ejpmr, 2024, 11(6), 503-509

SJIF Impact Factor 7.065

EUROPEAN JOURNAL OF PHARMACEUTICAL AND MEDICAL RESEARCH

www.ejpmr.com

Review Article

ISSN 2394-3211

EJPMR

DIGITAL COMPLIANCE: NAVIGATING THE FUTURE WITH 21 CFR PART 11"

Mrunal S. Kikale[1*], Nilam D. Chingale[2], Sushil D. Walunj[3], Omkar A. Devade[4] and Vivek Kumar Redasani[5]

[1,2,3]Student of YSPM's YTC, Satara, Maharashtra, 415011.
[4]Department of Pharmacology, YSPM's YTC, Satara, Maharashtra, 415011.
[5]Director of YSPM's YTC, Satara, Maharashtra, 415011.

***Corresponding Author: Mrunal S. Kikale**

Student of YSPM's YTC, Satara, Maharashtra, 415011.

Article Received on 19/04/2024 **Article Revised on 09/05/2024** **Article Accepted on 29/05/2024**

ABSTRACT

21 CFR Part 11, titled "Electronic Records; Electronic Signatures," is a regulation established by the USFDA. Enacted in 1997, this regulation governs the use of electronic records and electronic signatures in industries subject to FDA regulations, primarily the pharmaceutical, biotechnology, and medical device sectors. The main purpose of 21 CFR Part 11 is to ensure the reliability, authenticity, and integrity of electronic records and signatures used in regulated industries. It outlines requirements for the use of electronic records and signatures to ensure that they are trustworthy and equivalent to traditional paper records and handwritten signatures. Key provisions of 21 CFR Part 11 include requirements for: Validation of electronic systems, Access controls, Audit trails, Electronic signatures, Record retention and archiving. Compliance with 21 CFR Part 11 is essential for companies operating in regulated industries to ensure the safety, efficacy, and quality of their products. Non-compliance can result in regulatory action, including warning letters, fines, or even product recalls. Overall, 21 CFR Part 11 represents a critical regulatory framework that enables the adoption of electronic recordkeeping systems while maintaining the highest standards of data integrity, security, and accountability in the pharmaceutical and healthcare industries.

KEYWORDS: FDA, Code of Federal Regulation, Electronic records, Electronic signatures, Open system, closed system.

INTRODUCTION

The executive departments and agencies of the federal government of the United States publish general and permanent rules in the Federal Register, which are codified in the Code of Federal Regulations (CFR).[1] The 50 titles that make up the CFR indicate the main categories that fall under federal control. Every title is broken up into chapters, each of which has the name of the publishing company in it. Every chapter has additional sections that address different regulatory topics. Subparts may be formed from larger parts.[2] The FR is the FDA's official standard register, where notices from Federal agencies and organizations as well as official daily publications for regulations and proposed rules are kept up to date. The register also includes executive orders and other important presidential documents. The proposed rules were initially published in the Federal Register (FR) for public comment. The completed rule will be published in the Code of Federal Regulations (CFR). The final regulations will be inserted or codified into the printed version of the Code of Federal Regulations (CFR) on an annual basis following any necessary adjustments based on feedback from the general public and professionals.[18, 19]

BACKGROUND

Structure of 21 CFR Part 11

- Title: The number that comes before "CFR"
- Part: The number that appears before the period (".") and to the right of "CFR"
- Section/Subpart: The digit located immediately after the period (".). A subpart, instead of several separate sections, is a letter of the alphabet (A–Z) that is used to get a full subpart of the CFR. As an illustration: Section E.
- Editing Year: The year being quoted is shown as a four-digit year in the "Revised as of" wording.[4]

The Food and Drug Administration (FDA), the Drug Enforcement Administration (DEA), and the Office of National Drug Control Policy (ONDCP) are regulated by Title 21 of the Code of Federal Regulations when it comes to food and drugs in the United States.

