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

Contents

Administrative

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

A: An EIS Evaluation Checklist should be submitted to DAIDSCRSSEISChecklist.sm@ppd.com.

Please submit only one (1) EIS Evaluation Checklist at a time in a single email for tracking purposes.

When submitting the EIS Evaluation Checklist, the subject line of the email should include the entity (CRS, laboratory, or organization) name, Clinical Research Site (CRS) number (if applicable), and electronic system name.

2) Q: What timeline is expected for entities to submit a new EIS Evaluation Checklist following a revalidation?

A: DAIDS expects new EIS Evaluation Checklists to be submitted within 30 days of validation/revalidation or implementation of new Major system version.

It is expected that any changes to the system as initially submitted that would impact the data listed or alter the way in which the EIS Evaluation Checklist was filled out would prompt a new checklist to be submitted. Examples include changes in the validated state that would impact the Major version number listed, by whom the validation was performed, or changes to system capabilities, as well as changes in intended use of the system.

3) **Q: Is it DAIDS' expectation that the EIS Evaluation Checklist be completed by an individual at the entity who has the requisite expertise (i.e., computer validation, technical implementation of the software) to best complete the EIS Evaluation Checklist?**

   A: Yes, DAIDS expects an entity to have staff with requisite expertise to best complete the EIS Evaluation Checklist. An entity can contract an external subject matter expert (SME), if necessary.

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

   A: For technical questions or assistance regarding an electronic system, please contact your local Help Desk or consultant working on the electronic system, as applicable. Alternatively, you can contact the system vendor or software provider.

5) **Q: Whom do I contact for more information about the EIS Policy and FAQs?**

   A: Send inquiries to 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 entity name, contact name, phone number, and email address.

General

6) **Q: Does the EIS Policy include electronic health records (EHR) systems?**

   A: Yes, when they are integrated with an electronic data capture (EDC) system and when records will be included as part of a clinical trial.

   Food and Drug Administration (FDA) Guidance for Industry, Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations Questions and Answers, 2023 states, 21 CFR part 11 requirements apply to electronic records from real-world data (RWD) sources that were created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations or submitted to the Agency, even if such records are not specifically identified in FDA regulations. FDA acknowledges that there may be instances when electronic records from RWD sources were not originally created in part 11-compliant systems with the intention of being submitted to FDA as part of a marketing application, but such records can be used for that purpose. Sponsors that intend to rely on such data in support of a marketing application should ensure the quality and integrity of such electronic records.[2]

   As stated in FDA Guidance for Industry Use of Electronic Health Records Data in Clinical Investigations (2018), it still holds true that FDA does not intend to assess compliance of EHR systems with 21 CFR Part 11, although, if the data from an EHR is, or could be used as part of a DAIDS Clinical Trial, outside of an integration with an EDC, the EHR must meet the requirements of 21 CFR Part 11. FDA must have the ability to verify the quality and integrity of the data during FDA inspections.

7) **Q: In relation to the EIS Policy, what does NIAID DAIDS consider to be a formal agreement?**

   A: A formal agreement is an agreement between two (2) or more parties with respect to the requirements for electronic information 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 that is signed and dated by the involved parties.

8) **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 system that provides users the ability to create, edit, collaborate on, publish, and store digital content usually supported through workflows and content categorization. Examples of content management systems used in clinical research include but are not limited to Veeva eTMF, Documentum, and OpenText.

9) **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 Git, StarTeam, Apache Subversion, and Azure DevOps Server.

10) **Q: When would a new EIS Checklist need to be submitted, for example upon a major version change? Can you explain a major version change?**

   A: A major version change is in reference to the numerical designation of the software provided by the vendor or software provider. The major version refers to the first number in the series of numbers, for example, with the version number 3.2.1, 3 equals the major version number. Subsequently, 2 equals the minor version number and 1 equals the patch version number. Therefore, a major version change in this situation would be when the software moves to version 4 or higher. Major versions introduce significant changes and/or new features as opposed to minor versions which focus on incremental improvements and fixes. Some systems, usually cloud based, rely on releases rather than the standard software versioning, for example Veeva provides three (3) releases each year (e.g., 24R1, 24R2, 24R3). Each release is accompanied by release notes and must be assessed to determine the impact of the changes to your intended use. In these cases, a new EIS Evaluation

Checklist would need to be submitted under the same circumstances as a major version – the introduction of significant changes and/or new features.

