indium
Make Technology Work

21 CFR Part 11 Compliance Testing

White Paper

www.indiumsoftware.com

Food and Drug Administration's 21 CFR Part 11 regulation lays down guidelines for electronic signatures and other authenticate methods to improve safety, security, ensure integrity and establish the veracity of the electronic documents across Lifesciences industries that follow current Good Manufacturing Practices.

Documentation Guidelines for Electronic Documents

Food and Drug Administration,Department of Health, US, mandates that industries such as pharmaceutical, biotech and medical devices follow Current Good Manufacturing Practices (cGMP) to manufacture products that conform to specific requirements for identity, strength, quality, and purity. The entire production process needs to be recorded, tracked, managed, stored and accessed with compliance document that also details change history including Standard Operating Procedures (SOPs), Master Production Batch Record (MPBR), Production Batch Record (PBR), Equipment log books and so on. 21 CFR Part 11 for software validation and other related good software engineering practices are mandated to avoid such defects and resultant recalls. Validation requirements apply to

- Software used as components in medical devices
- Software that in is itself is a medical device
- Software used in production of the device or in implementation of the device manufacturer's quality system

The Need

Traditionally all documentation was in paper format. FDA started accepting electronic document as computerizsation and automation facilitated better process control, speed and efficiency in life sciences organizations. Between 1992 and 1998, Food and Drug Administration analyzed 3140 medical device recalls, of which 242 of them (7.7%) were due to software failures. Of this, 79% were due to software defects introduced when changes were made to the software after its initial production and distribution. FDA introduced 21 CFR Part 11 as a requirement of the Quality System regulation on October 7, 1996 and took effect on June 1, 1997.

21 CFR Part 11 on Electronic Records and Signatures

Food and Drug Administration's CFR - Code of Federal Regulations, Title 21, Part 11 sets down guidelines regarding electronic records and electronic signatures. The is set of regulations that aims to ensure the trustworthiness and reliability of electronic records Requirements of Part 11 are :

- Use of validated existing and new computerized systems
- Secure retention of electronic records and instant retrieval
- User-independent computer generated time-stamped audit trails
- System and data security, data integrity and confidentiality through limited authorized access to systems and records
- Use of secure electronic signatures for closed and open systems
- Use of digital signatures for open systems
- Use of operational checks
- Use of device checks
- Part 11 applies in one of the following situations:
- When electronic records are used instead of paper
- When persons make printouts but still rely on the electronic records in the computerized system to perform regulated activities
- Records submitted to the FDA, under predicate rules (even if such records are not specifically identified in agency regulations) in electronic format

- Electronic signatures intended to be the equivalent of handwritten signatures, initials and other general signings required by predicate rules
- This can help the Life Sciences industry manage records and other content electronically, thereby reducing risk of human errors, operational costs and time-to-market for pharmaceutical products

The Definitions

FDA clearly defines electronic signature and the related terms thus:

Electronic Record: Anything that contains text, graphics, data, audio, or pictorial information that is created, modified, maintained, archived, retrieved or distributed by a computer in digital form.

Electronic Signature: A compilation of any symbol(s) executed to be the legally binding equivalent of an individual's handwritten signature.

Handwritten Signature: The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form.

Digital Signature: An electronic signature based upon cryptographic methods of originator authent cation, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Closed system: Only persons responsible for the electronic records on the system are allowed access.

Open system: Where there is no access control for the electronic records.

Impact

Part 11 has an impact on the entire value chain, especially on Pharmacovigilance, Clinical Data Management and Manufacturing Execution Systems; and ERP, CRM or Training Management systems to a lesser extent. It has a significant impact on instrumentation, work processes and on the people in operations such as quality control laboratories and manufacturing operations.

21 CFR Part 11 brings significant benefits to Pharmaceutical companies by legalizing the electronic record keeping in GMP, GLP environment. This ensures:

- Acceptability of electronic submissions in areas of new drug applications and updates
- Permitting the introduction of new technology
- Preventing fraudulent changes being made to electronic records.
- Significant cost reduction through standardization
- Simplified exchange between industry players
- Increased use of electronic transactions and automation
- Ability to leverage e-business technologies
- Improved public perceptions and enhanced industry credibility
- Non-compliance can trigger enforcement action, and clearly, there is a great need along the value chain to apply the regulations.

The Benefit of Compliance Testing

Through Part 11 compliance, organizations can benefit from less enforcement, thus reducing the cost by up to 10-15 per cent. This helps organizations focus on value addition rather than preparing for an

inspection, further contributing to the financial health of the company as well as reducing effort.

Compliance Assessment

For successful compliance to Part 11 regulations, assessment becomes critical under the following conditions:

- Requirements are very clearly defined
- Gap Analysis will be repeated frequently
- Individuals don't have high degree of subject knowledge
- Narrow scope
- Goal is assessment only

Approach & Implementation

21 CFR Part 11 Key items

The following are mandated by the regulation:

- System validation
- Electronic Record Inspection / protection
- Security
- Audit Trail
- Operational checks
- Authority checks
- Device checks
- Personnel Qualifications
- Accountability and responsibility of actions
- System documentation controls
- Electronic signing requirements
- Controls for E Sign
- Linking E Sign to E Records
- Uniqueness of E Signature
- Verification of Individual Identities
- Certification to FDA
- E Sign components and controls
- Biometric E Sign
- Loss management

An organization falling under the ambit of the regulation cannot purchase a '21 CFR Part 11-compliant' system and instead need human intervention to make it compliant. Additionally, it needs appropriate software configuration, tight security norms and policies, procedures and appropriate training to make it fully compliant. Constant monitoring of changing laws and regulations are also important for the company to keep pace and make appropriate changes as and when required.