There are three chapters within it:

- Chapter 1: Food and Drug Administration (FDA)
- Chapter 2: Drug Enforcement Administration (DEA)
- Chapter 3: Office of National Drug Control Policy (ONDCP).[20]

21 CFR Part 11

The US Food and Drug Administration (FDA) regulation 21 CFR part 11 covers the use of electronic records and electronic signatures in the regulated pharmaceutical, biotechnology and medical device industries. It is intended to ensure that electronic records are trustworthy with a full audit trail.[5] With a few notable exceptions, Part 11 covers manufacturers of pharmaceuticals, medical devices, biotech firms, biologics developers, CROs, and other industries subject to FDA regulation.[6] In March 1997, the Food and Drug Agency released final part 11 regulations which defined regulations for the agency's acceptance of electronic records, electronic signatures, and written signatures executed on electronic records as comparable to paper records and, under certain conditions, handwritten signatures executed on paper. All FDA program areas are subject to these regulations, which were created to maximize the use of electronic technology while adhering to FDA's public health protection purpose. Following the effective date of August 1997, industry, contractors, and the Agency engaged in a great deal of discussion on the interpretation and application of Part 11 regulations.[7] The 21 CFR outlines the policies and processes created by the government to guarantee the following: pure and safe food; human and veterinary pharmaceuticals; biological products; medical devices; unadulterated cosmetics; and the registration and regulation of controlled drug substances.[1]

Fig No. 1

The FDA considers electronic systems, records, and electronic signatures to be trustworthy, dependable, and generally equivalent to paper records and signatures that are manually made on paper. These standards are outlined in 21 CFR part 11 (part 11).[8]

21 CFR PART 11 ADVANTAGES

- Improved data accessibility, confidentiality, and integrity
- Enhanced paperlessness
- Quicker Exchange of Information
- Minimised Risks
- Greater financial savings as a result of less storage space.[21]

The Part 11 is included in the Code of Federal Regulation Title 21. Following are the Subpart of parts of 21 CFR Part 11:

PART 11- ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A- General Provisions

- Sec. 11.1 Scope.
- Sec. 11.2 Implementation.
- Sec. 11.3 Definitions.

Subpart B- Electronic Records

- Sec. 11.10 Controls for closed systems.
- Sec. 11.30 Controls for open systems.
- Sec. 11.50 Signature manifestations.
- Sec. 11.70 Signature/record linking.

Subpart C- Electronic Signatures

- Sec. 11.100 General requirements.
- Sec. 11.200 Electronic signature components and controls.
- Sec. 11.300 Controls for identification codes/ passwords.[9]

Subpart A- GENERAL PROVISIONS

Sec. 11.1 Scope

This section contains the regulations that define the standards by which the agency determines that handwritten signatures executed on paper, paper records, and electronic signatures are generally equivalent, trustworthy, and accurate.[10] This section covers electronic records that are created, updated, preserved, archived, retrieved, or communicated in accordance with any records requirements specified in agency regulations. Even if agency regulations do not directly name such information, this section also applies to electronic records that are submitted to the agency in order to the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act.[9] The agency will consider electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations where the electronic signatures and the related electronic records meet the requirements of this part, unless specifically excluded by regulation(s) effective on or after August 20, 1997. FDA inspection rights are reserved for computer systems (including hardware and software), controls, and related documents kept under this part.[11]

Sec. 11.2 Implementation

People may substitute electronic records for paper records or electronic signatures for conventional signatures for documents that must be kept but are not submitted to the agency, in whole or in part, as long as they comply with this part's criteria. People may use electronic records in place of paper records or electronic signatures in place of traditional signatures for records submitted to the agency, in whole or in part, as long as they meet two requirements: (1) the requirements of this part are satisfied; and (2) the document or portions of the document to be submitted have been identified in public docket No. 92S-0251 as the format the agency accepts in electronic form.[9] Before attempting submission, inquire

with the FDA's receiving unit if there is any uncertainty regarding the acceptability of an electronic record.[11]

Sec. 11.3 Definitions

This section also includes the definitions of terms listed below:

- *Act:* Act refers to the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321–393), sections 201–903.[10]

- *Agency:* Agency means the Food and Drug Administration.[9]

- *Biometrics:* Biometrics is the term for a technique used to measure one's distinctive physical feature(s) or repeating action(s) that are measurable and specific to that person in order to confirm that person's identity.[12]