It is expected that a new EIS Evaluation Checklist be submitted when any changes are made to the system that would impact the data listed on the original EIS Evaluation Checklist. In addition to a Major Version change some examples include: by whom the validation was performed (e.g., in-house vs vendor or in-house and vendor), changes to system capabilities (e.g., addition of use of electronic signature), changes in intended use of the system (e.g., expanded clinical use of the system), or revalidation or expanded validation of the system (e.g., additional validation of system interfaces).

11) **Q: Do 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.

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

A: The entity must notify the Data Management Center (DMC) and DAIDS of staff departure within five (5) business days. There should be a procedure in place at the entity to ensure access to all electronic information systems is revoked upon staff reassignment or departure. It is recommended that the timeframe to complete access revocation be within the five (5) business days in which the DMC and DAIDS are to be notified.

It is recommended that the DMC also have a procedure that includes a process by which access will be revoked within five (5) business days after being notified of staff reassignment or departure by the entity and follow through to completion such that the DMC confirms access has been revoked.

13) **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. In Open Systems the users and signatories are not known in advance of accessing the system and would create their own user accounts. Examples of Open Systems include LinkedIn or Gmail.

14) **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. In Closed Systems the system owner knows the identity of all users and signatories and grants and controls their access rights to the system. Closed Systems are those used throughout clinical trials with examples represented within the EIS Policy such as Electronic Data Capture (EDC) Systems, Laboratory Information Management Systems (LIMS), and electronic Trial Management File (eTMF) systems.

15) Q: Is a validation certificate adequate to demonstrate validation?

A: Although a validation certification may be requested during an audit it, alone, is not adequate to demonstrate validation – full validation documentation is required per EIS Policy (e.g., requirements specification, validation plan, testing, traceability matrix, summary report) to be readily available whether it is produced by the entity or the software vendor.

