eSignatures Overview

31/07/2025 12:37 pm BST

Relates to version
Tags: 9.0

Certain digitally collected data may require a signature. For medical device manufacturers, FDA 21 CFR Part 11 establishes the requirements that ensure electronic signatures are legally equivalent to handwritten ones, and that digital records are as trustworthy and legally valid as traditional paper documentation.

FDA 21 CFR Part 11 Requirements

FDA 21 CFR Part 11 sets the regulatory framework for the use of electronic records and electronic signatures in FDA-regulated industries. It relates to the electronic systems as well as ensuring those systems are validated, secure, and auditable.

Signature profiles are central to ensuring compliance. Each profile defines:

- The number of required signatures (e.g., one or two).
- The meaning of each signature (e.g., approval, verification, data collection).
- The permissions required to sign (e.g., role-based access).
- The timing of the signature—whether it is captured live at the point of data entry or retrospectively at a later stage.

This structure ensures that signatures are not only secure but also contextually meaningful and auditable.

Main Regulatory Requirements

The main regulatory requirements for eSignatures are are:

Electronic Signatures

Electronic signatures must be:

- Unique to each individual.
- Linked to the corresponding record.
- Legally binding, with the same weight as handwritten signatures.

The system must verify the identity of the signer and ensure that signatures cannot be falsified or reassigned.

Uniqueness and Identity Verification

Each electronic signature must be unique to one individual and not reused or reassigned to anyone else.

Signature Components and Controls

Electronic signatures must include at least two distinct identification components, such as a username and password.

These credentials must be:

- Unique to each user.
- Securely maintained and periodically updated (e.g., password aging).
- Protected against unauthorised use, requiring collaboration of two or more individuals to misuse.

Linking Signatures to Records

Signatures must be permanently linked to their respective electronic records to prevent falsification or unauthorised transfer.

Audit Trails and Attribution

Systems must maintain audit trails that capture who signed what, when, and why. The meaning of the signature (e.g., approval, review) must be clearly indicated.

Customer Obligations

In addition to the system requirements, customers should be aware that they must adhere to the following to comply with FDA 21 CFR Part 11:

- Organisations must verify the identity of individuals before assigning electronic signatures.
- Certification to the FDA.
- Organisations must certify to the FDA that electronic signatures are legally binding equivalents of handwritten signatures.
- This certification must be signed with a traditional handwritten signature and submitted in paper or electronic form.

System Validation

Electronic systems must be validated to demonstrate that they function as intended. This includes:

- Accurate data capture.
- Reliable performance.
- Consistent behaviour under expected conditions.

Validation is essential to prove that the system can maintain data integrity and support regulatory audits.

Audit Trails

Systems must generate secure, computer-generated audit trails that record:

- Who accessed or modified a record.
- When the action occurred.
- What changes were made.

These trails must be tamper-evident and retained for the duration required by applicable regulations.

Record Retention and Accessibility

Electronic records must be:

- Readable and retrievable throughout their retention period.
- Available in both human-readable and electronic formats.
- Protected against loss or corruption.

This ensures that records can be reviewed during inspections or audits without technical barriers.

Security Controls

Access to electronic systems must be restricted to authorised users. This includes:

- Role-based permissions.
- Password policies.
- Account management procedures.

Security measures must prevent unauthorised access and ensure accountability for all actions taken within the system.