Electronic Information Systems Policy: **Frequently Asked Questions (FAQ)**

Contents

Administrative 1

General 2

Network Sites 5

Standard Operation Procedures (SOPs) and Documentation 5

Part 11 Compliance 8

Commercial Off the Shelf (COTS) Software 9

Validation 9

References 14

Administrative

1) **Q: How do I submit the EIS Policy Checklist?**

   A: EIS Policy Checklist should be submitted to DAIDSCRSSEISChecklist.sm@ppd.com. Please submit only one Checklist at a time in a single email. When submitting the Checklist, the subject line of the email should include the CRS number (if applicable) and electronic system name, if known.

2) **Q: Is it DAIDS' expectation that the EIS Policy Checklist be completed by an individual at the CRS or Laboratory who has the requisite expertise (i.e., computer validation, technical implementation of the software) at the CRS or Laboratory to best complete the EIS policy checklist?**

   A: Yes, DAIDS expects a CRS or Laboratory to have staff with requisite expertise to best complete the EIS Policy Checklist. A CRS or Laboratory could contract with a subject matter expert, if necessary.

3) **Q: Whom do I contact about technical questions regarding a specific electronic system?**

   A: For technical questions or assistance in regard to an electronic system, please contact the system vendor or software provider.

4) **Q: Whom do I contact for more information about this policy and FAQs?**

   A: Please contact DAIDSCRSSEISChecklist.sm@ppd.com. Please include in the email subject line the CRS number (if applicable), and in the body of the email include the CRS or Laboratory name, and contact name, phone number, and email address.

Electronic Information Systems Policy: **Frequently Asked Questions (FAQ)**

General

5) **Q: Does this policy refer to general computer systems or the electronic health records (EHR)? My understanding is that the FDA does not oversee the EHR?**

   A: The policy refers to electronic systems used to create, modify, maintain, archive, retrieve, or transmit an electronic record required for regulatory authority clinical investigations.

   The United States Food and Drug Administration (FDA) often refers to a specific regulation in the Code of Federal Regulations (CFR), specifically 21 CFR Part 11 which may be more simply referred to as “Part 11”.[1]

   Regarding EHR, the FDA draft guidance “Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11-Questions and Answers” indicates that, “electronic systems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. FDA does not intend to assess compliance of these systems.”[2]

   These electronic systems may produce additional electronic records during the course of patients’ care (for example: 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. Therefore, with regards to the DAIDS Policy, Electronic Medical Record (EMR) systems are not in scope of the DAIDS EIS policy, unless there is a data integration from the EMR to EDC used for DAIDS Clinical Trials. 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.”[5]

6) **Q: In relation to this policy, what does NIAID DAIDS consider to be a formal agreement?**

   A: An agreement between two or more parties with respect to the requirements for electronic systems used in the conduct of NIAID DAIDS Network studies conducted within the HIV/AIDS Clinical Trials Network. A formal agreement usually consists of a document delineating such arrangements and signed and dated by the involved parties.

7) **Q: What is a "content management system"? Can you provide examples of content management systems used in clinical research?**

   A: A content management system (CMS) is a software application that helps users to create, manage, and modify digital content. Examples of content management systems used in clinical research include but are not limited to Veeva eTMF, Documentum, and Open Text.

8) **Q: What is a "software versioning system"? Can you provide examples of software versioning systems used in clinical research?**

   A: The main purpose of a software versioning and revision control system is to capture the differences between software versions. A software versioning system assigns a unique name or number to a specific state of a software to communicate the quality, features, and overall state of the software. Examples of software versioning systems include but are not limited to StarTeam, Subverion, and Azure DevOps Server.

9) **Q: Does direct data capture systems also include telecommunication application systems (apps) used to collect data via Multimedia Messaging Service?**

   A: Yes, data can be captured via Multimedia Messaging Service (MMS). MMS allows data to be sent by attaching an image, sound file, video, or other forms of media.

10) **Q: When the policy says access to all electronic systems under the scope of this policy is revoked "promptly" upon staff departure, what does this mean?**

    A: There should be processes and procedures in place at the clinical research sites to ensure access to all electronic systems is revoked upon staff reassignment or departure. A site must notify a DMC and DAIDS of staff departure within 5 business days. It is recommended that a timeline be included within a DMC SOP by which the access will be revoked after being notified of staff departure from an institution, and 5 business days is the recommended timeframe. DAIDS recommends that the course be followed through to completion such that the DMC confirms access is revoked.

