IT Services and DHTs for Clinical Trials – What Your Contracts Need to Know about FDA's Latest Part 11 Draft Guidance

08-01-23 • alert • katherine leibowitz

FDA tackles information technology (IT) services and digital health technologies (DHTs) in its latest iteration of its current thinking on 21 CFR Part 11 (Part 11). With the revised draft guidance, Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations (March 2023(Draft Guidance), FDA updates its Part 11 recommendations to reflect the modernization and proliferation of IT used to conduct and support clinical trials. The Draft Guidance signals FDA's increased attention to electronic technologies and records that are subject to 21 CFR Part 11 (Part 11) and the accompanying systems and data security and integrity problems that they may bring to clinical trials.

The Draft Guidance impacts IT service providers, contract research organizations (CROs), sponsors, research institutions, investigators and institutional review boards (IRBs).

This post examines select issues that impact:

- Contracts for IT services that support clinical trials.
- The sponsor-CRO contract or master services agreement (CRO MSA)
- The use of DHTs in clinical trials, which we preciously wrote here and here.

We include numerous Takeaways for contracting parties.

Background: How the Draft Guidance Fits into Part 11

Boldly striding into the Part 11 space that is occupied by a variety of interrelated (sometimes confusingly) draft and final guidances, this Draft Guidance: (a) replaces the draft guidance entitled Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers (June 2017); (b) expands upon the guidance entitled Part 11, Electronic Records; Electronic Signatures – Scope and Application (August 2003); (c) when finalized, will supersede the guidance entitled Computerized Systems Used in Clinical Investigations (May 2007); and (d) lists eight Part 11-related guidance documents in the appendix.

As used in the Draft Guidance and this post, the term "Service Level Agreements (SLAs)" means the documents negotiated between IT service providers and their customers (as opposed to the service level agreements typically attached to a SaaS agreement, where the SLA details percentage uptime, remedies for failure to meet that uptime and other functional specifications).

The Draft Guidance repeatedly refers to, but does not define, "other regulated entities." We note that FDA identified

CROs and IRBs as examples of other regulated entities in the 2017 draft guidance that this Draft Guidance replaces.

Structure

The Draft Guidance uses a Q&A format to address:

1. Electronic Records (Questions 1-6)
2. Electronic Systems Owned or Controlled by Sponsors or Other Regulated Entities (Questions 7-16)
3. Information Technology Service Providers and Services (Questions 17-19)
4. Digital Health Technologies (DHTs) (Questions 20-23), and
5. Electronic Signatures (Questions 24-28)

This post follows the Q&A format of the Draft Guidance. We focus on select issues that impact IT contracts and the use of DHTs in the clinical trials enterprise. For each Question in Sections IIIB-E, we begin with the Draft Guidance's recommendations and add our commentary as "Takeaways."

Draft Guidance Questions and Answers, and Takeaways

Section III: Questions and Answers

The Draft Guidance highlights the importance of compliance with good clinical practices (GCPs) and ties in Part 11.

Section III.A: Electronic Records (Q1 – Q6)

For electronic records that are subject to Part 11, this section looks at real-world data sources (Q1), foreign studies (Q2), certification Q3 and Q4), record retention (Q5) and electronic communication methods (Q6).

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

Alphabet Soup of Electronic Systems

If you run fully or partially decentralized clinical trials (DCTs), the plethora of potential electronic systems supporting the study will come as no surprise. The Draft Guidance gives a veritable alphabet soup of examples of electronic systems used to produce electronic records required in clinical investigations, including eCRF, EDC, eTMF, eCDMS, eCTMS, electronic quality management systems (no acronym!), IRT, IVRS, IWRS, electronic IRB management systems, eIC and web portals that display ePRO, eCOA and DHT-collected data (you'll be quizzed at the end).

Risk-Based Validation and Enforcement Discretion (Q7)

FDA reiterates (from its 2003 Part 11 Guidance) that "FDA intends to exercise enforcement discretion regarding specific Part 11 requirements for validation of computerized systems."

The Draft Guidance lays out considerations for a risk-based approach to validation of electronic systems. FDA distinguishes between commercial off the shelf software (COTS) and customized software, and observes that validation

for the former is not generally required if the COTS is used as intended by the manufacturer.

> Takeaways: Sponsors do not need to validate commercial off the shelf software (COTS) if the COTS is used as intended by the manufacturer. Depending on the IT services, sponsors should consider whether to include corresponding representations and warranties in the SLA.

Sponsor Documentation and Inspections (Q8)

FDA recommends that for each study protocol, the sponsor should diagram the data flow from initial creation to final storage. The sponsor should describe (a) the electronic systems used to collect data; and (b) the electronic systems used to create, modify, maintain, archive, retrieve or transmit relevant electronic records.

