensors and other portable electronic devices intended for a single study participant to wear or use (e.g., small physiologic sensors with no display screen), basic user access controls may be difficult to implement. In cases where access controls are impractical, sponsors should consider obtaining a signed declaration from the study participant confirming that the device will only be used by the study participant. Basic user access controls are not necessary when using ingestible sensors and implantable electronic devices.

Q18. When using mobile technology to capture data directly from study participants in clinical investigations, how do sponsors identify the data originator?

For the purposes of recordkeeping, audit trail, and inspection, each electronic ***data element*** should be associated with an authorized data originator. The data originator may be a person, a computer system, a device, or an instrument that is authorized to enter, change, or transmit data elements via a secure protocol into the sponsor's EDC system or into the electronic system of a trusted proxy agent such as a contract research organization.[27]

If a study participant who is using the mobile technology actively participates in the performance measure by entering and submitting data to the sponsor's EDC system (e.g., when using an ePRO app or when performing visual acuity testing), the study participant should be identified as the data originator.

If the mobile technology, such as an activity tracker or a glucose sensor, transmits data automatically to the sponsor's EDC system without any human intervention, the mobile technology should be identified as the data originator. In these cases, a ***data element identifier*** should be created that automatically identifies the particular mobile technology (e.g., name and type) as the originator of the data element. Information associated with a data element includes the origin of the data element, the date and time of entry, and the ID number of the study participant to whom the data element applies. Once set by the electronic system, this value should not be alterable in any way.[28]

In some cases, data from the mobile technology may be obtained in the course of medical care and may be entered manually or automatically into an EHR. The EHR data may, in turn, be used in a clinical investigation and entered into the sponsor's EDC system. In this situation, identifying the EHR as the data originator is sufficient because sponsors are

[27] See footnote 24.

[28] See footnote 24.

not expected to know the details about all of the users and mobile health technologies that contribute information to the patient's EHR (see section IV.C).

The sponsor should develop, maintain, and make available a list of authorized data originators. When identification of data originators relies on usernames and unique passwords, controls must be employed to ensure the security and the integrity of the authorized usernames and passwords (see 21 CFR 11.10(d)). When electronic thumbprints or other biometrics are used in place of username and password combinations, controls must be designed to ensure that the biometric identifier cannot be used by anyone other than the identifier's owner (see § 11.200(b) and section V.Q27).[29]

Q19. Does FDA consider the mobile technology to contain the source data?

When mobile technology is used in a clinical investigation to capture, record, and transmit study-related data directly from study participants, the data are collected and stored, perhaps for very short periods of time on the mobile technology before being transmitted to the sponsor's EDC system. In some cases, the data may pass temporarily through various electronic hubs or gateways before reaching the sponsor's EDC system. This could make the location of the source data difficult to determine.

FDA considers source data as data that are first recorded in a permanent manner. In general, for data collected directly from study participants through mobile technology, the first permanent record is located in the sponsor's EDC system or the EHR, and not in the mobile technology. FDA does not intend to inspect each individual mobile technology used in a clinical investigation to capture, record, and transmit data directly from study participants because access controls (see section IV.D.Q17), audit trails (see section IV.D.Q20), and validation (see section IV.D.Q21) that would be applied would help ensure the reliability of the data.

Q20. What should sponsors consider when implementing audit trails on data obtained directly from study participants using the mobile technology in the clinical investigation?

When data are copied or transmitted directly from the mobile technology to the sponsor's EDC system or from the mobile technology to the EHR and then to the sponsor's EDC system, the audit trail begins at the time the data enter the sponsor's EDC system. The sponsor's EDC system should capture the date and time that the data enter the EDC system and identification of the data originator (i.e., study participant, mobile technology, or EHR). In addition, the date and time that the measurement was made should be recorded and available to FDA at the time of inspection if it differs from the date and time the data enter the EDC system.

In cases where the study participant actively participates in the performance measure and manually enters the data into the mobile platform (e.g., tablet computers, smart phones)

[29] See footnote 24.

or other portable device, the mobile technology should be designed to prevent unauthorized modifications to the data before those data are transmitted to the sponsor's EDC system.

After the data are transmitted to the sponsor's EDC system, only clinical investigators or delegated study personnel who are authorized to make changes should perform modifications or corrections to the data. Modified and corrected data elements should have data element identifiers that reflect the date, time, and data originator and the reason for the change. Modified and corrected data should not obscure previous entries. Clinical investigators should review and electronically sign the completed eCRF for each study participant before the data are archived or submitted to FDA. Use of electronic signatures must comply with part 11 (see section V).[30]

Q21. What should sponsors consider when using a risk-based approach to validation of mobile technology used in clinical investigations?