11) **Q: What is an "outsourced electronic service"?**

    A: According to FDA draft guidance "Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11-Questions and Answers," outsourced electronic service are services that the sponsors and other regulated entities have chosen to outsource in order to process data for FDA-regulated clinical investigations.[2] An example of an outsourced electronic service may include data management services including cloud computing services. It is the responsibility of the sponsor to ensure the reliability and confidentiality of the data including an assessment of risks associated with using an outsourced electronic service.

12) **Q: What is an Open system?**

    A: *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

13) Q: What is a closed system?

A: *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

14) Q: What is a data originator?

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

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

Data elements can be transcribed into the eCRF from paper or electronic source documents. The authorized person transcribing the data from the source documents is regarded as the data originator. For these data elements, the electronic or paper documents from which the data elements are transcribed are the source. These data must be maintained by the clinical investigator(s) and available to an FDA inspector if requested (e.g., an original or certified copy of a laboratory report, instrument printout, progress notes of the physician, the study subject's hospital chart(s), nurses' notes).[5]

Network Sites

15) Q: Does this policy apply to non-network sites?

A: This policy does not apply to sites outside of the NIAID HIV/AIDS Clinical Trial Networks.

16) Q: How do I determine if my CRS or Laboratory is participating in a NIAID HIV/AIDS Network trial?

A: HIV/AIDs Clinical Trials Networks are sponsored and/or supported by NIAID DAIDS and include AIDS Clinical Trials Group (ACTG), HIV Prevention Trials Network (HPTN), HIV Vaccine Trials Network (HVTN), and the International Maternal Pediatric Adolescent AIDS Clinical Trial group (IMPAACT). See the HIV/AIDS Network Coordination (HANC) website for additional information on HIV/AIDS Network Trials sponsored and/or supported by DAIDS.

Standard Operation Procedures (SOPs) and Documentation

17) Q: The policy states written standard operating procedures should be established for "each" electronic system. Do I really need to have an SOP for each electronic system, or can an overarching SOP be established outlining all electronic systems within the scope of this policy?

A: It is best practice to have an individual SOP for each electronic system; however, it is acceptable to establish a written policy defining the requirements of all electronic systems with the scope of this policy, in addition to, system-specific SOPs.

18) Q: What does NIAID DAIDS consider to be "adequate documentation" to support that SOPs are being followed?

A: Adequate documentation includes any original document, information, or data created, received, or maintained that functions as evidence of intentions or activities. It can describe methods, conduct, and/or results of an activity, the factors affecting an activity and the actions taken or decisions made in support of an activity. Examples of documentation sites may generate to demonstrate that they are following their EIS Policy related SOPs include but are not limited to the following: training materials, onboarding materials, electronic information systems documentation, roles and responsibilities, and Delegation of Duties documentation.

19) **Q: Can the electronic data originator and the user access of the respective electronic system be maintained in separate lists?**

A: Yes, this information may be maintained in separate lists. If maintained separately, the information must remain consistent between the lists. According to the FDA Guidance "Electronic Source Data in Clinical Investigations," it is recommended that "the sponsor develops, maintain, and make available a list of authorized data originators. Lists of electronic data originators should be available at each site."[5] When the 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. 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.

20) **Q: If a sponsor owns the system, should the sponsor send Part 11 compliance documentation to the site?**

A: If the site is relying on the sponsor system to create, modify, maintain, archive, retrieve, or transmit an electronic record required for FDA regulated clinical investigations and these records are considered the source for the site, this may be considered an "outsourced electronic service" and should be validated as appropriate.

In other words, if your site is relying on the sponsor system to be the system of record to meet FDA compliance, then Part 11 applies. However, most sponsor systems are intended to be helpful tools, and are not the site's system of record. Therefore, it is not common for sponsors to send Part 11 documentation to investigators sites.

However, if the sponsor system is the system of record (such as direct entry of data into the eCRF[5]), then your site should obtain documentation from the DMC that includes, but is not limited to, a description of standard operating procedures and confirmation that validation documentation is available at the DMC to establish that the outsourced electronic service functions in the manner intended.

For non-COTS/in-house systems under the scope of this policy, the end user validation may be carried out by either the software owner organization/entity or by the end user/entity.

For systems provided by the sponsor/DMC that are locally installed at a site/lab: It is the expectation that the site/lab will submit a separate checklist for their instance of the software.

21) Q: Where can I find the list of systems for which the DMC will be submitting the checklist?