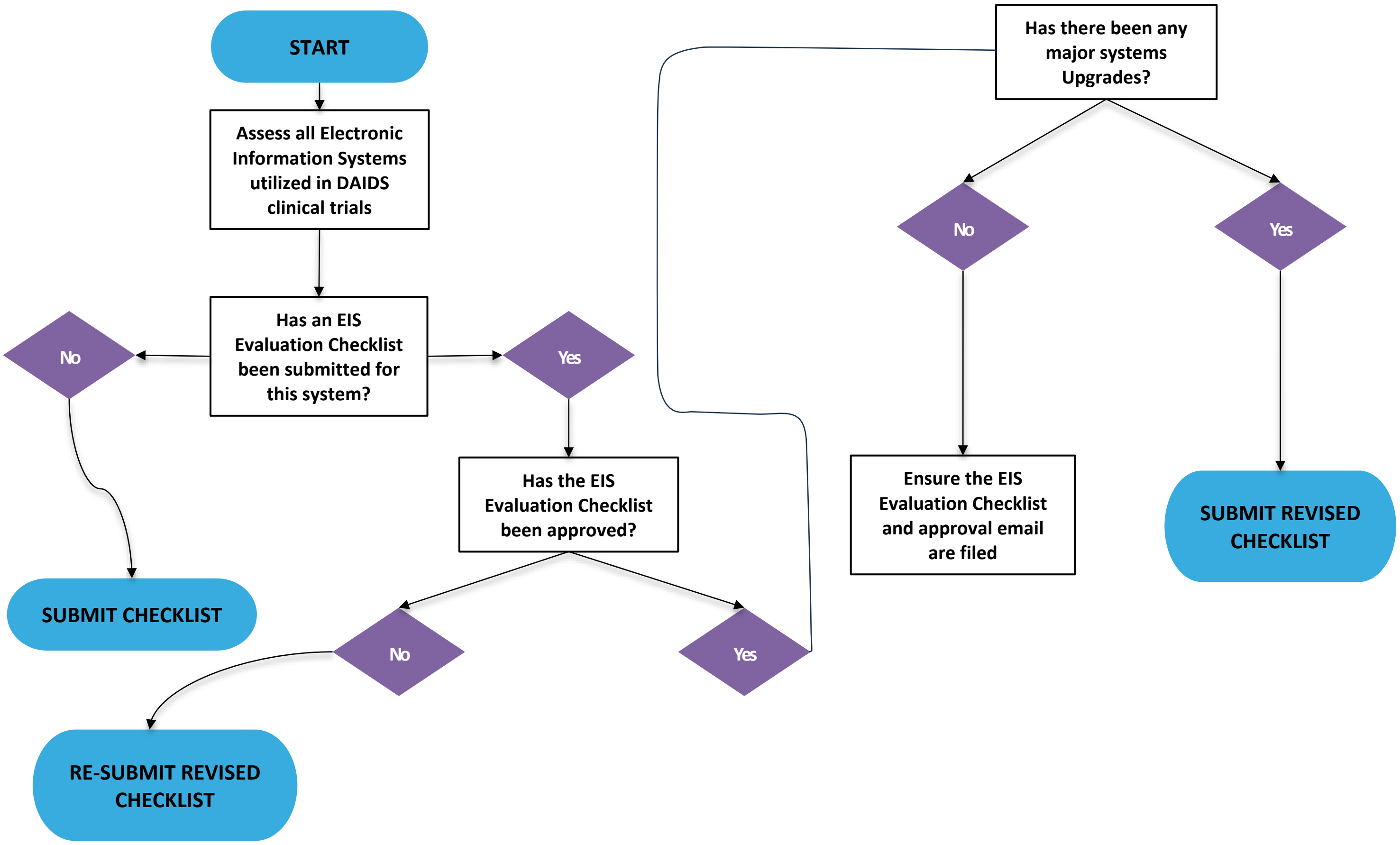
16) Q: What is the best way to comply with the new EIS Policy implementation?

A: Compile a list of all electronic information systems that support DAIDS clinical trials. For each of the systems on the compiled list, complete and submit an EIS Evaluation Checklist based on the criteria found in the following table and flow chart.

WHEN TO SUBMIT AN EIS EVALUATION CHECKLIST	
SCENARIO	**REQUIREMENTS FOR EIS EVALUATION CHECKLIST COMPLETION**
EIS Evaluation Checklist NOT Previously Submitted: Electronic information system utilized in DAIDS clinical trials for which an EIS Evaluation Checklist has NOT been previously submitted.	Complete Section 1.0 to determine whether the electronic information system is within the scope of the EIS Policy. • If electronic information system is determined to be out of scope, proceed to Sections 21.0 and 22.0 – Review Acknowledgement. • If electronic information system is determined to be within scope, complete the remainder of the EIS Evaluation Checklist, as applicable.
EIS **E**valuation Checklist Previously Submitted**:** Major system upgrade of electronic information system assessed in previously submitted EIS Evaluation Checklist.	Complete and resubmit an EIS Evaluation Checklist for the newly upgraded version of the system. Complete all applicable sections of the EIS Evaluation Checklist as described above.
EIS Evaluation Checklist Previously Submitted:	Complete and resubmit an EIS Evaluation Checklist for the current version of the

Previously submitted EIS Evaluation Checklist that was not approved by DAIDS.	system. Complete all applicable sections of the EIS Evaluation Checklist as described above.

EIS COMPLIANCE ASSESSMENT WORKFLOW


START
Assess all Electronic Information Systems utilized in DAIDS clinical trials
Has an EIS Evaluation Checklist been submitted for this system?
No
Yes
SUBMIT CHECKLIST
Has the EIS Evaluation Checklist been approved?
No
Yes
RE-SUBMIT REVISED CHECKLIST
Has there been any major systems Upgrades?
No
Yes
Ensure the EIS Evaluation Checklist and approval email are filed
SUBMIT REVISED CHECKLIST

17) Q: What is a Data Originator?