- *Closed system:* A closed system is one in which those in charge of the information contained in electronic records on the system have access controls.[9]

- *Digital Signature:* A digital signature is an electronic signature that is generated using a set of parameters and rules that allow the integrity of the data and the signer's identity to be confirmed. It is based on cryptographic techniques for originator authentication.[10]

- *Handwritten signature:* A handwritten signature is an individual's scripted name or legal mark that has been created by that person and is executed or adopted with the current goal of permanently authenticating writing. The practice of signing documents using a pen or stylus or other writing or marking device is kept alive. Although scripted names and legal marks are typically written on paper, they can also be written on various types of devices that record them.[12]

- *Electronic records:* A computer system can produce, modify, manage, archive, retrieve, or disseminate any combination of text, graphics, data, audio, pictures, or other digital representations of information that is called an electronic record.[10]

- *Electronic signature:* An electronic signature is any combination of symbols or computer data that has been executed, accepted, or approved by a person as the legally binding replacement for a handwritten signature.[9]

- *Open system:* An open system is one in which those in charge of the information contained in electronic records on the system have no control over who has access to it.[10]

- *Audit trail:* An audit trail is a procedure that records information changes, deletions, and additions made to an electronic record without erasing the original record. It makes it easier to reconstruct how these electronic record-related details transpired.[13]

Subpart B- ELECTRONIC RECORDS

Fig No. 2

Sec. 11.10 Controls for closed systems

Closed system controls (an environment where access is restricted by those in charge of the electronic records). The following policies and procedures must be used by anyone utilising closed systems to "create, modify, maintain, or transmit electronic records." It is also important to make sure that the signer cannot retract the records as being false. Such procedures and controls shall include the following:

a) Validation of systems to guarantee their correctness, dependability, ability to identify tampered or erroneous records, and consistent intended performance.

b) The capability of producing precise and comprehensive records in both electronic and human readable formats that are appropriate for the agency's inspection, evaluation, and reproduction. Any queries people may have about the agency's capacity to carry out this kind of electronic document examination and copying should be directed to the agency.

c) Records are safeguarded to allow for precise and timely retrieval throughout the duration of the records retention period.

d) Restricting access to the system to those who are authorised.

e) The date and time of operator entries and actions that produce, edit, or remove electronic records are separately recorded by means of secure, computer-generated, time-stamped audit trails. Changes to the records must not mask information that has already been recorded. This audit trail documentation must be kept on file for as long as necessary to accommodate agency examination and copying of the relevant electronic documents.

f) When necessary, use operational system checks to enforce the allowed order of actions and events.

g) Authority checks are used to make sure that only those with permission can access the system, sign

documents electronically, operate computer systems, change records, or carry out the current task.

h) Use of device (such as a terminal) checks to ascertain the reliability of the operational instruction or data input source as needed.

i) Confirmation that those who create, manage, or utilise electronic record and electronic signature systems possess the knowledge, expertise, and experience necessary to carry out their given responsibilities.

j) To identify record and signature falsification, written procedures that hold people accountable and responsible for acts taken using their electronic signatures must be established and followed.

k) Use of suitable controls over the distribution, availability, and use of documentation for system upkeep and operation, such as: (1) Sufficient measures to regulate the distribution, availability, and utilisation of documentation related to system maintaining and operation. (2) Procedures for revision and change control are necessary to keep an audit trail that shows the chronological growth and alteration of systems documentation.[9]

Sec. 11.30 Controls for open systems

In order to guarantee the validity, integrity, and, when necessary, confidentiality of electronic records from the time of creation to the time of reception, those who utilise open systems for creating, modifying, maintaining, or transmitting electronic records must apply policies and procedures.[15] These protocols and controls must include those mentioned in section 11.10, if applicable, as well as extra steps such document encryption and the use of suitable digital signature standards to guarantee record authenticity, integrity, and secrecy, as needed under the circumstances.[11]

Sec. 11.50 Signature manifestations

Electronically signed documents must provide information on the signature that clearly states each of the following:

a) The signed party's printed name;
b) The time and date of the signature's execution; and
c) The signature's associated meaning (e.g., review, approval, responsibility, or authorship).[9]

