EBOOK

21 CFR Part 11: A Complete Guide

Etienne Nichols,
Medical Device Guru, Greenlight Guru

greenlight guru

www.greenlight.guru

21 CFR Part 11: A Complete Guide

Table of Contents

2 What is 21 CFR Part 11?

3 What are the different parts of 21 CFR Part 11?

- 4 21 CFR Part 11: Subpart A—General Provisions
- 6 21 CFR Part 11: Subpart B—Electronic Records
- 8 21 CFR Part 11: Subpart C—Electronic Signatures

9 Key takeaways of 21 CFR Part 11

10 How Greenlight Guru helps you comply with 21 CFR Part 11

Medical device companies that wish to sell their devices in the US and EU must implement a quality management system that meets the requirements of 21 CFR Part 820 and ISO 13485:2016.

We believe in “right-sizing” your quality management system (QMS), allowing it to scale with your company as you work through product development to establish supplier controls and a CAPA process, etc. But what are you going to do with all of that paper being generated as a result?

Many medical device companies today can see the value of investing in a medical device specific eQMS that helps to bring your product to market faster, and can make FDA inspections and ISO audits go smoother; however, the added caveat is that these systems are subject to validation.

Specifically, 21 CFR Part 11, the FDA’s regulations for electronic documentation and electronic signatures. This regulation is widely misunderstood and this confusion even causes some medical device companies to resist moving to electronic systems when they know it’s the right move.

In this comprehensive guide, we’ll take you through each section of 21 CFR Part 11, explaining what the requirements actually mean and expounding the most important points for you to know as a medical device company.

Then in the conclusion, we’ll also highlight a few key features of Greenlight Guru’s eQMS platform and how those have proven to be instrumental in helping medical device companies get to market faster while remaining compliant with 21 CFR Part 11.

What is 21 CFR Part 11?

In March of 1997, the United States FDA issued regulations that established the criteria for the acceptance by the FDA of electronic records, electronic signatures and handwritten signatures executed to electronic documents.

These laws are codified as Part 11 of Title 21 in the Code of Federal Regulations, or 21 CFR Part 11, or Part 11 for shorthand.

Since its original publication, 21 CFR Part 11 has generated a significant amount of confusion among medical device makers and other industry professionals that may use electronic records. The FDA published a guidance document in August 2003 to clarify the scope and implications of various parts of the regulations.

This document also served to further elucidate the requirements for software validation, audit trails, managing legacy systems, keeping copies of records and record retention. It also contained helpful information about what companies need to do in order to comply with its 21 CFR Part 11 requirements.

With that said, it is important to remember these kinds of guidance documents themselves are not the law and medical device companies should always refer directly to 21 CFR Part 11 when assessing their compliance status with FDA regulations.

What are the different parts of 21 CFR Part 11?

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.

Let's take an in-depth look into each section of 21 CFR Part 11 and pick out the most important points that medical device companies need to be aware of.

21 CFR Part 11: Subpart A—General Provisions

As the opening section of 21 CFR Part 11, Subpart A provides us with the *who*, *what*, *where*, *when*, *and why* of the regulation. In three succinct sections, Subpart A of 21 CFR Part 11 establishes:

- The purpose of 21 CFR Part 11
- How 21 CFR Part 11 works
- The circumstances, settings, and when the regulation should be applied
- Definitions for the key terms used throughout the 21 CFR Part 11 regulation's text

Sec. 11.1 Scope—The regulations in 21 CFR Part 11 set forth the criteria under which the FDA considers records and signatures in an electronic format to be trustworthy, reliable, and generally equivalent to paper 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.

While there are some examples listed of agency-required records that are not subject to 21 CFR Part 11, quality management records are not listed among the exclusions here. As soon as a medical device company uploads any part of their quality management system to a computer, they are subject to the requirements of 21 CFR Part 11. (And this is a little known fact that many paper-based companies are not aware of.)

Sec. 11.2 Implementation—This section explicitly states that medical device companies can use paperless record-keeping systems if they are in compliance with 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.

- Act: Refers to the Food, Drug, and Cosmetic Act.
- Agency: Refers to the Food and Drug Administration.
- Biometrics: means a method of verifying an individual's identity based on measurement of the individual's unique physical feature (such as a fingerprint) or repeatable action (such as typing style).
- Closed System: A computer system whose user access is controlled by the same people responsible for its contents.
- Digital Signature: A type of electronic signature that includes a way of verifying the identity of the signer, the validity of their signature, and the integrity of the record they signed.
- Electronic Record: Information in a digital form that is created or used in some way by a computer system.
- Electronic Signature: A set of symbols that is as unique and legally binding as a handwritten signature, but that is used to sign records in a computer system.
- Handwritten Signature: A scripted name or legal mark created by an individual that is unique to that individual and is used to authenticate something in writing.
- Open System: A computer system where user access is NOT controlled by the same people responsible for its contents.