The Draft Guidance sets forth 11 bullet points for which sponsors should determine whether documentation or SOPs are appropriate. Documentation related to the bulleted list should be retained as part of the clinical investigation records and available for inspection by FDA.

FDA identifies seven areas that FDA will generally focus on during a sponsor inspection. Of special note for IT vendors, sponsors and CROs, this list includes "contracts with vendors or other delegated entities that detail their functions and responsibilities."

> Takeaways: For each study protocol, sponsors should perform an electronic systems mapping and a data mapping exercise. When negotiating an SLA, the parties should take into account FDA's bulleted list and the seven areas for sponsor inspection, keeping in in mind that FDA may review vendor contracts like the SLA.

Investigator Site Documentation and Inspections (Q9)

Sponsors should provide information (e.g. policies and procedures) to sites about the Part 11-regulated electronic systems they or their vendors use. Investigators should retain this information and have it available for an FDA inspection, as the information may bear on the sponsor's compliance.

Sites whose systems fall under Part 11 should follow the answers to Question 8. Not surprisingly, FDA may inspect the site's SOPs and documentation regarding the use of electronic systems.

> Takeaways: Sponsors need to provide sites with information about the sponsors' relevant electronic systems and be prepared for the site to share that information with FDA as part of an FDA audit of sponsor compliance. Sites should also be prepared to follow Question 8 if their own systems fall under Part 11.

Audits of IT providers by Sponsors and Other Regulated Entities (Q10)

FDA generally will not review audits conducted by sponsors or other regulated entities of their IT providers.

> Takeaways: SLA parties generally do not need to worry that sponsor audits of their IT providers will be shared with FDA. It is unclear what the exceptions might be.

Security Safeguards (Q11)

Turning to the security of these electronic systems, FDA recommends security fundamentals like using logical and physical access controls, cumulative records of authorized access, and standard security safeguards. Examples include:

- Prevention of unauthorized access to the system
- Logging off when leaving workstation
- Automatic logoff for idle workstations
- Limiting the number of login attempts
- Recording unauthorized login attempts
- Maintaining and continually updating safeguards like firewalls, antivirus, anti-malware and anti-spyware software
- Encryption

Takeaway: Follow security basics. In today's world, how can you afford not to?

We have written about cybersecurity here, here and here. Katherine Leibowitz is a frequent speaker on cybersecurity issues in technology contracting and the clinical trials enterprise at industry conferences and webinars.

Security Breach – Validation and (Yikes) Reporting (Q11 continued)

Tucked quietly into the end of Q11, FDA recommends two things:

1. For "security breaches to devices or systems, sponsors and other regulated entities should make reasonable efforts to ensure the continued validity of the source data." The footnote observes that this security functionality should be part of the software validation process.
2. "Security breaches that could impact the safety or privacy of clinical investigation participants and data should be reported to the IRB and FDA as soon as possible."

Takeaways: The security breach terms of #2 are vague and leave a lot to the imagination. This is a common conundrum in IT contracting. What is a security breach? What is the threshold for when an event "could impact" safety or privacy? Which contracting party makes this determination? What triggers a report to the sponsor? How quickly? Who reports to the IRB and FDA? What about notifying study subjects? The answers will vary depending on the party, the IT and data at issue, and the relative negotiating positions of each party. Keeping FDA in mind, the negotiated compromises need to baked into the SLAs and clinical trial agreements.

Audit Trails (Q12)

FDA reiterates its intent to exercise enforcement discretion regarding audit trails under Part 11 and reminds everyone that compliance with the predicate rules is still a "must."

Reflecting FDA's focus on the impact of technology impact on trial data integrity, FDA observes, "Even where there are no predicate rule requirements related to documentation, it is nonetheless important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the electronic records."

Takeaway: Regulations aside, best practices include having audit trails or other physical, logical, or procedural security measures in place to ensure data integrity. This is another no-brainer in today's interconnected world.

Section III.C: Information Technology Service Providers and Services

Subsection C addresses IT service providers and IT services (e.g. data hosting, cloud computing software, platform and infrastructure services). FDA reminds everyone that sponsors and other regulated entities are responsible for ensuring that electronic records comply with Part 11.

The introduction to Subsection C contains a bulleted list of due diligence items for sponsors and other regulated entities to consider when assessing an IT service provider's ability to ensure the authenticity, integrity and confidentiality of study records and data.

> Takeaways: Due diligence of IT vendors is critical. FDA's bulleted list serves sponsors and IT vendors alike. Sponsors and other regulated entities should remember to check the list when performing due diligence of their IT vendors, and to build appropriate representations and warranties into the SLA. IT vendors should be prepared to respond by having appropriate policies and documentation on hand, and by examining the nature and extent of what they are warranting and confirming that the SLA does not overpromise.