The items mentioned in the section above must be a part of any human-readable version of the electronic record (such as an electronic display or printout) and must be subject to the same controls as electronic records.[11]

Sec. 11.70 Signature/record linking

To guarantee that handwritten and electronic signatures executed on electronic records cannot be removed, copied, or otherwise transferred to falsify an electronic record using common means the signature must be connected to the relevant electronic record.[15]

Subpart C- ELECTRONIC SIGNATURES

Fig No. 3

Sec. 11.100 General requirements

Electronic signatures can only be used by one person at a time and cannot be transferred to another person. An organisation must confirm the identification of the person before establishing, assigning, certifying, or in any other way endorsing the person's electronic signature or any component thereof.[11] When utilising electronic signatures, individuals must first attest to the agency that the signatures in their system, whether created before or after August 20, 1997, are meant to serve as the legally binding counterpart of conventional handwritten signatures.

a) The certification must be sent to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857, on paper, with a typical handwritten signature.

b) Those who use electronic signatures must certify or testify in writing that a particular electronic signature is the legally binding equivalent of the signer's handwritten signature upon request from an agency.[9]

Sec. 11.200 Electronic signature components and controls

Electronic signatures that do not rely on biometric technology for identification must:

a) Use a password and an identification code, or at least two different identifying elements. (1) If a person performs multiple signatures within a single, uninterrupted session of authorised system access, the first signature must be performed using every electronic signature component; the remaining signatures must be performed using a minimum of one electronic signature component that is executable and intended for use exclusively by the person. (2) Every electronic signature component must be used when a person performs one or more signatures that are not done within a single, uninterrupted period of controlled system access.

b) Be utilised exclusively by their authorised owners; and

c) Be administered and executed to assure that attempted use of an individual's electronic signature by anyone other than its authorized owner requires collaboration of two or more individuals.[15]

Biometric-based electronic signatures must be created in such a way that only their authorised owners can use them.[9]

Sec. 11.300 Controls for identification codes/ passwords

Controls must be used to guarantee the security and integrity of electronic signatures used by individuals utilising identifying codes combined with passwords. These measures will comprise:

Preserving the distinctiveness of each combination of password and identification code, such that no two people have the same combination.

Ensuring that password and identification code issuances are reviewed, recalled, or updated on a regular basis (e.g., to cover such events as password maturation).

In accordance with loss management protocols, tokens, cards, and other devices bearing or generating identification code or password information that are lost, stolen, missing, or otherwise potentially compromised may be electronically deauthorized. Temporary or permanent replacements may then be issued using appropriate, stringent controls.

Use transaction safeguards to stop passwords and/or identification codes from being used without authorization. You can also use them to identify and report any attempts at unauthorised use of passwords or identification codes to the system security unit and, if necessary, organisational management, right away.

Devices that carry or create an identity code or password should be tested both initially and on a regular basis to make sure they are working correctly and haven't been tampered with.[9]

Part 11 of CFR 21 has the following essential requirements

a) Program modifications are logged separately from the programs themselves.
b) The source or sources of an output can be determined.[17]

Classification of 21 CFR Part 11 specifications

Table No. 1: Requirements of 21 CFR part 11.

Requirement	Section of Rule
Validation	11.10(a)
System Security	11.10(d), 11.10(f), 11.10(g)
Audit Trails	11.10(e), 11.10(k2)
Electronic signature management	11.5, 11.70, 11.100, 11.200
Electronic records management	11.10(b), 11.10(c)
Open Systems validation	11.30
Documentation control	11.10(k1), 11.10(k2)
Training of personnel	11.10(i), 11.10(j)
Management of codes and passwords	11.300

Validation

Enforcement discretion will be exercised with regard to the particular Part 11 validation criteria (accuracy, consistent intended performance, altered and invalid records). According to the FDA, the validation's base and scope should be established by a well-supported and documented risk assessment of the system.[16]

Security

a) Physical Security: To guarantee restricted physical access to computerized systems and that only authorized personnel have access, external protections must be in place. Employees need to be completely informed about the security measures in place. The Standard Operating Procedures ought to provide a description of these security measures.

b) Logical Security: A computerized system's logical security should cover internal security measures and data access control mechanisms. These security measures ought to specify how the software, log-on process, security protocol, and audit trail are used to limit data access. The names, titles, and access privileges of authorized personnel should be listed in a cumulative record that is available through the system. A computerized system should be re-evaluated if "any" software changes are made in order to identify any changes to the logical security. Controls that identify and prevent computer viruses should also be implemented. If a computerized system is used for other purposes, efforts should be made to prevent a compromise of the data through an interaction with other software.

