LIGHTHOUSE
WORLDWIDE SOLUTIONS

21 CFR PART 11
OVERVIEW

Lighthouse Worldwide Solutions

Overview

21 CFR Part 11 outlines the federal requirements that help to ensure that electronic records are trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper. 21 CFR Part 11 has 10 chapters over 3 subsections. These subsections are General Provisions, Electronic Records and Electronic Signatures.

21 CFR Part 11 is divided into three sub-parts:

The General Provisions section discusses the scope of the regulations, when and how it should be implemented, and defines some of the key terms used in the regulations.

The Electronic Records section sets forth the requirements for administration of closed and open electronic record-keeping systems, then discusses signature manifestations and requirements for establishing a link between signatures and records.

The Electronic Signatures section is split into three parts: general requirements for electronic signatures, electronic signature components and controls, and controls for identification codes/passwords.

Below we see the three subsections with each section outlined.

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**

The FDA guidelines from Part 11 help establish accountability and traceability throughout your documentation processes, by ensuring that:

- **Access to electronic records is limited to authorized individuals**
- **Account sharing between individuals, groups or departments is not permitted**
- **Adequate security protocols are followed to ensure the integrity of passwords and login credentials for all users**
- **Electronic signatures cannot be transferred or copied between documents**
- **Electronic signatures are certified to be the same as handwritten signatures, and that the certification is mailed to the FDA**
- **Records are tracked through document controls and an audit trail that monitors changes and discerns invalid or altered records**

The basic premise of the 21 CFR Part 11 summary is simple: the data and electronic signatures used in any business efforts need to be secure and need to follow all of the guidelines of this compliance code. The manifestation is more than a digital signature or key—it is an actual physical representation of a wet signature, and it has to meet all of the criteria in order to be proven compliant and legally binding.

In addition, all electronic records must be stored according to the regulation in a validated, secure system that has met all of the compliance markers set forth by the FDA in the code that was established in 1997. Life sciences organizations utilizing electronic systems for learning and training, data storage and record keeping, and other operations and functions will need to familiarize themselves with CFR Part 11 and how it impacts their business.

Let's get into the details of 21 CFR Part 11 so you can have a well-grounded understanding of the requirements from the General Provisions to understanding what an electronic record is and what is an electronic signature and how to apply 21 CFR Part 11 into your companies' systems. So, let's look at each section to get a good overview of

SUBPART A - GENERAL PROVISIONS

Sec. 11.1 Scope - This is the first section of 21 CFR Part 11, and its goal is to establish what this regulation does and when it should be applied. The regulations in 21 CFR Part 11 set forth the criteria under which the FDA considers electronic records and signatures to be trustworthy, dependable, and equivalent to paper-based records. 21 CFR Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, and/or transmitted under any records requirement set forth by the FDA.

Sec. 11.2 Implementation - This section explicitly states that medical device companies can use paperless record-keeping systems if they are following this regulation. For medical device companies who wish to transmit electronic records to the FDA, they may do so if they comply with this regulation and if the documentation, they wish to submit is identified in docket No. 92S-0251 as a type of submission that the agency accepts in electronic form.

Sec. 11.3 Definitions - The FDA provides definitions for some of the terminology that will be used later in Part 11. One example would be the difference in definitions between closed systems and open systems. A closed system is a record-keeping system where system access is controlled by persons who are responsible for the content of electronic records on the system. In an open system, access is not controlled by persons who are responsible for the contents of the electronic records on the system.

SUBPART B - ELECTRONIC RECORDS

Sec. 11.10 Controls for closed systems - This section sets forth 11 separate and distinct security management requirements for companies that wish to keep electronic records using a closed software system. Some of the requirements include limiting system access to authorized individuals, authority, and device checks to verify the integrity of data and signatures, the establishment of written accountability policies for maintaining system security, and the appropriate validation of the record-keeping system to ensure consistency in its intended performance. The FDA also establishes the audit trail requirements in this section. Companies must maintain appropriate control over systems documentation, including revision and change control procedures to maintain an audit trail that documents change in the system. An audit trail ensures that every activity which happens in the record-keeping system generates a record and can be reviewed later.

Sec. 11.30 Controls for open systems - Open systems typically mean that more people have access to the record-keeping system, so the security requirements should be slightly more comprehensive to help ensure that the records kept are accurate and reliable. This section recommends that open systems are subject to the same 11 security requirements as closed systems, along with any additional appropriate measures such as document encryption and the use of digital signature standards to ensure the integrity and confidentiality of the records.

Sec. 11.50 Signature Manifestations - This section deals with how signatures should appear on electronic records. The FDA expects to see the printed name of the signer, the date and time that the signature was executed, and the meaning of the signature (approval, review, authorship, etc.) subjected to the same controls as the records themselves and included on any human readable form of the electronic record.