For mobile technology, validation ensures that the mobile technology is reliably capturing, transmitting, and recording data to produce accurate, reliable, and complete records. For example, if a wearable biosensor detects a blood glucose level of 87 milligrams per deciliter, the validation should ensure that the value is correctly and reliably captured, transmitted, and recorded in the sponsor's EDC system. Sponsors should validate the mobile technology before use in the clinical investigation. In addition, sponsors should ensure that device and software updates do not affect the reliability of the data that enter the sponsor's EDC system.

Part 11 regulations do not address the performance of wearable biosensors, mobile apps, or portable devices (i.e., the ability to measure what they are designed to measure). For example, validation does not apply to the ability of an activity tracker to accurately and reliably measure the number of steps walked. Although performance of the mobile technology is critical to the clinical investigation, recommendations for the performance of specific mobile technology designed to measure specific biomarkers or physical activity are beyond the scope of part 11 and therefor beyond the scope of this guidance. For mobile technology that meets the definition of device as defined in section 201(h) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321(h)), other regulations and policies may apply.

Q22. What security safeguards should sponsors implement to ensure security and confidentiality of data when mobile technology is used to capture, record, and transmit data directly from study participants in clinical investigations?

The mobile technology must ensure the security and confidentiality of the data when the technology is used in clinical investigations (see 21 CFR 11.10 and 11.30). If the data are transmitted wirelessly from the mobile technology to the sponsor's EDC system in a

[30] See footnote 24.

clinical investigation, the data must be encrypted at rest and in transit to prevent access by intervening or malicious parties (see § 11.30).

For wearable biosensors and other portable or electronic implantable devices, data encryption may be sufficient to ensure the security and confidentiality of the data. For raw data temporarily recorded in large quantities used to produce aggregated data, such as data generated by an accelerometer with a high measurement frequency, it may be impractical to encrypt this data. If large amounts of unintelligible data are temporarily generated by a mobile device, FDA will use enforcement discretion regarding the part 11 encryption control requirement, up until the data is transmitted or summarized, whichever occurs first.

Additional controls may be important when using mobile apps and mobile platforms. In addition to having encryption and basic user access controls in place (see section IV.D.Q17), sponsors should consider implementing additional security safeguards as follows:

- Remote wiping and remote disabling
- Disable function for installing and using file-sharing applications
- Disable automatic software and operating system upgrades
- Firewalls
- Procedures and processes to delete all stored health information before discarding or reusing the mobile device

Q23. Does FDA expect sponsors, clinical investigators, study personnel, and study participants to be trained on the use of a specific mobile technology if the technology is used in a clinical investigation?

Yes. Sponsors, clinical investigators, study personnel, and study participants must be adequately trained on the use of any mobile technology they will use in a clinical investigation (see 21 CFR 11.10(i)). Training should occur before the use of the mobile technology and whenever changes are made (e.g., software or system upgrades) to the mobile technology during the course of the clinical investigation. In addition, clinical investigators and study personnel should periodically reassess and retrain study participants, as necessary, on systems that are more complex or that pose a higher risk to the conduct of the study.

E. Telecommunication Systems

Clinical investigators and study personnel may use many different types of telecommunication systems, such as telephones, email, live chat, and ***telemedicine*** or video conferencing systems to communicate with study participants during the conduct of clinical investigations. Clinical investigators and study personnel may record study-related data obtained during the course of the communications in the study participant's health record or in the case report form.

When these telecommunication systems are interactive and used for real-time communication, the interactions are regarded as similar to face-to-face interactions (i.e., the clinical investigator or study personnel and the study participant actively participate in real-time communication through audio, video, and other live chat communication), and part 11 regulations do not apply to the telecommunication system. In these interactions, there is an opportunity to hear or see the

study participant or to query the source of the text to confirm that the study participant who is interacting with the investigator is the study participant participating in the study.

When these interactive telecommunication systems are used to record source data in a permanent manner, allowing the interactive communication and data to be reviewed at a later date by the sponsor, clinical investigator, study personnel, and FDA, sponsors and other regulated entities should consider whether there are adequate controls in place to ensure that the reliability, confidentiality, and privacy of records are preserved. Sponsors should also consider the processes that are in place to ensure user authentication and to prevent alteration of source data.

V. 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 (§ 11.3(b)(7)). In general, a signature may not be denied legal effect or validity solely because it is in electronic format, and a contract or other 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.[31]

FDA regulations found in part 11 set forth the criteria under which FDA considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to a handwritten signature executed on paper (see 21 CFR 11.1(a)). To be considered equivalent to full handwritten signatures, electronic signatures must comply with all applicable requirements under part 11. Electronic records that are electronically signed must contain information associated with the signing that clearly indicates the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature (see § 11.50). The name, date and time, and meaning are subject to the same controls as electronic records and must be included as part of any human readable form of the electronic record (see § 11.50(b)). In addition, electronic signatures and handwritten signatures executed to electronic records must be linked to the respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means (§ 11.70).