A: Here is the list of validated systems at the DMC (Frontier Science (FS) and SCHARP) for which the sites need not submit the EIS checklist. The DMCs will be posting the Validation Summary Report/Validation certificate and the EIS checklist on their portals. Below are the links for FS and SCHARP respectively. Access to the portal will need to be requested by each site/user.

I. Frontier Science (FS):

1. Biological Sequencing System (BSS)
2. Data Submission System (DSS)
3. Medidata Rave
4. Protocol Deviation Reporting System
5. Query System (QS)
6. Study Enrollment System (SES)
7. Therapeutic Drug Monitoring Dose Recommendation Utility (TDM)
8. LDMS (refer to Question 36 of the FAQ)

FS portal Link:
https://frontierscience.org/apps/cfmx/apps/common/validationcertificates/index.cfm

FS portal access request: usersprt@fstrf.org

II. SCHARP:

1. Atlas
2. Medidata Rave
3. DatStat Illume
4. Lab Upload Tool
5. SpeQs (Specimen QC)

ATLAS portal link:
https://atlas.scharp.org/cpas/project/Collaborators/Computer%20System%20Validation%20Portal/begin.view

ATLAS portal access request: support@scharp.org

Part 11 Compliance

22) **Q: Does Part 11 apply if we are keeping both electronic AND paper copies (such as wet ink copies that are scanned and saved to our shared drive)?**

    A: Simply put, Part 11 applies to your site if you're relying on electronic records or electronic signatures to meet an FDA requirement. The FDA's draft guidance[2] on Part 11 indicates that if a "regulated entity intends to use an electronic copy in place of the paper source data (intends to destroy the paper source data), then Part 11 regulations apply to the electronic system used to create the copy (see 21 CFR 11.10 and 11.30)."[1] If a true copy of a paper record is created by scanning the original paper record thus creating an electronic record, the scanned copy should be "certified" per Good Documentation Practices (GDP) and maintained in a Part 11 compliant system.[8]

23) **Q: Not all cloud solutions are necessarily Part 11 compliant. How would one know?**

    A: Ask the vendor if they are Part 11 compliant and ask them to provide documentation. Ask if they have undergone a third-party assessment for validation or are willing to. If they haven't, you may want to audit the vendor. Even though you may be purchasing a system, you're still responsible at the site to make sure that the system is Part 11 compliant. So, even if the vendor says it is Part 11 compliant, your site is still responsible for doing your due diligence to ensure it and documenting that it is so.

24) **Q. Regarding the application of Part 11 to our site, we utilize a cloud based clinical trial management system (CTMS) which houses participant demographics (not procedure/health records). Is the CTMS vendor responsible for being Part 11 compliant? Is our site accountable in this case?**

    A: 21 CFR Part 11 applies to your site if you're relying on electronic records or electronic signatures if the CTMS falls within the scope of the EIS Policy. Additionally, you cannot outsource your regulatory compliance obligations, so you're still responsible. You're still the one that has to answer to the FDA about whether your data are reliable. This means that you need to ensure due diligence and properly vet any potential vendor and to verify they can produce documentation of validation and Part 11 compliance.

25) **Q: Is Part 11 applicable if my site uses a secure drive (limited access) to archive a portion of the regulatory binder?**

    A: If you intend to use an electronic copy in place of the paper source data (intend to destroy the paper source data), then Part 11 regulations would apply to the electronic system used to create the copy. True copies of a paper record created by scanning the original paper record thus creating an electronic record, should be "certified" per Good Documentation Practices (GDP) and maintained in a Part 11 compliant system.[8] Using an electronic resource, such as a durable electronic storage device is an acceptable method to archive study-related records at the end of the study. You should ensure that the integrity of the original data and the content and meaning of the record are preserved. The electronic records must be archived in such a way that the records can be retrieved, searched, sorted, or analyzed. The sponsors, sites, and other regulated entities should provide electronic copies with the same capability to FDA during inspection if it is reasonable and technically feasible.

Commercial Off the Shelf (COTS) Software

26) **Q: In the Responsibilities section of the Policy, it mentions non-COTS/in-house systems which seems those may be in scope if proper risk mitigations are in place. Is this the case?**

    A: Yes. For non-COTS/in-house systems under the scope of this policy, the end user validation may be carried out either by the software owner organization/entity or by the end user/entity. If a system is developed in-house or through a vendor, the system must be evaluated, and risks should be assessed to ensure appropriate measures are taken to comply with Part 11.

