APRIL 2017

Clinical Researcher™

The Authority in Ethical, Responsible Clinical Research

Ensure Your Site's Compliance with Part 11: *See page 2*

Technology for Trials:

Are You Falling Behind, Keeping Up, or Getting Ahead?

INCLUDING the Latest in Workforce Innovation

Association of Clinical Research Professionals (ACRP)
www.acrpnet.org

Ensuring Compliance with Part 11: *A Site's Perspective*

PEER REVIEWED | Cristina Ferrazzano Yaussy, MPH, CCRP | James Wetzel

[DOI: 10.14524/CR-17-0005]

Today's clinical research sites are under tremendous pressure to produce more in an increasingly complex environment; however, the sophistication of sites' information technology (IT) systems often remains antiquated, lagging those used by the healthcare organizations with which they work. Office bookshelves bursting with paper binders function better as cubicle walls than workable repositories. Manual processes limit credentialed staff from realizing potential, and siloed systems and departments prevent productive collaboration.

In this environment, as more sites are looking to implement technology to go paperless, improve standardization, and provide secure access to essential documents, site staff's experience with ensuring compliance with 21 CFR 11 (Part 11) of the *Code of Federal Regulations*—focusing on the U.S. Food and Drug Administration's (FDA's) standards for electronic records and electronic signatures—may be limited. Balancing the need to maximize efficiency and ensure compliance presents a challenge, but with the right resources, the challenge is an achievable one. Gaining a better understanding of the purpose, scope, and components of Part 11 will help sites achieve their compliance goals.

Understanding Part 11: Purpose & Scope

In light of the Paper Reduction Act of 1995, the FDA aimed to rid itself of inefficiencies in record keeping. Recognizing the value of computer systems, yet the need to balance the security, authenticity, and reliability of electronic records, the FDA set forth to define regulations that would allow for the use of electronic records in the agency's mission. Thus, Part 11 was released in 1997.

Part 11 plays a vital role in the larger purpose of the FDA. By ensuring the security, authenticity, and reliability of data collected during a trial—and the systems that manage and process those data—the agency aims to ensure the safety and protection of the public.

Much debate has ensued over the applicability of the regulation, largely due to a lack of understanding. Essentially, Part 11 applies to any organization engaged in FDA-regulated research that maintains records electronically. This includes any records in electronic form, whether created, modified, maintained, archived, retrieved, or transmitted to others.[1] The general rule is that if a record is sent to the FDA or is required by the FDA to be maintained, and is managed electronically (electronically signed, disseminated, stored, etc.), it falls under the regulation.

Understanding Part 11: Five Components

Developing a process for Part 11 compliance at a research site can be a good thing. More often than not, it becomes an opportunity to look at the site's internal processes, the state of its standard operating procedures (SOPs), the presence or lack of a quality management system, and its ability to entertain inspections and audits. Furthermore, addressing the expectations of Part 11 thoroughly better prepares a site for the technologies of tomorrow.

The development of a site's Part 11 compliance process can be broken down to five main components, as described in the following sections.

Define Policies and Procedures

The first step to building out a Part 11-compliant process is to have a solid foundation and appropriate guidance, policies, and SOPs.[1] SOPs demonstrate

LEARNING OBJECTIVE
After reading this article, participants should be able to understand and identify critical components related to 21 CFR 11 compliance and how to implement and maintain an effective compliance process.

DISCLOSURES
Cristina Ferrazzano Yaussy, MPH, CCRP; James Wetzel: *Nothing to disclose*

a commitment to quality and reinforce the operational practices that a site upholds. They also serve as a resource for training staff, so that research teams understand their roles in following procedures and maintaining compliance with Part 11.

As a best practice, sites should maintain a portfolio of SOPs (see Table 1). This will help facilitate a consistent approach to implementing technology and safeguard against any potential oversights of the critical components of Part 11.

When moving to a document management system, sites should determine in advance which record(s) will be maintained in electronic format and document this decision in an SOP. Should a sponsor, monitor, or auditor inquire about such procedures, a well-developed SOP will ease their concerns.