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

FDA does not mandate or specify any particular methods for electronic signatures, including any particular biometric method upon which an electronic signature may be based. Part 11 regulations permit a wide variety of methods to create electronic signatures, including the use of computer-readable ID cards, biometrics, ***digital signatures***, and username and password combinations.

[31] See the Electronic Signatures in Global and National Commerce Act, which was enacted on June 30, 2000 (Public Law 106-229;114 Stat. 464) (15 U.S.C. 7001-7006).

When a document is electronically signed, the electronic signature must be accompanied by a computer-generated, time-stamped audit trail (see §§ 11.10(e) and 11.50(b)). When study participants provide an electronic signature, clinical investigators should ensure that the participants understand the legal significance of the signature.

Q25. How should sponsors and regulated entities verify the identity of the individual who will be electronically signing records as required in 21 CFR 11.100(b)?

Electronic signatures should be instituted in a manner that is reasonably likely to prevent fraudulent use. Therefore, the part 11 regulations require that an organization verify the identity of an individual before the organization establishes, assigns, or otherwise sanctions an individual's electronic signature or any element of such electronic signature (see § 11.100(b)). The electronic signature should also be implemented in a manner that prevents repudiation by the signatory and includes safeguards to confirm the identity of the individual and safeguards to prevent alteration of the electronic signature.

FDA does not specify any particular method for verifying the identity of an individual and accepts many different methods. For example, verifying someone's identity can be done by using information from some form of official identification, such as a birth certificate, a government-issued passport, or a driver's license. In addition, use of security questions to confirm an individual's identity may also be considered.

Q26. When an individual executes a series of signings during a single, continuous period of controlled system access, could the initial logging into an electronic system using a unique username and password be used to perform the first signing and satisfy the requirements found in 21 CFR 11.200(a)?

When an individual logs into an electronic system using a username and password, it is not necessary to re-enter the username when an individual executes a series of signings during a single, continuous period of controlled system access. After a user has logged into a system using a unique username and password, all signatures during the period of controlled system access can be performed using the password alone (see § 11.200(a)).[32] The signed document must contain information that clearly indicates the printed name of the signer, the date and time the signature was executed, and the meaning associated with the signature (see § 11.50).

In addition, in such cases, the signing should be done under controlled conditions that prevent another person from impersonating the legitimate signer. Such controlled conditions may include (1) requiring an individual to remain in close proximity to the workstation throughout the signing session (2) using measures for automatic inactivity disconnect that would de-log the first individual if no entries or actions were taken within

[32] See 62 FR 13430 at 13457 (March 20, 1997).

a fixed, short time frame and (3) requiring that the single component needed for subsequent signings be known to and usable only by the authorized individual.[33]

To make it impractical to falsify records, the electronic signature component executed for initial signing must be used only by its genuine owner (see § 11.200(a)(2)). The electronic signatures must be administered and executed to ensure that attempted use by anyone other than the genuine owners requires collaboration of two or more individuals (see § 11.200(a)(3)).

Q27. What requirements must electronic signatures based on biometrics meet to be considered an accepted biometric method?

Biometrics means "a method 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."[34] Examples of biometric methods may include fingerprints, hand geometry (i.e., finger lengths 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 (§ 11.200(b)). Therefore, suitable biometrics should be uniquely identified with the individual and should not change over time.

FDA does not specify any particular biometric method upon which an electronic signature may be based. Electronic signatures based on biometrics are accepted if they meet the requirements found in the part 11 regulations, as stated earlier in this section (i.e., the signed electronic record must contain pertinent information associated with the signing (see § 11.50), the electronic signatures are subject to the same controls as the electronic records and must be included as part of any human readable form of the electronic record (see § 11.50(b), and the electronic signature must be linked to its respective electronic records (§ 11.70)). In addition, biometrics should be performed based on government and industry standards. For example, the various government agencies and standards development organizations that develop biometric standards include the following:

- National Institute of Standards and Technology
- International Committee for Information Technology Standards
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1/Subcommittee 37
- Organization for the Advancement of Structured Information Standards
- American National Standards Institute

[33] See footnote 32.

[34] See 21 CFR 11.3(b)(3).

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. Compliance with the provisions of part 11 is the basis for FDA's acceptance of any electronic signature system, regardless of the particular technology or brand used. This approach is consistent with FDA's policy in a variety of program areas. For example, FDA does not certify manufacturing equipment used to make drugs or medical devices.