Audit Trail

Electronic record systems must keep an audit trail to guarantee the authenticity, integrity, and confidentiality of those records as required by the Electronics Records and Electronic Signatures Rule (21 CFR 11.10(e)). Therefore, in order to "independently" record the date and time of operator entries that create, modify, or delete records, people must employ secure, computer-generated, time-stamped audit trails. It is important to

build the audit trail in a way that makes it impossible for that person to modify it. The audit trail needs to be sequential and incremental, and it needs to be kept up to date for as long as the study records are needed.[14]

Electronic signature management

Every user and system administrator has a unique electronic signature assigned to them. Electronic signatures can be created using biometrics, token-based authentication, passwords, and user names. An electronic signature system addresses nonrepudiation, user authentication, and record integrity. To guarantee that they are only used by the owners, security measures are in place. When it comes to electronic signatures without biometric connections, two or more distinct identification methods are used. It is recommended that both of these unique identification processes be used for the first signature, and that each subsequent signing within the same session employ at least one of them. It's crucial to ensure that the design of the system for electronic signatures with biometric links prohibits users other than the owners from using them. Steps done to guarantee that each electronic signature is unique and that they are only provided to people whose identities have been verified.

Electronic records management

It is necessary to have controls in place to guarantee that electronic records are created, saved, protected, and retrieved in both electronic and human formats appropriately. One method to make sure this part of the ruling is followed is to use industry standard portable formats for electronic records.[7]

Training of Personnel

To execute this activity, an individual must possess the necessary "education, training, and experience," or a combination of these, if they are entering or processing data. Not only should specific operations be trained for, but ongoing training should also be given as needed to ensure familiarity with any operational changes. Documentation of training requirements and completion is required.[14]

Management of Codes and Passwords

Controls in this region include the following:

a) Every password and identifying code must be distinct.
b) Checking passwords and identifying codes on a regular basis
c) Techniques for managing losses
d) Transaction protection to stop illegal use of identification codes or passwords
e) Tests of gadgets that provide password or identifying code data.[14]

ELECTRONIC CODE OF FEDERAL REGULATIONS (e-CFR)

The Office of the Federal Register (OFR) of the National Archives and Records Administration, along with the Government Printing Office, generated the unofficial editorial collection of CFR material and FR changes that is known as the e-CFR, which is the most recent updated edition of CFR. It is a legitimate, official publication of the CFR, nevertheless. The OFR will update the e-CFR with the new contents every day. Every e-CFR webpage has the most recent update Status displayed at the top.[3]

CONCLUSION

In conclusion, a review of 21 CFR Part 11 highlights its significance in regulating electronic records and signatures within FDA-regulated industries. The article emphasizes the importance of compliance with Part 11 requirements to ensure the integrity, reliability, and security of electronic data in these sectors. It discusses key aspects such as electronic recordkeeping, audit trails, electronic signatures, and validation requirements, underscoring the need for organizations to adopt robust systems and procedures to meet regulatory standards. Furthermore, the review article likely discusses challenges and best practices associated with Part 11 compliance, including technological advancements, data security concerns, and evolving regulatory expectations.

Overall, this review article serves as a valuable resource for stakeholders in FDA-regulated industries, providing insights into the regulatory landscape, compliance strategies, and the evolving role of technology in maintaining data integrity and regulatory compliance.