Pay attention to 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.

This terminology should not be confused with "open source" or other uses of "open/closed" as a descriptor. In this context, a closed system is one where the company keeps the records only on its own hardware and is accessible through its own internal network, while an open system is one where a vendor offers record-keeping software through a license to the medical device company and therefore controls access to the software and the records.

21 CFR Part 11: Subpart B—Electronic Records

With formal introductions out of the way, Subpart B of 21 CFR Part 11 digs into the details of electronic records. In four sections, Subpart B covers:

- Basic requirements for electronic record keeping
- Additional security requirements for open systems
- Details on signature appearance on electronic records
- Requirements for linking signatures to 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.

- **Validation** to provide proof that the data in a computer system can be trusted.
- **Rendering Records** to ensure that all electronic records are provided in a readable format that humans (not just computers) can understand.
- **Document Storage & Record Retention** to safeguard documentation and keep it available as long as needed
- **System Access** to ensure that only the right people have access to each computer system.
- **Audit Trails** to provide a complete history of all electronic records automatically captured by a computer system
- **Workflows** to ensure computer systems function correctly.
- **Authority Checks** to limit user access (system level and record level) and verify that the users performing functions in the system are authorized to do so.
- **Device Checks** to verify that equipment being used for regulated purposes is functioning properly.
- **Personnel Qualifications** which ensures only trained and qualified people perform functions on or within the system.
- **Personnel Accountability** which holds individuals accountable for the integrity of their actions related to electronic records and electronic signatures.

- **Document Control** for electronic records related to system operation and maintenance and the preservation of the complete history of changes made to these documents.

The audit trail requirements in this section are similar to the document control requirements of 21 CFR Part 820. Medical device companies must maintain appropriate control over systems documentation, including revision and change control procedures to maintain an audit trail that documents changes 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.

21 CFR Part 11: Subpart C—Electronic Signatures

You can't have electronic records without electronic signatures, and 21 CFR Part 11 makes this abundantly clear in Subpart C. In three distinct section, Subpart C establishes:

- Requirements for identity verification in electronic signatures
- Security controls for electronic signatures
- Guidance on the usage of logins and passwords

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.

Key takeaways of 21 CFR Part 11

21 CFR Part 11 provides an opportunity for medical device companies to reap the organizational benefits of paperless record-keeping systems. It also helps the FDA ensure that when medical device companies use electronic record-keeping systems, that document security and authenticity are adequately maintained.

While some may argue that regulations of 21 CFR Part 11 place an additional regulatory burden on these companies, it's important to note significant benefits can be derived from implementing these electronic systems.

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

Medical device companies will benefit from embracing the regulations of 21 CFR Part 11 because it will serve as a catalyst in protecting the integrity and confidentiality of their proprietary data.

How Greenlight Guru helps you comply with 21 CFR Part 11

Greenlight Guru is the only electronic quality management system (eQMS) designed exclusively for medical devices and is built to help MedTech companies ensure compliance with industry-specific regulations, such as 21 CFR Part 11.

Our purpose-built solution is built with a suite of superior functionalities, such as our “no-effort” validation process, allowing companies to seamlessly carry out the validation process through our own validated OQ PQ process, which includes key requirement components of Part 11.

We believe it’s imperative that we follow the same practices as our customers; so, with every new release of our software we include validation documentation of executed test cases confirming the steps that were followed in the validation process.

We provide objective evidence from a third party assessment confirming the validation of the automated process we use – adhering to the same stringent document and record security and audit trail requirements set forth by the FDA for compliance with 21 CFR Part 11.

Let’s consider other contrary methods to approaching this process. Companies who use paper-based systems must manually oversee these operations, ensuring complete accuracy and efficacy with document control and security-based activities. A lot of effort is required for doing it this way, not to mention the myriad of risks associated with the likelihood of human error.

Let’s say you’re not paper-based but instead use a general-purpose QMS tool. Given how it’s general-purpose, you will need to spend a great deal of time and effort to engineer the system you want. This introduces a lot of risk because medical device QMS best practices won’t be built in.

But what if you have a great team and are able to pull it off?

Once you reach the validation check point, you’ll be presented with a whole new set of challenges. Because your environment is customized this means you will

need to carry out all the tests yourself to validate your system which will likely take weeks if not months. Then any time you're looking to make a change, you're looking at going through that whole validation process again.

At Greenlight Guru, it's our goal to alleviate these efforts and streamline your processes through our multi-tenant, cloud-based QMS platform.

Whether your're using our QMS or EDC product or both, our solution enables you to take your product to market faster, with less risk and more security to ensure optimal outcomes for patients.

Get your demo of Greenlight Guru to see how our solution can help you achieve and maintain compliance with 21 CFR Part 11.

21 CFR Part 11: A Complete Guide

Schedule Your Personalized Demo of Greenlight Guru

greenlight guru

www.greenlight.guru