A: Data Originator means the original source of data. Each data element is associated with an origination type that identifies the source of its capture in the electronic Case Report Form (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
- Digital Health Technologies (DHT) such as activity trackers or glucose sensors

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 be made 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).[4]

Network Sites

18) Q: Does the EIS Policy apply to non-network sites?

A: No, the EIS Policy does not apply to sites outside of the NIAID HIV/AIDS Clinical Trial Networks.

19) 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 Operating Procedures (SOPs) and Documentation

20) **Q: The EIS Policy states written SOPs should be established for "each" electronic information system. Do I really need to have an SOP for each electronic information system, or can an overarching SOP be established outlining all electronic information systems within the scope of the EIS Policy?**

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

21) **Q: What does 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 entities may generate to demonstrate that they are following their EIS Policy related SOPs include but are not limited to the following: training materials and documentation of training, onboarding materials, electronic information systems documentation, roles and responsibilities, and Delegation of Duties documentation.

22) **Q: Can the electronic data originator and the user access of the respective electronic information 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 for Industry, Electronic Source Data in Clinical Investigations (2013), it is recommended that the sponsor develop, maintain, and make available a list of authorized data originators. Lists of electronic data originators should be available at each site.[4]

    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.

23) **Q: If a sponsor owns the electronic information system, should the sponsor send 21 CFR Part 11 compliance documentation to the entity?**

A: If the sponsor system is the system of record, such as direct entry of data into the electronic Case Report Form (eCRF), then the entity should obtain documentation from the Data Management Center (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 electronic information system functions in the manner intended.

For in-house systems within scope of the EIS 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 an entity, it is the expectation that the entity will submit a separate checklist for their instance of the software.

24) **Q: Where can I find the list of systems for which the Data Management Center (DMC) will be submitting an EIS Evaluation Checklist?**

A: Here is the list of validated systems at the DMC (Frontier Science (FS) and SCHARP). There is no need for site and laboratories to submit an EIS Evaluation Checklist for the systems listed below. The DMCs will be posting the Validation Summary Report/Validation Certificate and the EIS Evaluation Checklist on their portals. Below are the links for FS and SCHARP respectively. Access to the portals will need to be requested by each entity by utilizing the portal access request links below.

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)
9. STARS
10. Apache Subversion

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)
6. Delphi
7. REDCap Cloud (RCC)

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

ATLAS portal access request: support@scharp.org

21 Code of Federal Regulation (CFR) Part 11 Compliance

25) Q: Does 21 CFR Part 11 apply if keeping both electronic AND paper copies (such as wet ink copies that are scanned and saved to a shared drive)?

A: Yes, if an entity intends to maintain and retain a copy of an electronic record required for the clinical investigation in place of an original paper or original electronic record, the copy maintained and retained should be a certified copy. A certified copy is a copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information, including data that describes the context, content, and structure, as the original.[2] It is FDA's expectation that the entities will ensure that records are maintained throughout the records' retention period per applicable regulations and, as applicable, be made available to FDA during an inspection.[2]

26) Q: Not all cloud solutions are necessarily 21 CFR Part 11 compliant. How would one know?

A: Evaluation of vendor capabilities is generally achieved through an established auditing and/or vendor management program. It is important to remember that purchased systems such as cloud solutions are not designed to be 21 CFR Part 11 compliant, they are designed to be 21 CFR Part 11 capable. Compliance to Part 11 is established through documented validation of the individual purchasers intended use of the system. Thus, the entity is responsible for ensuring 21 CFR Part 11 compliance of electronic information systems that fall within EIS Policy Scope. Each entity needs to ensure due diligence and properly vet any potential vendor to verify they can produce documentation of validation to support the entities established standards and requirements for 21 CFR Part 11 compliance.

27) **Q. Regarding the application of 21 CFR Part 11 when utilizing a cloud based clinical trial management system (CTMS) which houses participant demographics (not procedure/health records), is the CTMS vendor responsible for being 21 CFR Part 11 compliant? Is the entity accountable in this case?**

A: The entity is responsible for ensuring 21 CFR Part 11 compliance of electronic information systems that fall within EIS Policy Scope. Each entity needs to ensure due diligence and properly vet any potential vendor to verify they can produce documentation of validation and Part 11 compliance.