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

Yes. We included the full question here because we find it astonishing that sponsors and other regulated entities would consider not having a written service level agreement (SLA) with their IT providers.

After performing the due diligence based on the bulleted list located in the introduction to Section III.C (discussed immediately above), FDA recommends that the sponsor or other regulated entity enter into a written SLA with the IT service provider. Among other things, the SLA should address data integrity and security safeguards, and should clearly set forth the scope of the services, the respective roles and responsibilities of each party to the contract and details regarding data access throughout the regulatory retention period.

FDA reminds stakeholders that the sponsor is responsible for duties and functions related to the study that are not specifically and lawfully transferred to and assumed by IT service provider (e.g. via a transfer of regulatory obligations (TORO) to a CRO under 21 CFR 312.52; this applies to drug studies; there is no parallel under 21 CFR 812 for device studies).

> Takeaways: Don't use IT services for your clinical trial without a written contract with the IT vendor. Don't enter into that written contract unless you have performed due diligence on the IT vendor with FDA's list in mind (and the vendor passed with flying colors).

How to Demonstrate that the IT Services are Performed in Accordance with FDA Regulations (Q18)

Even more firmly inserting itself in the IT relationships, FDA explains that "Sponsors and other regulated entities who outsource IT services should make the following information available for FDA upon request:

- SLAs and ay other agreements that define the sponsor's expectations of the IT service provider
- All quality or risk management procedures related to the IT service
- Documentation of ongoing oversight of IT services

Takeaways:

- FDA may request to see the SLAs, other vendor contracts, procedures and oversight documentation (but see Q10 above about generally not reviewing the sponsor's audit). Sponsors and other regulated entities should maintain these documents and should be prepared to share them with FDA.
- Sponsors frequently outsource IT service providers and to CROs. In turn, CROs often provide IT services for sponsors through a combination of proprietary (e.g. EDC system) and outsourced software and/or services (e.g. cloud host, IWRS). The Draft Guidance applies to IT services provided directly by "pure" IT vendors (e.g. EDC vendor) and through third parties like CROs.
- For outsourced IT services, sponsors and other regulated entities need to understand the chain of upstream and downstream agreements that they and their vendors have in place for the clinical trial IT services. These agreements need to contain appropriate flow-down clauses, warranties, and risk mitigation provisions that coordinate effectively throughout the chain? How should the CRO or sponsor handle a liability cap provided by the IT service provider who is several contracts downstream?
- It is common for stakeholders in the clinical research enterprise to enter into a letter of intent (LOI) to enable them to get started on the work. This is particularly true of the sponsor-CRO relationship. LOIs can make it difficult for the customer to (a) perform proper due diligence; and (b) negotiate and execute a balanced contract. Busyness sets in so that by the time the parties get around to negotiating the full contract, the customer is heavily invested in the work that it no longer has negotiating leverage or the parties are getting along so well that they do not want to devote the time and effort to complete a full contract. Nevertheless, sponsors and other regulated entities should take care to draft sufficiently robust contracts concerning IT services both to comply with best practices and for when FDA comes knocking.

Would FDA Inspect IT Providers in a Clinical Investigation? (Q19)

FDA may inspect IT service providers who are subject to a TORO.

"FDA can also request to conduct focused investigations of IT service providers for examination of trial records" even if there is no TORO, such as if FDA has a specific concern about data integrity. The SLA should provide the sponsor with access to all study-related records maintained by IT service providers, as FDA can review those records during a sponsor inspection.

Takeaways: The SLA should give the sponsor access to all study-related records. Further, IT providers (whether or not subject to a TORO) might be inspected.

Section III.D: Digital Health Technologies

Section III.D discusses special Part 11 considerations for DHTs used to collect data in clinical investigations. In addition, the principles of Sections III.A – C regarding electronic systems apply equally to DHTs. The Draft Guidance builds on FDA's draft guidance from December 2021 on the use of DHTs in clinical trials, which we previously wrote about here and here.