System Functionality Review

When selecting a system to manage electronic documents and signatures, sites should conduct a thorough review, as specific functionality is required under Part 11 (see Table 2). This review should not be limited to the minimum required functionality, such as audit trails and authority checks; sites should use this as an opportunity to evaluate how the system can impact other site operational areas.

Consider, for example, the general auditability and configurability of the system. Does the system provide advanced keyword search functionality, so that documents are easily retrieved by staff or reviewers who are unfamiliar with naming conventions or file structures? Inadequate accessibility or retrievability can impede the auditing process, which could lead to findings. Furthermore, files that are organized, secure, and readily accessible will improve overall staff efficiency.

Can the system be configured or modified by administrators without requiring time-consuming revalidation? For example, you hire a new regulatory specialist and need to modify the system to allow access to regulatory documents, but not financial documents. A well-designed system can accommodate these types of administrative changes without requiring revalidation (explored further below). Furthermore, it will help a site to accommodate growth without needing to rely on the vendor for every modification.

Site leaders will want to decide if they desire a system with advanced access functions that allow administrators to control whether certain users can upload and edit documents, but others only to view and sign those same documents (or not see them at all). Robust access controls and permissions can allow for a more controlled, yet more collaborative team.

While the software manufacturer can provide guidance in this review, it is the responsibility of the site to conduct and document a review of the system's functionality as it relates to Part 11. Use the system review as an opportunity to learn how the system can impact overall efficiency and usability.

Vendor Selection: Finding the Right Partner

Similar to an FDA inspection of a site, a site's evaluation of a vendor provides insight into the vendor's development and quality management processes. As vendors are entrusted with site data, site leaders should ensure they have adequate controls in place to prevent issues and handle exceptions.

Furthermore, auditing a vendor facilitates constructive dialogue between the site and vendor,

TABLE 1: EXAMPLES OF STANDARD OPERATING PROCEDURES (SOPS)

SOP	Description
SOP Development and Maintenance	Outlines the process by which all other SOPs are developed, approved, and maintained
Vendor Selection/ Audit	Outlines the procedures of performing vendor audits to ensure software providers are selected based on their capability to provide quality software and documentation for system validation
Records Management	Outlines how and by whom documents will be managed, including matters related to certified copies, retention, and accessibility
Software Implementation and Maintenance	Outlines initial validation, user acceptance testing (UAT), ongoing maintenance, and change control procedures
Electronic Signature Policy	Attests that users understand that their electronic signature holds them accountable; a letter of Non-Repudiation Agreement for digital signatures must be submitted to the FDA prior to change[3]
Training	Ensures users have adequate training and agree to terms of using the system

TABLE 2: CRITICAL COMPONENTS OF PART 11 FUNCTIONALITY

System Feature	Part 11 Compliant Application
Electronic Records Management	• System designed for electronic records management and functions as designed • Records are available for export and review throughout the retention period • Workflow follows sequential steps and prevents nonsequential actions
Audit Trail	• Automatic tracking of changes to electronic records • Date and time stamp for all actions and changes • Audit trail available for review and export throughout retention period
Security	• Access controls based on user role or permissions • Prevention of unauthorized access • Alerting of unauthorized access attempts • Secure access/password reset methods
Electronic Signatures	• Automatic tracking of name, date, time, and Statement of Testament associated with signature • Viewable and exportable manifestation of eSignature with Statements of Testament • Executing and linking the signature to the underlying record • Signatures cannot be attached to other record or removed

Balancing the need to maximize efficiency and ensure compliance presents a challenge, but with the right resources, the challenge is an achievable one. Gaining a better understanding of the purpose, scope, and components of Part 11 will help sites achieve their compliance goals.

which can lead to improvements in product quality. Poor development practices can lead to performance issues resulting in lost time (e.g., recovering information) and money (e.g., to purchase another system), damage to data integrity, and exposure to gaps in compliance with Part 11 or SOPs.