FDA is aware of various systems advertised as Part 11 compliant. While many systems may be capable of implementing Part 11 controls as described in the regulations, Part 11 compliance is dependent on the implementation and processes followed for each application of that system. An extreme example of how a system advertised to be Part 11 compliant may not be Part 11 compliant after implementation is that of a system in which the Part 11 controls can be turned off, or optionally configured. FDA does not certify systems as Part 11 compliant.

APPENDIX I: OTHER GUIDANCES WITH APPLICABLE RECOMMENDATIONS[35]

Guidance for Industry *Part 11, Electronic Records; Electronic Signatures – Scope and Application*

ICH Guidance for Industry *Q9 Quality Risk Management*

Guidance for Industry *Computerized Systems Used in Clinical Investigations*

Guidance for Industry *Electronic Source Data in Clinical Investigations*

Draft Guidance for Industry *Use of Electronic Health Records Data in Clinical Investigations*

Guidance for Industry and Food and Drug Administration Staff *Mobile Medical Applications*

ICH Guidance *E6(R2) Good Clinical Practice – Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(R2)*

Guidance for Institutional Review Boards, Investigators, and Sponsors *Use of Electronic Informed Consent, Questions and Answers*

[35] Draft guidances have been included for completeness only. As draft documents, they are not intended to be implemented until published in final form.

APPENDIX II: GLOSSARY OF TERMS

The following is a list of terms and definitions used in this guidance and their definitions:

Audit Trail is a process that captures details of information, such as additions, deletions, or alterations, in an electronic record without obscuring the original record. An audit trail facilitates the reconstruction of the course of such details relating to the electronic record.

Biometrics means a method 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 (21 CFR 11.3(b)(3)).

Bring Your Own Device (BYOD) refers to the policy of permitting study participants to use their personally owned mobile devices to capture, record, and transmit data in clinical investigations.

Certified Copy is a copy (paper or electronic) of original information that has been verified, as indicated by a dated signature, as an exact copy, having all of the same attributes and information as the original.

Cloud Computing is 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.

Commercial Off-The-Shelf (COTS) Systems refer to commercially available electronic systems (including hardware or software) that can be purchased from third-party vendors.

Critical Data may include documentation of informed consent, drug accountability and administration information, or study endpoints and protocol-required safety assessments.

Customized Electronic Systems refer to systems and software that are specially developed for a specific user, an organization, or a business to meet specific business needs.

Data Element is 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.

Data Element Identifier is 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.

Data Originator is an origination type associated with each data element that identifies the source of the data element's 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).

Digital Signature means an electronic signature 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 (21 CFR 11.3(5)).

Electronic Case Report Form (eCRF) is an auditable electronic record of information that generally is reported to the sponsor on each trial subject, according to a clinical investigation protocol. The eCRF enables clinical investigation data to be systematically captured, reviewed, managed, stored, analyzed, and reported.

Electronic Data Capture (EDC) Systems refer to electronic systems designed to collect and manage clinical trial data in an electronic format.

Electronic Record means 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 (21 CFR 11.3(b)(6)).

Electronic Signature means 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 (21 CFR 11.3(b)(7)).

Electronic Systems refer to systems, including hardware and software, that produce electronic records.

Mobile Applications (Mobile Apps) are software applications that can be executed (run) on a mobile platform (i.e., a handheld commercial off-the-shelf 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. [36] An example includes electronic patient-reported outcomes (ePRO) applications on smart phones.

Mobile Platforms are commercial off-the-shelf (COTS) computing platform, with or without wireless connectivity, that are handheld in nature. Examples include tablet computers, smart phones, or other portable computers.[37]

Mobile Technology refers to portable electronic technology used in clinical investigations that allows for off-site and remote data capture directly from study participants and includes mobile platforms, mobile apps, wearable biosensors and other remote and ingestible sensors, and other portable and implantable electronic devices.

[36] For more information, see the guidance for industry and Food and Drug Administration staff *Mobile Medical Applications*.

[37] See footnote 36.

Source Data are all information in original records and certified copies of original records of clinical findings, observations, or other activities (in a clinical investigation) used for the reconstruction and evaluation of the trial. Source data are contained in source documents (original records or certified copies).

Telemedicine refers to the use of electronic applications, devices, and services, including two-way video, email, smart phones, wireless tools and other forms of telecommunications systems in the provision of health care.

Vendor refers to a third-party supplier not regulated by FDA that sells electronic goods and services to sponsors and other regulated entities.

Wearable Biosensors comprise miniaturized sensors worn as on- or in-body accessories (e.g., watches, bracelets, clothing) that allow for continuous monitoring of physiological, biochemical, and motion signals for both diagnostic and monitoring applications. These wearable biosensors may be paired with mobile platforms (e.g., smart phones). Examples of wearable biosensors include accelerometers, activity trackers, wireless heart rate monitors, pulse oximetry sensors, and glucose sensors.