28) **Q: Is 21 CFR Part 11 applicable when utilizing a secure drive (limited access) to archive a portion of the regulatory binder?**

A: Yes, the entity is responsible for ensuring 21 CFR Part 11 compliance of electronic information systems that fall within EIS Policy Scope. It is FDA's expectation that the entities will ensure that records are maintained throughout the records' retention period per applicable regulations and, as applicable, made available to FDA during an inspection. As part of an inspection, entities may be requested to provide all records and data needed to reconstruct a clinical investigation, including associated metadata and audit trails. There are various ways to retain electronic records, including durable electronic storage devices and using cloud computing services. Entities must ensure the authenticity, integrity, and confidentiality of the data from the point of creation and ensure that the meaning of the record is preserved.[2] The electronic records must be archived in such a way that the records can be retrieved, searched, sorted, or analyzed. The entities should provide electronic copies with the same capability to FDA during inspection if it is reasonable and technically feasible.

Validation

29) **Q: In the Responsibilities section of the EIS Policy, it mentions in-house software systems. Are these within EIS Policy Scope?**

A: Yes, for in-house systems under the scope of the EIS 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 21 CFR Part 11.

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

A: Yes, in order to evaluate the risk of an electronic information 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 subjects and study results.

31) **Q: Is a Validation Plan required for electronic information systems within EIS Policy scope?**

A: Yes, validation activities should be planned, documented, and approved. The validation plan should include information on the validation methodology, the risk-based approach taken and if applicable, the division of tasks between the responsible party and a service provider.[3]

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

A: Yes, if the shared drive is being used for regulated or clinical data and records. It is FDA's expectation that the entities will ensure that records are maintained throughout the records' retention period per applicable regulations and, as applicable, be made available to FDA during an inspection.[2] Per 21 CFR Part 11, systems used to create, modify, maintain, archive, retrieve, or transmit electronic records must be validated.

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

A: 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. Other examples of critical records include 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 information systems, entities should consider 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 the attributes and intended use of the electronic system used to produce the record.

34) **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 a specific intended use of a computer system has been met.

Qualification refers to systematic testing of the computer system.

For example, various qualification activities (installation, operational, and performance or IQ/OQ/PQ) are a part of an overall validation.

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

A: No, systems do not require annual revalidation. A full system validation or revalidation is required when there are significant changes to the system, such as a Major version upgrade. There should be an on-going change control process in place to maintain the validated state of the system between validations. In addition, periodic system reviews should be conducted to assess and document whether the system can still be considered to be in a validated state, or whether individual parts or the whole system needs revalidation.[3]

36) **Q: If the sponsor is providing software, for example EDC software, are they responsible for validation or is the entity required to have their own System Validation procedure?**

A: The entity is expected to have their own System Validation procedure. Even if the system of record is provided and validated by the Sponsor, it is the responsibility of the entity to obtain documentation from the Data Management Center (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 electronic information system functions in the manner intended. The entity's System Validation procedure would provide the details and requirements necessary to prove the system was functioning in the manner intended by the entity.

37) **Q: Are there any regulatory documents that can be used when going to a vendor to request their validation documentation to support the request? Does it include the validation documentation an entity can expect to have access to?**

A: Yes, Guideline on computerized systems and electronic data in clinical trials, 2023[3] can be referenced.

Specifically, Annex 2 Computerised systems validation, A2.1 General principles, which states, if the responsible party relies on the vendor's validation documentation, inspectors should be given access to the full documentation and reporting of the responsible party's examination of the vendor, the validation documentation should be made available to the inspectors in a timely manner, irrespective of whether it is provided by the responsible party or the vendor of the system. Contractual arrangements should be made to ensure continued access to this documentation for the legally defined retention period even if the sponsor discontinues the use of the system or if the vendor discontinues to support the system or ceases its activities.[3]

Annex 1 Agreements states, in the context of clinical trials, system-documentation (including e.g. software/system validation documentation, vendor standard operating procedures (SOPs), training records, issues log/resolutions) should be retained for the full retention period. It should be clear from the agreement which party is retaining and maintaining which documentation and how and in what format that documentation is made available when needed (e.g., for an audit or an inspection). If appropriate agreements cannot be put in place due to the inability or reluctance of a service provider to allow access to important documentation (e.g., system requirements specifications) or the service provider is unwilling to support pre-qualification audits or regulatory inspections, systems from such a service provider should not be used in clinical trials.[3]

38) **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/.