For DHTs specifically, the Draft Guidance tackles:

data originators (Q20):

- The data originator may be a person, computer system, DHT or an EHR, depending on various factors.
- The Draft Guidance provides examples of data originators when DHTs are used.
- FDA recommends that sponsors keep a list of authorized data originators for FDA inspection.

data attribution (Q21):

- Sponsors should ensure the data obtained via the DHT is correctly attributed to the data originator. Options include access controls, study subject education and data monitoring.
- DHTs should prevent unauthorized changes to the data stored on the DHT before it is transmitted to and recorded in a durable electronic data repository.
- Access controls (e.g. biometrics or MFA) should be in place for mobile applications to ensure the data comes from the person who is authorized to enter the data.
- For DHTs where access controls may be difficult to implement (e.g. wearable sensors), sponsors should consider how they will address user authentication and data attribution, particularly if the DHT data will be used to support an endpoint. The investigator should discuss the appropriate use of these DHTs with the subjects, who should receive proper training. This discussion should be documented in the study records. FDA notes that periodic monitoring of DHT data during the study can help identify situations where data is not coming from the intended user.

Initial transfer of data for DHT to durable electronic data repository (Q22):

- Both the data captured from the DHT and the relevant metadata should be transmitted per the sponsor's pre-specified plan to the durable electronic data repository, which can be owned by the sponsor or vendor like an IT service provider.
- Transmission should occur contemporaneously or as soon as possible after data generation.
- The audit trail should include the date and time the data are transferred.
- By using a validated process, source data captured by a DHT can be moved from one durable electronic data repository to another.

Location of source data collected by DHT and FDA inspection of DHT-collected data (Q23):

- Electronic source data are located in the first durable electronic data repository to which the data are transferred (e.g. EDC system, study site database, cloud-based platform).
- FDA does not intend to inspect individual DHTs for source data if the data and metadata captured by the DHT are securely transferred to and retained by the durable electronic data repository per the sponsor's pre-specified plan.
- The Draft Guidance discusses FDA verification of sponsor data in submissions and applications and discusses Part 11 requirements, enforcement discretion and recommendations regarding having records in human readable form.

Takeaways: This Section III.D. expands upon FDA's December 2021 DHT draft guidance by introducing more granular recommendations regarding the use of DHTs in clinical trials. While DHTs may have previously fallen under the radar, as studies become increasingly decentralized and technology-centric, the Draft Guidance illustrates increased FDA attention to DHTs. Stakeholders in clinical trials that employ DHTs should review this

entire Draft Guidance with particular attention to Section III.D (and should do so in conjunction with the December 2021 DHT draft guidance).

Section III.E: Electronic Signatures

Electronic signatures and their associated electronic records that comply with Part 11 generally will be viewed as the equivalent of handwritten signatures.

The Draft Guidance tackles:

Creation of valid electronic signatures (Q24)

- The Draft Guidance provides examples of methods to create valid electronic signatures, such as biometrics, digital signatures and username and password combinations.
- For COTS electronic signature services, sponsors, investigators and other regulated entities should ensure that these services conform to Part 11 requirements based on either information from the COTS vendors or their own validation "when warranted."

Signatures drawn with a finger or electronic stylus (Q25)

- FDA views signatures drawn with a finger or a stylus as handwritten signatures, not electronic signatures, as long as they are properly linked to their electronic record and are properly placed on the electronic document.

Verifying the identity of the individual who signs electronically (Q26)

- How do you know the person who signs electronically is who they say they are? The Draft Guidance gives examples of methods to verify identity, including government-issued identification, security questions or strong digital login credentials with multi-factor authentication or video observation.

Biometric electronic signatures (Q27)

- Biometric examples include fingerprints, hand geometry, iris patterns, retinal patterns or voice prints. The biometric should be uniquely identified with the individual and should not change over time.

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

- No. FDA recommends that sponsors work with the COTS vendor to ensure compliance with Part 11.

Takeaways: The Draft Guidance updates FDA's electronic signatures recommendations to account for new technologies. Stakeholders should review these recommendations when building out their IT support. Authentication of a person's identity (is the electronic signatory who they say they are?) is always a challenge in the electronic world and has become even more so with the explosion of generative artificial intelligence software

that can, for example, create quite convincing voice clones. But that's a story for another day...

Conclusion

The recently revised Part 11 Draft Guidance reflects a deep dive by FDA into IT services supporting clinical trials, including granular attention to DHTs. The document includes best practices for contracting, outsourcing and documentation, and serves as a warning to stakeholders of FDA's increased attention to data integrity and security in the increasingly-technologized clinical trials enterprise. It's also a reminder that contracts in regulated industries need appropriate regulatory seasoning. With the modernization and decentralization of clinical trials mandated by FDORA, we expect FDA to continue focusing on the impact of IT services on clinical investigation study data and participant integrity, security, privacy and safety. We will continue to monitor developments and encourage you to check our Insights for updates.

Access the Draft Guidance.

Access our Alert on DHTs, FDORA and cybersecurity here, here and here.

If you have any questions or would like more information about these developing issues, please contact the following:

KATHERINE LEIBOWITZ
1-610-896-5788
Katherine.Leibowitz@LeibowitzLawTeam.com