Controls

Compliance is achieved through three levels of controls:

1. Administrative
2. Procedural
3. Technical

For successful compliance, interaction between the vendor/ supplier and user/ customer is very important. Also, some of the rules have implications at different levels and therefore, any slackening can have a cross level impact.

ADMINISTRATIVE	PROCEDURAL	TECHNICAL
Policies	SOPs/written instructions for using system -	Functional aspect ensuring integrity and reliability of E Records and E Sign
E Sign usage -	Authorized users	
Verification of individual identities	backup/recovery/archive/ restore procedure software upgrade change control User ID/Password administration	

Implementation

Compliance Assessment begins with the evaluation of the current process of generating signatures, developing new procedures for limited authorized access to systems and data, developing a procedure on how to define Part 11 controls and defining Part 11 requirements for each system. A gap analysis will help determine missing functionality and procedures for systems. This can help in developing an implementation plan to bring identified systems into Part 11 compliance with ready to use SOPs and templates. Also identify areas where there is room for interpretations to ensure that it is implemented correctly.

- Whether the information is complete
- Whether all records can be tracked/ connected to source
- Date/time of information entered/ modified is recorded
- Whether the records are secured
- That the original information is not altered by any means
- That it is used by only authorized people
- That there is clear documentation
- That the users are properly trained and aware of the processes and their importance
- Whether the system is tested before usage
- Whether the information can be easily viewed in Electronic form and human readable form

For the implementation to be successful, the team needs to be provided with the right guidance to ensure that the organization remains compliant at all times.

Achieving Successful Compliance

Having evaluated the existing systems, define the objective of the implementation, understand the policies, SOPs, plan, audits, and so on in place, identify gaps and define an action plan.

Define Action Plan

- Compare current practices against the defined criteria
- Identify the existing compliance vulnerabilities in the systems reviewed
- Prioritize the compliance issues that these gaps present to the business
- Recommend how to solve the compliance issues identified
- Based on this, develop a framework that includes:

  Core Requirement Compliance - This ensures that the software is compliant with key requirements of the regulation, and any change to any record is captured in the audit trail. These entries are time stamped with additional information including operator name and why the record was changed.

  Authorization - System provides adequate security to prevent unauthorized modification by ensuring role-based access and preventing users from directly updating the database. The software employs electronic signatures for any transaction into the system.

Software Development Lifecycle

In case of the organization initiating the development of the software, CFR Part 11 requires clearly defined and approved system requirements before any design or coding effort starts. All system functions must be identified at this stage. Test plans, test procedures and test cases should be developed as early in the development lifecycle as possible, and include multi-level testing methodology such as unit test, functional test, integration test and system test. In addition, stress testing and disaster recovery testing must be performed to ensure that system performance requirements are met. Closed-loop change control ensures that proper change control documentation, approval and testing procedures are followed for any changes including, correcting software defects or adding new capabilities for a new version of the software or making changes to software configuration. Change control procedures must be written and well understood through training, to ensure compliance. Unauthorized changes to a validated system, even during the implementation process, can have a detrimental effect on the system integrity.

Infrastructure

In addition to the computer software system, the FDA regulation also provides guidelines or other related aspects of electronic records related to cGMP:

Facility: The vendor facilities or the software development lab should have adequate security controls to prevent unauthorized access to software, computer rooms and backup media storage rooms.

Organization: The software developers, designers and QA engineers should have adequate trained in the technical skills needed to do their jobs. The company also must have training policies to ensure right skilling the team on a continuous basis.

Validation for intended use: The requirement specifications detailing the intended use of the system and the system documentation are compared to identify any gaps. The system is also tested against the specifications to identify any additional gaps. The closed-loop change control method is used to close the gaps and the system is retested before final validation.

Indium's Approach for 21 CFR part 11 Compliance Testing and CSV

Indium Software has a Regulatory Compliance team of verification & validation specialists testers with years of experience in compliance testing for 21 CFR Part 11 and Computer System Validation. Its proven experience in working with leading life sciences firms assures 99.9% success in computer system validation. Jump start kits (Template, Guidelines, Checklists, reports) to address immediate requirements and a framework-based approach helps in implementing validation strategy, templates, checklists and operating procedures and developing essential validation deliverables. Some of the factors contributing to the success of compliance testing solutions for FDA CFR Part 11 include:

- Integrating quality processes and compliance tasks
- Solution mapping to various compliance parameters
- Delivering computer system validation audit report and metrics dashboard
- Providing extensive documentation and process improvement reports templates
- Providing and training Information Technology users on compliance regulations

INDIA

Chennai | Bengaluru | Mumbai
Toll-free: 1800-123-1191

USA

Cupertino | Princeton
Toll-free: +1 888 207 5969

UK

London

SINGAPORE

+65 9630 7959

Sales Inquiries
sales@indiumsoftware.com

General Inquiries
info@indiumsoftware.com