REFERENCES

1. Marlene S. Bobka the 21CFR Online Database, Medical Reference Services Quarterly, 1993; 12(1): 7-15, DOI: 10.1300/J115V12N01_02.
2. Code of federal regulations [Internet]. 2022 [cited 2024 Apr 8]. Available from: https://www.govinfo.gov/help/cfr
3. Prakash Srinivasan, Timiri Shanmugam, Pugazhenthan Thangaraju, Nandakumar Palani, Thamizharasan Sampath; Medical Device Guidelines and Regulations Handbook; Springer publication; Page no 189; Available at, https://doi.org/10.1007/9783-030-91855-2 ; ISBN 978-3-030-91855-2.
4. Title 21 of the code of federal regulations [Internet]. Wikimedia Foundation; 2022 [Cited 2024 Apr 8]. Available from:https://en.wikipedia.org/wiki/Title_21_of_the_Code_of_Federal_Regulations
5. Hyde A, Burgess S, Goulden J. The Use of 'Live Chemical Imaging' to Enhance and Increase Productivity in SEM/EDS Investigation of Pharmaceutical Samples, While Still Conforming to 21 CFR Part 11 Regulations. Microscopy and Microanalysis, 2019; 25(S2): 1276-1277. Doi: 10.1017/S1431927619007116
6. "Food and Drug Administration CFR Title 21 Part 11" Microsoft. Retrieved 15 September 2016.
7. Chaugule, Shruti, et al. "Review on 21 CFR Part 11 in pharmaceutical industry." World Journal of Pharmacy and Pharmaceutical Science, 16 May

2022; 11(6): 845–864. https://doi.org/7. 10.20959/wjpps20226-22292.
8. Centre for Drug Evaluation and Research. "Electronic Systems, Electronic Records, and Electronic Signatures." U.S. Food and Drug Administration, FDA, 15 Mar. 2023, www.fda.gov/regulatoryinformation/searchfdaguidancedocuments/electronicsystemsel ectronic-records-andelectronicsignaturesclinicalinvestigationsquestions.
9. FDA, 21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule. Federal Register, March 20, 1997; 62(54): 13429.
10. Code of federal regulation, 2023; 21(1): 241-246.
11. RICHESON, MARIN. The Ultimate Guide to 21 CFR Part 11, Perficient, www.perficient.com/-/media/files/guide-pdf-links/the-ultimateguideto21cfrpart11.pdf. Accessed 7 Apr. 2024
12. CFR− Code of Federal Regulations Title 21 [Internet]. Part 11 Electronic Records; Electronic signatures. Available online at: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/ CFRSearch.cfm? CFRPart=11&showFR=1, Updated 1 April 2010. Accessed 18 April 2011.
13. FDA Guidance for Industry [Internet]. Computerized Systems Used in Clinical investigations. Available online at: http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidance/ UCM070266.pdf, Updated May 2007. Accessed 14 April 2011.
14. Kendy L. Keatley (2000) A Review of US EPA and FDA requirements for electronic records, electronic signatures, and electronic submissions, Quality Assurance, 7: 2, 7789. http://dx.doi.org/10.1080/10529410050133844
15. US Food and Drug Administration. 21 Code of Federal Regulations 11, Electronic Records; Electronic Signatures Final Rule. Office of the Federal Register, National Archives and Records Administration, Washington DC, USA (1997).
16. CFR American pharmaceutical review McDowall-Part-11-is-Dead-AmPhRevDec2003
17. Garbutt D.J. (2008) 'Implementing CFR 21 part 11 for SAS®without tears or joins', pharmaceutical programming, 1(2): 78-91. Doi: 10.1179/175709208x387003
18. U.S. Food and Drug Administration. 19 Sept. 2019, www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPartFrom=800&CFRPartTo=1299. Accessed 22 Jun. 2020
19. FEDERAL REGISTER. The Daily Journal of the United States Government, www.federalregister.gov/agencies/food-and-drug-administration. Accessed 2 June 2020
20. CFR Title 21 US FDA. Retrieved February 10, 2014 https://en.wikipedia.org/wiki/Title_21_of_the_Code_of_Federal_Regulations
21. Title 21 CFR part 11(2024) Wikipedia. Available at: https://en.m.wikipedia.org/wiki/Title_21_CFR_Part_11 (Accessed: 24 April 2024)