Sites should review the vendor's SOPs related to training practices, servers, records retention, disaster recovery, and software development/validation. This will provide insight into the vendor's development practices, as well as its understanding of the requirements of Part 11.

Evaluating the vendor's implementation and software release (or update) process is also important, as this will play a key role in ongoing maintenance and stability of the system. System updates are necessary for ongoing security and functionality improvements. However, if updates are released hastily or without adequate notice from the vendor, a site may be unprepared to perform adequate testing or training. Conversely, if updates are infrequent, desired improvements in functionality will not be met and known problems or "bugs" can perpetuate unreliable records.

If a site has an IT department, that department's staff should be involved in the process from the very beginning. Not only will they provide insight from a technology perspective, but they may also need to work closely with the vendor to ensure their procedures or requirements can be met. Sites without dedicated IT support should look for a vendor that provides additional assistance.

Sites should also closely review the level of support the vendor will provide for training and ongoing validation. Without adequate support, a site will need to plan for additional time and expertise in these areas. In the larger sense, a vendor that is knowledgeable and dedicated to Part 11 compliance can function more as a partner by ensuring a smooth transition and long-term success.

Validation

The process of performing and documenting systematic testing (validation) of the system is also a critical component of compliance with Part 11. In the same manner a car manufacturer may conduct a crash test to ensure the airbags work, sites must test their systems to ensure they function reliably. As we increasingly trust systems to perform tasks, we must ensure they perform them correctly.

While validation can be a complex chore, industry trends point to an increased focus in this area. In fact, the November 2016 revisions to the International Council for Harmonization's (ICH) Guideline for Good Clinical Practice E6 (R2) specifically require that computer systems be validated.[2] This requirement was developed to offset sites' increased reliance on allowing sponsors, contract research organizations (CROs), and vendors to conduct validation on their behalf.

While a qualified and knowledgeable partner can help, ultimately, validation is the responsibility of the site. It is not a one-time occurrence or something that is "covered" by a vendor or sponsor—it is an ongoing process that sites need to own.

To conduct system validation, sites should develop a user acceptance testing (UAT) protocol to systematically evaluate performance. The UAT protocol should outline what the system should do (requirements), how it should do it (specifications), and how testing should be performed to ensure it functions correctly. The results should be documented along with any unusual observations. UAT should be repeated (revalidation) when requirements and specifications relating to Part 11 are modified, which typically happens with a major system update.

Similarly, validation of the infrastructure (hardware) hosting the system must also be conducted. The process may change whether the system is hosted by the site or by the vendor. However, the responsibility of ensuring the integrity of the hardware ultimately falls on the site. When using a vendor, a site is entrusting the protection of its information in the vendor's hands, therefore the site should ensure the hardware being used to host its data is properly validated.

Training

Training is an integral part of selecting and using electronic systems for research projects. The processes surrounding how and when training is conducted and documented is a responsibility of the site that can be made more efficient with assistance from vendors. Simply put, persons who develop, maintain, or use electronic records and electronic signature systems (staff for vendors and the site end-users) must have procedures in place so that they have the proper education, training, and experience to perform their respective tasks.

Training is everyone's responsibility, and is necessary to ensure that the system is used properly and that users can identify when it may not be working correctly. Inadequate training may lead to compliance issues, as data integrity and access controls can be compromised through misuse of a system. Training should be conducted upon implementation and updated along with any major changes to the system that follow.

As an added level of support to sites, and to help promote compliance with Part 11, a system can offer automated training to all individuals upon entry and request that they attest to understanding their responsibilities for documentation purposes. Training should be consistent with the function/responsibility of the end-user, and should be documented along with the eSignature attestation. This attestation is to document that users understand that when they use a system and apply their eSignature, it is equivalent to their hand-written signature, which is a fundamental aspect of Part 11.

Where Do You Start?