39) **Q: If an entity used RedCAP to collect data for investigator-initiated studies that will later be sent to the FDA for approval, must the entity have a System Validation procedure for their RedCAP?**

A: Yes, if any of the following hold true for your use of RedCAP you must have a System Validation procedure.

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

- Records needed for FDA to reconstruct a clinical investigation that are maintained and archived under predicate rules in electronic format in place of paper format or where the electronic record is relied on to perform regulated activities.
- Records submitted to FDA in electronic format under predicate rules, even if such records are not specifically identified in FDA regulations.[2]

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

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

A: The entity may rely on validation documentation provided by the vendor of a system if they have assessed the validation activities performed by the vendor and the associated documentation as adequate; however, they may also have to perform additional validation activities based on a documented assessment. Any shortcomings should be mitigated by the entity by requesting or performing additional validation activities.[3] The details and requirements associated with the expectations of system validation by the entity would be outlined in an entity specific System Validation procedure.

41) **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: No, it is not advisable to skip the test/validation environment. From a software perspective, system testing should occur prior to live utilization (production environment). 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 production environment. No, the system does not need to be revalidated once in the production environment, unless changes are made, at which time you would follow your normal System Validation procedure for change control and/or validation.

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

A: Some examples of systems for which the EIS Evaluation Checklist needs to be submitted can be found in the table below.

	Site (Clinic)	**Pharmacy**	**Laboratory**
Clinical Trial Management System (CTMS)	X		
Electronic Clinical Outcome Assessment (eCOA)	X		
Document Management System	X	X	X
Electronic Data Capture (EDC)	X		
Electronic Informed Consent (eIC)	X		
Electronic Patient-Reported Outcomes (ePRO)	X		
Electronic Signature	X	X	X
Learning Management System (LMS)	X	X	X
Quality Management System (QMS)	X	X	X

	Site (Clinic)	Pharmacy	Laboratory
Environmental Monitoring System	X	X	X
Interactive Voice / Web Response System (IxRS)	X		
Electronic Investigator Site File (eISF)	X	X	
Electronic Health/Medical Record (EHR) (EMR)	X		
Laboratory Information System (LIS)			X
Laboratory Information Management System (LIMS)			X
Electronic Trial Master File (eTMF)	X		
Sample Tracking System		X	X
Patient Recruitment	X		
Regulatory Information Management System (RIMS)	X		
Clinical Safety and Pharmacovigilance	X		
Source Code Management (Software Versioning System)	X	X	X
Electronic Lab Notebook (ELN)			X
File Share/Storage	X	X	X
Lab Instrument	X		X
Portal Technology	X	X	X
Biometric Participant ID	X		

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

43) Q: Will there be an EIS Evaluation Checklist specific to Laboratories as labs may provide data to numerous sites?

A: No, labs will utilize the same EIS Evaluation Checklist as sites and organizations. Labs are not required to capture all site numbers they provide data to but can include this information.

References

1. FDA 21 CFR Part 11 Electronic Records, Electronic Signatures, 1997
2. FDA Guidance for Industry: Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations Questions and Answers, 2023
3. EMA Guideline on computerized systems and electronic data in clinical trials, 2023
4. FDA Guidance for Industry, Electronic Source Data in Clinical Investigations, 2013
5. FDA Guidance for Industry, Use of Electronic Health Record Data in Clinical Investigations, 2018
6. ICH E6 (R2) Good Clinical Practice: Integrated Addendum to International Conference of Harmonization (ICH) E6 (R1)
7. FDA Guidance for Industry, Electronic Records: Electronic Signatures – Scope and Application, 2003
8. FDA Guidance for Industry, Computerized Systems Used in Clinical Trials, 2007