7 Key FDA e-Signature Requirements

A 21 CFR Part 11 Checklist

How does your organisation authorise, authenticate, document and police the use of electronic signatures within your eQMS? Do you meet the specific standards of the infamous FDA CFR Part 11? Here's a helpful 7 point checklist to help you navigate your med dev compliance responsibilities:

cognidox

1. Is your e-signature control and activity logging robust enough for CFR Part 11?

Medical device developers need the ability to control and manage electronic signatures as an approval mechanism within an eQMS. Your system should be capable of managing e-signature use and validity across your organisation, authorising only specific individuals to edit, update and sign off on documents. The system should also be capable of generating complete audit trails showing the edit and approval history of each document. These records need to be retained & accessible for audit, for as long as the law requires:

The regulation itself states:

11.10 Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.

11.10b The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.

11.10c Protection of records to enable their accurate and ready retrieval throughout the records retention period.

11.10d Limiting system access to authorized individuals.

11.10e Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

11.10g Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

2. What information does your system capture when a document is signed electronically?

Does your e-signature solution capture the name, date/time and meaning of electronic signatures as they are applied to documents? If the document is printed out are those details always automatically appended?

11.50 Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

11.50b The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

3. Does your e-signature solution meet these key authentication requirements?

In order to further safeguard the integrity of the digital signing process there must be measures in place to ensure they are only used by their genuine owners. Does your system require the following ID combinations to 'sign' a document, as well as 'authentication on approval' functionality to further confirm a user's identity?

11.200a Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

4. Are your e-signatures the equivalent of traditional handwritten signatures?

What do you need to do to ensure your electronic records and signatures are regarded as the 'equivalent' of printed documents hand signed 'in ink.'? The FDA website says that you must send a letter of confirmation:

11.100c 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.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

5. How do you enforce your password controls?

The following controls for identification codes and passwords are mandatory to ensure they are unique to individuals and you are regularly checking exactly who has access to your systems:

11.300 Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

11.300a Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

11.300b Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

6. Can you remotely cancel or freeze access to your eQMS?

The FDA require you to have complete and instantaneous control over who can access your system and use e-signatures:

11.300c Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

7. Are you scanning your system to prevent unauthorized access

Your system needs to proactively safeguard against unauthorised e-signature use

11.300d Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

Conclusion

As shown in this guide the e-signature requirements for medical device developers are as robust and demanding as you would expect. But they actually don't insist on things like digital signature encryption or biometric solutions as some often assume.

The truth is there's a lot of misunderstanding and misinformation about the exact requirements of 21 CFR Part 11. Some eQMS solutions signature solutions are frankly over-engineered and overly expensive. But if you do try to 'do it yourself' with Google Drive, DropBox and various plug ins, there is a danger you could end up falling short on the exact detail of the operational requirements. Get that wrong and you risk failing audits and facing fines.

Maybe it's time to do an audit of your current capabilities against the full details of FDA Part 11 listed here. As you prepare your product for launch you need to ensure your system is able to deliver what the regulation demands, in a way that won't slow you down.

Discover how Cognidox can help you.

See how to integrate FDA compliant e-signatures into a LEAN digital QMS.

Book A Demo Here

cognidox