So, how do research site staff begin to tackle Part 11, especially if they are questioning if it will even be worth the effort? Besides pleasing an auditor, what benefits will a site realize from compliance with this regulation? Moreover, where does one begin, given the volumes of information about Part 11 that a simple Google search provides?

Some site leaders may even question if, in the event of an FDA inspection, the agency is really going to look at Part 11 compliance—especially given that there have been few if any inspection findings to-date of research sites nonconformance in this area. The concerns are valid, but consider the following: Recent FDA guidance on investigator responsibilities highlights an increased focus on the research site. In fact, the aforementioned ICH E6 (R2) references many of the same concepts outlined in 21 CFR Part 11 as they relate to the investigator's responsibilities for data handling, record keeping, and audit trails. Further, the increased use of technology systems to manage essential documents means these systems are more likely to be looked at closer by auditors and inspectors.

The best place for site leaders and staff to start is to evaluate what they don't know about Part 11. Know when a function falls under compliance and when validation should occur. At a minimum, know that it is not a "task" to be relegated to the IT team, nor is it a product feature to be bought or a box to be checked. While others can certainly help, maintaining compliance is an operational process whose responsibility is shared throughout the site.

Next, take inventory of what needs to be done. One critical question that needs to be asked early on is "What can we improve as a site before, during, and after this compliance effort?" Perhaps new SOPs need to authored? Responsibilities need to be better defined. Online shared drives need to be organized. Make a list.

Next, evaluate how current processes and procedures may be impacted. How might this affect staff onboarding? Does the site have specific training requirements? Does it have specific back-up or retention requirements that are different from what vendors provide?

Also evaluate the capabilities of everyone at the site to carry out these tasks. How will this affect new staff? Is it a large site with a dedicated training or validation team? Or a small site with stretched resources? Take stock of where help may be needed.

There is an abundance of resources at sites' disposal for assisting with complying with 21 CFR Part 11; whitepapers, websites, federal regulations, case studies, vendors, consultants, and even CROs and sponsors can be a resource for learning the steps involved. Do not be afraid to lean on vendors or reach out to CROs and sponsors, but most importantly, find a resource that has successfully navigated these compliance waters.

After the validation and compliance efforts have been completed, understand that it is a journey and not a destination. Documentation of ongoing efforts of compliance, making use of a quality system, documenting and doing what your SOPs say—these are all part of the process.

In summary, then, the following is a high-level view of key considerations for implementing a Part 11 compliance process:

- Perform a self-assessment and gap analysis
- Identify how to fill in the gaps
- Develop policies and procedures
- Find a solution and a knowledgeable partner to fill gaps
- Implement new processes
- Implement and validate the system
- Train your team
- Perform ongoing evaluation and quality assurance

Once site staff have undertaken the process and received feedback on their efforts (hopefully through something other than an FDA Form 483), they will be equipped to apply the process to new technologies that require compliance. Additionally, sponsors and CROs will recognize the site's new-found level of sophistication and be more likely to want to conduct studies at the site.

Conclusion

One of the greatest challenges facing clinical research sites is ensuring regulatory compliance, especially when using technology to manage documentation. While not easy, the journey to compliance can improve the research site in more ways than just in terms of its validation and audit preparedness; it can bring better SOPs, happier staff, and more efficient research conduct.