27) **Q: When the policy says Commercial Off the Shelf (COTS) should be "adapted as necessary", what does this mean?**

    A: If a COTS system is used, the system still must be evaluated to ensure the software is appropriate and sufficient for the site's intended use. Due to that fact that COTS software is usually written with proprietary information, the vendor may refuse to provide full validation documentation. However, as mentioned in the FDA guidance documents they should provide documentation to support that the system functions as intended.

Validation

28) **Q: Is it expected that a risk assessment be performed at the system level for each electronic system prior to system utilization?**

    A: In order to evaluate the risk of an electronic system, a risk assessment must be performed and documented which may include within its scope the procedural and electronic activities throughout the data lifecycle. Mitigation and control strategies identified to be implemented should be appropriate to the criticality of data and the level of risk to human subject and study results.

29) Q: How does your site/organization currently manage electronic regulatory and trial documents? Does your site/organization currently have a Validation Plan?

A: According to FDA 21 CFR Part 11 and ICH-GCP E6 (R2), clinical research sites that rely on electronic records or electronic signatures are required to perform validation to ensure their system operates correctly. While the FDA does not indicate how to meet this requirement, you still must demonstrate how you intend to perform validation.

30) Q: Do network shared drives really need to be validated?

A: Any essential documents stored electronically for FDA regulated research fall under Part 11 regulation. So, if you’re storing important documents (such as 1572s, consent forms, protocols, any portion of participant records, accountability records and more) in a shared drive, and relying on this information to make study decisions, that shared drive should be validated.

31) Q: How do you decide what is "critical" and should be tested?

A: The FDA recommends a risk-based approach to validation, so it depends on the impact the system will have on data quality and integrity, as well as participant safety. Critical components are those that have impact on the data quality and integrity of the study as well as participant safety. For example, components related to data and systems that an IRB may use to make their determinations when there are critical outcomes that will result from using these systems would be considered critical. In the draft guidance[2], the FDA provides examples of critical records such as records containing laboratory and study endpoint data, information on serious adverse events and study participant deaths, information on drug and device accountability and administration.

When using a risk-based approach for validating electronic systems, 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.[2]

32) Q: I often hear the terms Validation and Qualification when referring to computerized systems. What's the difference between those two terms, if any?

A: Validation is the confirmation that the requirements for the specific intended use or application of the computer system have been met. According to the FDA draft guidance[2], “validation may include, but is not limited to, demonstrating correction installation of the electronic system and testing of the system ensure that it functions in the manner intended.”

The qualification process aids in determining when a system is reliable and stable enough to support validated processes. From an IT perspective, the terms qualification or installation qualification, are actually very different concepts. Installation qualification refers to ensuring the software or the system being implemented is installed correctly. Qualification refers to systematic testing of the system.

33) **Q: Once a system is validated, does it need to be revalidated annually?**

A: Change control involves making modifications to the system. Systems should be validated or revalidated when there are significant changes. There may be minor modifications such as minor tweaks such as fixing bugs that don't warrant full revalidation, whereas new features or critical updates would require revalidation, or validation of those new components. It is really about confirming integrity of the system, and if there are any changes, those changes are tested prior to implementation.

34) **Q: If the sponsor is providing software, for example EDC software, are they responsible for validation? Or is the site required to have their own separate policy as well?**

A: It depends on what the intended purpose is for that particular system. If you intend to use it as your authentic source for this data, there should be some type of process in place, whether you're gathering their validation plan or the outcomes of their validation for your records. If you intend to rely on those systems, then you will be held accountable for making sure that that system complies with your requirements. So, it really depends on your intentions for those systems, but if you intend to rely on it, then you need to do your due diligence and gather that information from the site's perspective.

35) **Q: Is there anything in the regulations that we can use to go to vendors with asking for their validation documents? Most vendors are protective of their systems and validation documents.**

A: Reference the FDA draft guidance document "Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11-Questions and Answers"[2].

Further, per ICH GCP E6 (R2) Section 4.2.6, "If the investigator/institution retains the services of any individual or party to perform trial-related duties and functions, the investigator/institution should ensure this individual or party is qualified to perform those trial-related duties and functions and should implement procedures to ensure the integrity of the trial-related duties and functions performed and any data generated."[4]

If the vendor is not willing to provide adequate documentation, you may want to consider another vendor.