Sec. 11.70 Signature record/linking - A section so short, we can quote it: Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

This means that medical device companies must use a record-keeping software that tracks the approval status of documents using secure attribution data. The system should not allow any user with inadequate permissions to affect a signature by copying a signature from one document and attaching it onto another.

SUBPART C - ELECTRONIC SIGNATURES

Sec. 11.100 General Requirements - This section sets forth some of the requirements for personal accountability in electronic signatures that are central to this regulation. It requires organizations to verify the identity of any individual who is assigned an electronic signature on the system and that medical device companies who wish to use electronic signatures must notify the FDA in writing by mail. The agency's Rockville, MD address is provided.

Sec. 11.200 Electronic signature components and controls - The FDA wants electronic signatures to use at least two identifying components - such as including an identification code and a password. Electronic signatures should be assigned to individual persons - not to groups or departments - such that each electronic signature can only be executed by a single person to whom it is assigned and whose identity was verified in compliance with this part. The FDA really wants to make sure that approval and review signatures cannot be disputed once they are entered into the system.

Sec. 11.300 Controls for identification codes/passwords - 21 CFR Part 11 requires special security measures for the control of passwords. No two individuals should use the same identification/ password to access the system, and passwords should be changed periodically to protect against password aging. Medical device companies must establish transaction safeguards that prevent unauthorized use of passwords. Loss management procedures should be established to ensure that compromised security tokens, cards or other devices are deauthorized to prevent security breaches.

As suppliers of environmental monitoring systems and instruments we design our products to have the best technological advances which enable data integrity and adherence to 21 CFR Part 11. However, there are some requirements of 21CFR Part 11 which the end user must conform to let's examine each of these requirements, so you are fully aware of your responsibilities.

Subpart B - Electronic Records

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

[Section (i) requires the End Users to verify that the persons who develop, maintain, or use electronic records/signatures need to have the education, training and experience. By maintaining employee records on a Quality System and a job description for that employee this end user requirement is straightforward]

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

[Section (j) requires written policies to hold individuals accountable and responsible for actions initiated under their electronic signatures to deter record and signature falsification, individuals must receive training and acknowledgement of such policies and it all must be documented on the quality system]

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

[Section (k) Requires documented controls for access to and system operation and maintenance – these controls can be developed from User Manuals and internal policy and procedures outlined and these documents need to follow change control procedures with an audit trail with time stamps on the development of system documents.]

Subpart C - Electronic Signatures

Sec. 11.100 General requirements

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

[In Subpart C - Electronic Signatures - section (B) requires the organization to verify the identity of the individual within the company who will be using an electronic signature. In section (C) requires an organization to certify that any electronic signatures used after Aug 20th, 1997, are legally binding].

21 CFR PART 11 KEY TAKEAWAYS

GENERAL

21 CFR Part 11 refers to a particular chunk of the Code of Federal Regulations issued by the United States to regulate drugs.

21 CFR Part 11 consists of three Subparts:

- **A – General Provisions**
- **B – Electronic Records**
- **C – Electronic Signatures**

SUBPART A – General Provisions

Part 11 applies to all electronic records that fall under FDA regulations. If an organization can prove to an auditor that their electronic records/signatures are as trustworthy as paper records/ink signatures, the FDA will accept electronic instead of paper. The FDA will accept electronic submission instead of paper if those submissions **1)** adhere to Part 11 requirements and **2)** are included among the types of documents that the FDA accepts electronically.

SUBPART B – Electronic Records

Organizations using electronic records must establish and document procedures and controls that ensure the following qualities in their electronic records:

- **Authenticity**
- **Integrity**
- **Confidentiality (when appropriate)**
- **Irrefutability (i.e., no way to deny that a record is genuine)**

The following topics must be addressed in documented procedures and controls: computer systems validation (CSV), record rendering, document storage and record retention, system access, audit trails, workflows, authority checks, device checks, personnel qualifications, personnel accountability, and document control. Systems that fall into the category of "Open" (as defined in Subpart A) require additional procedures/controls.

Electronic signatures must include the printed name of the signer, the date and time of the signature, and the meaning of the signature. Electronic signatures must be forever linked to their respective records.

SUBPART C – Electronic Signatures

Organizations that wish to use electronic signatures must inform the FDA in writing prior to making the switch. Each individual who will be using an electronic signature must 1) have their identity confirmed and 2) use a unique signature that has never been and will never be used by another individual.

There are specific design requirements for electronic signatures that are biometric (e.g., fingerprint scan) and those that are not (e.g., user ID and password). For electronic signatures that make use of user IDs and passwords/passcodes, there are specific requirements for passwords and for passcode generating device.

End Users Responsibility

There are sections of 21 CFR Part 11 that are required to be addressed by the end user. Specifically, about;

- **Access**
- **User ID and training**
- **Internal Policies**
- **Certification responsibilities**
- **SOP's**

For further information on 21 CFR Part 11 the Lighthouse Worldwide Solutions is a library of knowledge and you can access this information here.

https://www.golighthouse.com/en/knowledge-center