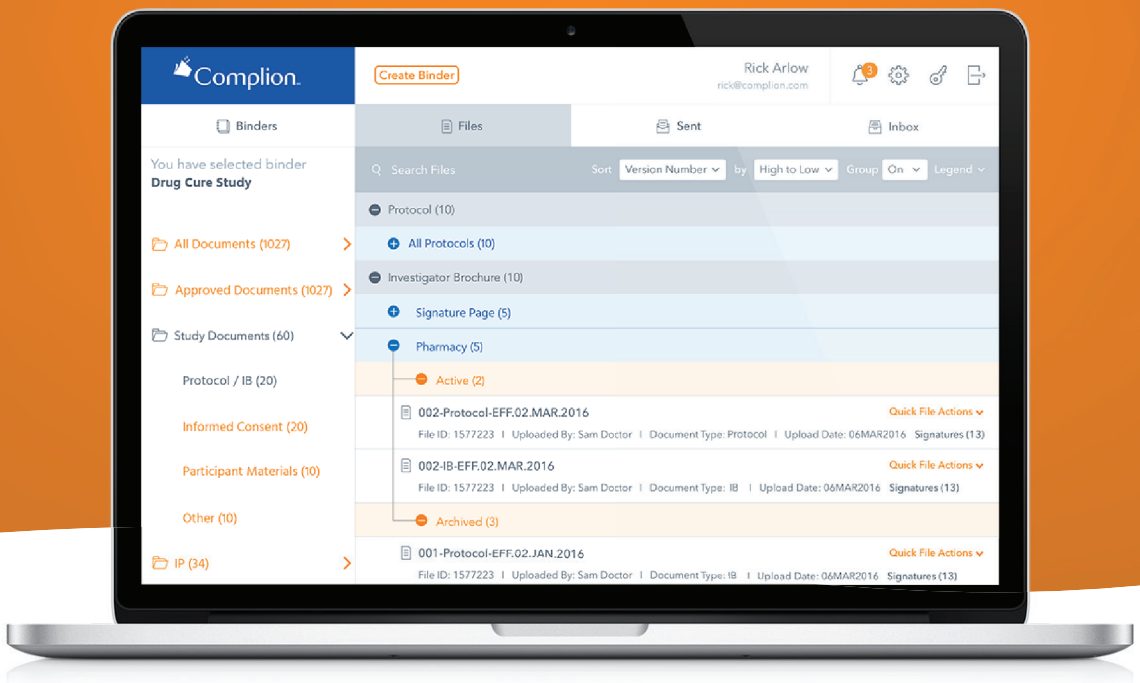
References

1. U.S. Food and Drug Administration. Part 11 of Title 21 of the *Code of Federal Regulations* on Electronic Records; Electronic Signatures—Scope and Application. https://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm
2. ICH Harmonised Guideline. 2015. Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(R2). https://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E6/E6_R2__Addendum_Step2.pdf
3. U.S. Food and Drug Administration. Electronic Submissions Gateway—Appendix H: Letters of Non-Repudiation Agreement. https://www.fda.gov/ForIndustry/ElectronicSubmissionsGateway/ucm113964.htm

Cristina Ferrazzano Yaussy, MPH, CCRP, (cristina@complion.com) is vice president for professional services with Complion, Inc., in Cleveland, Ohio

James Wetzel (jwetzel@okheart.com) is a director at the Oklahoma Heart Hospital.

GO PAPERLESS. STAY COMPLIANT.



Are you tired of fighting with messy binders, cluttered inboxes or misplaced documents? Is the accumulation of regulatory and administrative tasks adding to your already heavy workload?

Complion helps clinical research sites save time and focus on your trials by reducing the hassle associated with managing regulatory and trial paperwork.

- Find the right document quickly with beautifully organized files, standard templates, and powerful keyword searching
- Save time managing PI delegation records, Safety Reports, CVs, Licenses and training with Part 11 compliant signatures and workflows built for you
- Eliminate printing and redundancy by connecting to your existing email, CTMS, IRB or EMR systems without costly development or custom coding
- Collaborate across multiple sites and institutions instantly
- Partner with our team of certified clinical professionals to learn best practices, train your team, and maintain 21 CFR Part 11 compliance

Complion℠

ACRP ALLIANCE PARTNER

Complion is a proud ACRP Alliance Partner

Join the leading sites, hospitals, academic medical centers and cancer centers around the country using Complion to streamline paperwork and improve compliance.

UR Medicine | Wilmot Cancer Institute — Medicine of the Highest Order

CRC Group

Mary Crowley Cancer Research — Hope Lives Here

optimed Research, LTD

ACR Advanced Clinical Research

Del Sol Research Management, LLC

Contact us today!

800-615-9077
www.complion.com
sales@complion.com