36) **Q: How do I request assistance with end user validation and testing for LDMS (windows or web version)?**

A: Laboratory staff can request assistance from Frontier Science by submitting a request through the LDMS validation web page available on the LDMS public website (link included below). LDMS laboratories have access to numerous validation resources and documents on the LDMS website to assist users with end user testing and validation efforts in general. LDMS validation website: https://www.ldms.org/resources/validation/

37) **Q: What documentation can a site reasonably expect a vendor to release to them, since most vendors consider their documentation proprietary.**

A: For commercial off the shelf systems (COTS) that perform functions beyond office utilities such as COTS EDC 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.

38) **Q. If a site used RedCAP to collect data for investigator-initiated studies that will later be sent to the FDA for approval, must the site have a System Validation process for their RedCAP?**

A: The FDA has identified the following records as being applicable to Part 11:

If any of the following hold true for your use of RedCAP, then the answer is “yes” you must have a validation process.

- 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 21 CFR 11.1(b))[1]
- Electronic signatures required for clinical investigations intended to be the equivalent of handwritten signatures, initials, and other general signatures

For example, an investigator must maintain records of drug disposition and case histories for any individual that receives the investigational product. If your site keeps an electronic version of those disposition logs and case histories, then Part 11 applies to you. Part 11 applies to you regardless of whether you're using an in-house system or a vendor system.

39) **Q: If the vendor provides validation documents as evidence and upon review internally, it meets our requirements, do we (as the investigator site) still need a validation document?**

A: This would depend on your Standard Operating Procedures to define what you deem acceptable. The extent of any validation procedures completed by the site should be tailored to the nature of the system and its intended use.

40) **Q: If you validate in a test/validation system, should you revalidate once you're in the live/production system? Can we skip the test/validation step and validate directly in production?**

A: From a software perspective, system testing should occur prior to live utilization (production). It is best practice to validate and revalidate any critical system changes in a validation environment prior to utilization and deployment of the critical updates to the live environment. The system does not need to be revalidated once you're in the production system, unless any changes are made and, as per your procedures, meets the requirements for revalidation.

41) **Q: If revalidation is required after a major system upgrade or version change, what timeline is expected for institutions/sites to submit a new EIS policy checklist?**

A: As part of the change control process, revalidation of electronic systems is required to follow the DAIDS EIS policy. In compliance with the DAIDS EIS policy guidelines, a new electronic system has to be validated (21 CFR Part 11 compliant) for its intended purpose prior to use, and this applies to version changes and systems upgrade. A new DAIDS EIS policy checklist should be submitted when there are significant changes, such as a version change, or any major changes such as a system upgrade, after initial validation. DAIDS expects new versions of an electronic system or upgraded electronic systems to be validated not later than one month from the new version release or system upgrade date. For appropriate assessment and for timely compliance, DAIDS recommends that an EIS policy checklists be submitted not later than two weeks from the new version release date.

42) **Q: What are some examples of electronic systems that fall under the scope of the EIS Policy for which a checklist should be submitted?**

A: The DMCs post the EIS validation reports EIS on their portals. Refer to Q21 above for details. Here are some examples of systems for which the EIS checklist needs to be submitted.

- Laboratory Remote temperature monitoring systems for refrigerators/freezers.

- Electronic signatures platform e.g., DocuSign

- Electronic systems used to store Clinical research Site SOPs

- Pharmacy remote temperature monitoring systems for refrigerators/freezers.

- Web applications on a centralized platform used to facilitate rapid and secure data collection and storage. A checklist is required if documents are essential documents.

- Applications providing automation tools for an investigational drug service, such as it is used by the Investigational Drug Pharmacy (IDS) to track Investigational Products.

Refer to question 21 for information about where to find the list of systems for which the DMC will be submitting a checklist and the links for to DMC portals for EIS checklist information.

References

1 – 21 CFR Part 11

2 – FDA Draft Guidance for Industry: Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers (June 2017)

3 – FDA Guidance for Industry: Use of Electronic Health Records Data in Clinical Investigations (July 2018)

4 – International Council For Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH), Good Clinical Practice [ICH-GCP E6 (R2)]

5 – FDA Guidance for Industry: Electronic Source Data in Clinical Investigations (September 2013)

6 – FDA Guidance for Industry: Part 11, Electronic Records; Electronic Signatures - Scope and Application (September 2003)

7 – FDA Guidance for Industry: Computerized Systems Used in Clinical Investigations (May 2007)

8 – WHO Final Annex 5, Guidance on Good Data and Records Management Practices (TRS-996)